



PROVINCIA DI PESCARA

SETTORE I - TECNICO

REGISTRO GENERALE N. 542 del 03/06/2026

Determina del Dirigente di Settore N. 386 del 03/06/2026

PROPOSTA N. 804 del 03/06/2026

OGGETTO: Approvazione DPIA ex art.35 Regolamento UE 679/2016 per sistema di videosorveglianza per la tutela delle postazioni di rilevamento infrazioni superamento velocità in SS714-SP2 e adeguamento determinazioni n. 266/2026-278/2026

Il Comandante della Polizia Provinciale, Dott. Giulio Honorati, in qualità di R.U.P del provvedimento in oggetto, giusto atto di determinazione n. 1316 del 28.11.2023(e decreto del Presidente n. 105/2022),

Visto il Decreto Presidenziale n. 10 del 29/10/2025 di “Conferimento incarico di dirigente del Settore I Tecnico all’Ing. Marco Scorrano.”

Visti il Decreto Presidenziale n.22 del 28/10/2022 “Servizio di Polizia provinciale: provvedimenti” e la Determinazione dirigenziale n.1250 del 28/11/2025 del Dirigente del Settore III Risorse Umane e Presidenza “Incarico di EQ del Servizio di Polizia provinciale periodo 01/12/2025 - 30/11/2026” conferito al Comandante Dott. Giulio Honorati”

La Delibera del Consiglio Provinciale N. 10 del 28.01.2026 “Bilancio di Previsione 2026 - 2028 e relativi allegati – Approvazione in via definitiva” e smi approvata nella seduta del Consiglio Provinciale del 28.01.2026;

Il Decreto del Presidente n. 15 del 04.02.2026 “PEG - Piano Esecutivo di Gestione 2026-2028” e smi

Vista la Delibera del Consiglio provinciale n. 35 del 28.11.2025 di approvazione del “Regolamento per dispositivi di acquisizione immagini e trattamento dei dati”

Premesso:

- che la Provincia di Pescara, ha fra i compiti istituzionali, la sicurezza delle strade che rientra nell'attività di pubblico interesse dell'esercizio delle funzioni amministrative dell'Ente;
- che tra gli strumenti idonei per l'espletamento di tale specifica funzione rientra quella di dotarsi di apparecchiature per il controllo della velocità da usare al fine di dissuadere l'utenza dal violare il Codice della Strada
- che con DdP n. 28 del 15.3.23, esecutivo ai sensi di legge, l'intervento in questione è stato inserito nel “programma biennale degli acquisiti di beni e servizi
- che con Determinazione n. 1345 del 06.12.2023 è stato approvato il capitolato speciale, anche con funzione di contratto, avente ad oggetto
“servizio di fornitura, noleggio, installazione e manutenzione ordinaria e straordinaria di dispositivi elettronici di rilevazione della velocità istantanea, ai sensi dell'art. 142 cds, fornitura di hardware e software per la gestione del ciclo sanzionatorio e servizi di back-office e front-office, l'attività di stampa ed imbustamento delle sanzioni ed affidamento del servizio di supporto alla gestione della riscossione coattiva derivanti da violazioni alle norme del codice della strada commesse da veicoli di cittadini italiani o stranieri e di supporto legale”

CIG A035F73B44 – CUI S00212850689202300008

per l'importo complessivo **massimo** di € 4.900.000,00, pubblicato con il

disciplinare, bando

gara e altri atti in data 12.12.2023 con scadenza 23.01.2024;

con atto di determinazione n°923 del 07/10/2024 è stato affidato tale servizio all'O.E.

R.T.I.

CROSS CONTROL SRL(ora SAFETY 21 SPA);

In data 25.06.2025 è stato siglato il relativo contratto di appalto con rep. n. 8756 (prot. n.12084/2025);

RILEVATO che:

- il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito "GDPR") relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, ha abrogato la direttiva 95/46/CE ed è diventato pienamente efficace in tutti gli Stati membri dal 25 maggio 2018;
- il GDPR è basato sul principio di accountability (responsabilizzazione) in virtù del quale il Titolare del trattamento adotta politiche e attua misure adeguate a garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali effettuato è conforme al GDPR;
- l'articolo 35 del GDPR stabilisce, in particolare, che il Titolare del trattamento è tenuto ad effettuare una valutazione di impatto (c.d. Data Protection Impact Assessment- DPIA) quando un trattamento, allorché prevede l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- ai sensi del GDPR la valutazione d'impatto sulla protezione dei dati è, pertanto, uno strumento importante di accountability in quanto permette di valutare e dimostrare il rispetto dei requisiti del trattamento come previsti dal Regolamento attraverso un processo inteso a: rappresentare le caratteristiche del trattamento dei dati personali; valutare la necessità e la proporzionalità del trattamento; valutare i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento, individuando le misure per affrontarli;
- l'art. 35 comma 3 prevede che la valutazione di impatto è richiesta, tra l'altro, nei casi di sorveglianza sistematica, su larga scala, di una zona accessibile al pubblico come nel caso di trattamento di dati personali effettuato tramite sistemi di videosorveglianza.

RICHIAMATO il regolamento per la disciplina della videosorveglianza sul territorio provinciale approvato con Deliberazione del Consiglio Provinciale n. 35 del 28/11/2025;

VISTO il Decreto Presidenziale n. 12 del 18.12.2025 di "Designazione Responsabile per il Trattamento dati personali acquisiti dal sistema di videosorveglianza previsto dal Regolamento provinciale(deliberazione consiliare n.35 del 28.11.2025) con attribuzione e delega di specifici compiti."

VISTA la determinazione n. 266 del 24.03.2026 di "Approvazione DPIA ex art. 35 Regolamento UE 679/2016 per utilizzo telecamere finalizzate al rilievo infrazioni superamento velocità su SS 714 e SP2";

DATO ATTO che gli impianti sotto indicati hanno anche un sistema di videosorveglianza finalizzato alla tutela degli stessi impianti e quindi che in attuazione dell'art. 35 del GDPR, e in accordo con il proprio Responsabile della protezione dei dati (DPO), la Provincia di Pescara ha rilevato la necessità di avviare un'analisi di impatto privacy per tale sistema di videosorveglianza finalizzato alla tutela del patrimonio relativamente a:

Installazione di due sistemi per il controllo della velocità media sulla Strada Statale S.S. 714 Tangenziale di Pescara, dal km 5+400 al Km 6+500 in direzione Sud e dal km 6+500 al km 5+400 in direzione Nord;

Installazione di due postazioni fisse di controllo elettronico della velocità istantanea monodirezionali con contestazione differita al km 11+850, in direzione Pescara, ed al km 13+360, in direzione Teramo, sulla Strada Provinciale S.P. 2 Lungofino;

al fine di valutare il rispetto ai principi privacy di tale trattamento ulteriore sulle medesime postazioni installate, i rischi connessi e le eventuali misure idonee ad affrontarli;

PRESO ATTO che è stata, pertanto, elaborata una prima versione della Valutazione per l'impiego di sistemi di videosorveglianza per l'uso di tali impianti finalizzati alla tutela da atti di vandalismo delle postazioni adibite al rilievo di infrazioni del superamento limiti di velocità:

in S.S.714 Tangenziale di Pescara – controllo velocità media - dal km 5+400 al Km 6+500 in direzione Sud e dal km 6+500 al km 5+400 in direzione Nord e
sulla S.P. Lungofino - controllo velocità istantanea - al km 11+850, in direzione Pescara, ed al km 13+360, in direzione Teramo.

CONSIDERATO che nel documento è contenuta una descrizione funzionale del trattamento, l'individuazione della relativa base giuridica, le modalità di utilizzo delle telecamere di videosorveglianza e le relative finalità, una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità, le regole per la conservazione delle immagini, le modalità di installazione della cartellonistica, una valutazione dei rischi per i diritti e le libertà degli interessati e le misure previste per affrontare i rischi;

TENUTO CONTO che:

- in data 01.06.2026 il DPO della Provincia di Pescara, ai sensi dell'art. 39 comma 1 lett. c) del GDPR, ha espresso *“A seguito dell'esame della Valutazione d'Impatto sulla Protezione dei Dati (DPIA) relativa al sistema di videosorveglianza installato a protezione dei rilevatori di velocità presenti sul territorio comunale, si esprime parere favorevole in merito all'iniziativa proposta, ritenendo che il trattamento, così come configurato, persegua una finalità legittima riconducibile alla tutela del patrimonio pubblico e alla prevenzione di atti vandalici che potrebbero compromettere il corretto funzionamento dei dispositivi destinati al controllo del rispetto delle norme del Codice della Strada.*

L'analisi svolta evidenzia infatti la presenza di misure organizzative e tecniche orientate alla protezione dei dati personali trattati e, in particolare, la previsione di un periodo di conservazione delle immagini che appare congruo rispetto alle finalità perseguite. Si ritiene tuttavia opportuno formulare alcune osservazioni migliorative che il Titolare del trattamento è invitato a valutare e recepire nell'ambito della documentazione definitiva, al fine di rafforzare ulteriormente la completezza della valutazione e garantire il più elevato livello di sicurezza e conformità del trattamento

Fermo restando quanto sopra evidenziato, le osservazioni formulate assumono carattere migliorativo e non pregiudicano il giudizio complessivamente favorevole sull'iniziativa. Si auspica pertanto che il Titolare del trattamento tenga conto delle raccomandazioni sopra riportate in sede di aggiornamento della documentazione, al fine di incrementare ulteriormente il livello di trasparenza, sicurezza e conformità del trattamento rispetto ai principi stabiliti dal Regolamento (UE) 2016/679.

TUTTO CIÒ PREMESSO IL DPO - esprime parere POSITIVO, fermo restando le prescrizioni sopra evidenziate.”

Preso atto delle osservazioni del DPO e cioè:

- *In primo luogo, si rileva l'opportunità di rendere maggiormente coerenti le diverse sezioni della DPIA. In particolare, il titolo del documento richiama espressamente la "tutela contro gli atti di vandalismo sulle telecamere facenti parte del sistema di rilevazione delle violazioni al Codice della Strada", mentre la descrizione del trattamento risulta prevalentemente focalizzata sulle attività di accertamento delle violazioni al Codice della Strada. Considerato che il sistema oggetto della valutazione è finalizzato alla protezione dei dispositivi e non all'accertamento delle infrazioni, si suggerisce di uniformare i contenuti del documento affinché emerga con chiarezza la reale finalità perseguita.*
- *Si raccomanda inoltre di descrivere in modo più dettagliato il flusso delle informazioni all'interno dell'architettura tecnologica adottata. Sebbene in altre sezioni del documento sia indicato che la trasmissione dei dati avviene mediante router 4G, tale informazione dovrebbe essere riportata anche nella descrizione generale del sistema, al fine di consentire una migliore comprensione delle modalità di trattamento. Nella medesima prospettiva, sarebbe opportuno chiarire le modalità di attivazione della registrazione, specificando se essa avvenga in maniera continua oppure a seguito dell'attivazione di sensori di movimento o di altri meccanismi di rilevazione.*
- *Con riferimento alle categorie di dati trattati, si suggerisce di menzionare espressamente, oltre alle altre informazioni già indicate, anche le immagini e i filmati che consentono l'identificazione o la riconoscibilità dei soggetti che si avvicinano ai dispositivi oggetto di tutela. Tale integrazione contribuirebbe a rappresentare in maniera più completa l'effettiva portata del trattamento.*
- *Per quanto riguarda la sezione dedicata alla necessità e proporzionalità del trattamento, si osserva che il documento risulta prevalentemente concentrato sugli aspetti di necessità, senza sviluppare adeguatamente la valutazione di proporzionalità richiamata nel titolo del paragrafo. Sarebbe pertanto opportuno illustrare le ragioni che rendono necessario installare un sistema di videosorveglianza a protezione di altri dispositivi di controllo, evidenziando, ove esistenti, precedenti episodi di danneggiamento o vandalismo che abbiano interessato i rilevatori fissi di velocità e che abbiano indotto l'Ente ad adottare misure di protezione e deterrenza ulteriori. Nello stesso contesto si rileva che il riferimento all'esecuzione di un contratto quale base giuridica del trattamento non appare sostenibile, considerato che l'articolo 6, paragrafo 1, lettera b), del Regolamento (UE) 2016/679 presuppone l'esistenza di un contratto tra il titolare e l'interessato, circostanza evidentemente non configurabile nei confronti di eventuali soggetti responsabili di atti vandalici.*
- *Particolare attenzione dovrà essere inoltre riservata agli obblighi di trasparenza. Si raccomanda che l'informativa semplificata relativa al sistema di videosorveglianza oggetto della presente DPIA sia distinta da quella concernente i rilevatori di velocità. Le finalità dei due trattamenti risultano infatti differenti: nel primo caso la videosorveglianza è finalizzata alla protezione del patrimonio e alla dissuasione di eventuali atti vandalici, mentre nel secondo caso il trattamento è diretto all'accertamento delle violazioni del Codice della Strada. Conseguentemente, il cartello informativo dovrà riportare chiaramente la specifica finalità di tutela dei dispositivi ed essere collocato prima dell'area sottoposta a ripresa.*
- *Si presume inoltre che l'informativa completa venga resa disponibile sul sito istituzionale dell'Ente in una sezione facilmente individuabile dagli interessati.*
- *Per quanto concerne le misure di sicurezza, si suggerisce di integrare la documentazione con una descrizione più dettagliata delle modalità di gestione delle credenziali di autenticazione, specificando le procedure di rilascio, i criteri utilizzati per individuare password deboli, la lunghezza minima richiesta e l'eventuale politica di scadenza periodica delle password.*
- *Si segnala inoltre la necessità di correggere alcuni aspetti descrittivi relativi all'archiviazione dei dati. Dalla documentazione emerge infatti che la conservazione*

delle registrazioni non avviene mediante hard disk dedicati, bensì attraverso schede di memoria installate direttamente sulle telecamere; tale circostanza dovrebbe essere rappresentata correttamente nella DPIA.

-Infine, la sezione dedicata alla crittografia presenta alcune incongruenze rispetto alle misure di controllo degli accessi logici illustrate in precedenza e contiene riferimenti a sistemi di convalida delle infrazioni che non sembrano rientrare nell'oggetto del trattamento analizzato. Si suggerisce pertanto una revisione del testo finalizzata ad eliminare tali incoerenze e a circoscrivere la descrizione esclusivamente alle componenti effettivamente ricomprese nel sistema oggetto della presente valutazione.

-Dal punto di vista organizzativo, pur risultando presenti gli elementi fondamentali, la DPIA non fornisce un quadro completo delle misure di governance della protezione dei dati, omettendo riferimenti a aspetti rilevanti quali la gestione dei data breach, la tracciabilità dei log, la protezione fisica dei dispositivi. Tali elementi devono essere

integrati per assicurare una rappresentazione esaustiva del sistema di gestione della protezione dei dati.

-Infine, con riguardo alla valutazione dei rischi, si rileva una non piena coerenza tra minacce, impatti e misure di mitigazione descritte. In più punti le categorie di rischio (riservatezza, integrità, disponibilità) risultano sovrapposte o non correttamente distinte, e alcune misure richiamate non trovano adeguata descrizione nelle sezioni precedenti. È pertanto opportuno rivedere l'analisi dei rischi secondo una logica più rigorosa e aderente agli standard metodologici, includendo anche il riferimento allo sfruttamento delle vulnerabilità informatiche come minaccia rilevante. “

CONSIDERATO necessario, per quanto sopra richiamato, approvare con riserva il documento di Valutazione di impatto – DPIA sulla protezione dei dati acquisiti mediante telecamere di videosorveglianza finalizzate al rilievo di infrazioni del superamento limiti di velocità, allegato e parte integrante al presente provvedimento, al fine di garantire che il trattamento avvenga nel rispetto delle disposizioni del GDPR e senza violare i diritti dei soggetti interessati;

PRECISATO che le considerazioni del DPO sopra riportate vengono formalizzate per consentire che la DPIA allegata e parte integrante del presente provvedimento, venga integrata e migliorata nei mesi successivi e comunque nell'anno in corso;

Ritenuto opportuno adeguare di conseguenza le determinazioni, sia nella premessa che nel dispositivo di entrambe,

n.266 del 24.03.2026 di approvazione DPIA per per utilizzo telecamere finalizzate al rilievo infrazioni superamento velocità su SS 714 e SP2”;

n.278 del 26.03.2026 di approvazione DPIA per utilizzo telecamere finalizzate al rilievo infrazioni semaforiche in località Cerratina di Pianella”

prevedendo al posto di “di integrare e migliorare la presente DPIA secondo le considerazioni del DPO entro il mese di giugno 2026

la frase “**di integrare e migliorare la presente DPIA secondo le considerazioni del DPO nei mesi successivi e comunque nell'anno in corso**”

RIBADITO che viene garantire un costante e puntuale aggiornamento dei contenuti del documento di DPIA anche mediante un continuo dialogo con il DPO per garantire la tutela degli interessati e, ove necessario, operare con un tempestivo intervento per risolvere eventuali criticità riscontrate in sede di applicazione;

Precisato che il R.U.P. Comandante della Polizia Provinciale, Dott. Giulio Honorati,

assicura per il procedimento in argomento il corretto iter amministrativo e il rispetto delle norme a riguardo;

Ciò premesso e considerato si propone l'adozione del presente atto.

Il sottoscritto Dott. Ing. Marco Scorrano, Dirigente del Settore I Tecnico

e Responsabile del Trattamento dei dati personale alla luce di quanto sopra;

Vista l'istruttoria del procedimento de quo a cura del R.U.P., della quale se ne condivide la correttezza;

Espresso parere favorevole attestante la regolarità e la correttezza dell'azione amministrativa, ai sensi dell'art. 147bis, comma 1 del D.Lgs.vo n. 267/2000 ss.mm.ii.;

VISTI:

- il decreto legislativo 30 giugno 2003, n.196 "Codice in materia di protezione dei dati personali" come modificato dal decreto legislativo 10 agosto 2018, n.101 e dalla legge 27 dicembre 2019, n.160;
- il 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 – RGPD);
- i Provvedimenti dell'Autorità Garante per la protezione dei dati personali "in materia di videosorveglianza" dell'8 aprile 2010 (pubblicato in Gazzetta Ufficiale n. 99 del 29 aprile 2010) e n. 467 (allegato n. 1) dell'11 ottobre 2018 rubricato "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018", (pubblicato in Gazzetta Ufficiale, Serie Generale, n. 269 del 19 novembre 2018);
- le Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248)
- la Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio";
- il decreto del Presidente della Repubblica 15 gennaio 2018, n.15 "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia";
- il decreto legislativo 18 maggio 2018, n.51 recante "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Con

Visto l'art. 107 (*Funzioni e responsabilità della dirigenza*) del TUEL 267/2000;

Dichiarata l'insussistenza di situazioni, anche potenziali, di conflitto d'interesse ai sensi dell'art. 6-bis della L.241/90;

Verificata la coerenza con la check list di riferimento di cui alla determina n.738/2024 relativa al piano operativo di controllo di regolarità amministrativa 2024

DETERMINA

- 1. di approvare** la premessa quale parte integrante e sostanziale del presente atto;
- 2. di approvare** il documento di Valutazione di impatto sulla protezione dei dati personali (DPIA), parte integrante e sostanziale del presente provvedimento, per il sistema di videosorveglianza finalizzato alla tutela da atti di vandalismo sugli impianti/postazioni di rilevazione immagini per il rilievo di infrazioni del superamento limiti di velocità in **S.S.714 Tangenziale di Pescara** – controllo velocità media - dal km 5+400 al Km 6+500 in direzione Sud e dal km 6+500 al km 5+400 in direzione Nord
S.P. Lungofino - controllo velocità istantanea - al km 11+850, in direzione Pescara, ed al km 13+360, in direzione Teramo;
- 3. di integrare e migliorare** la presente DPIA secondo le considerazioni del DPO nei mesi successivi e comunque nell'anno in corso;
- 4. di prevedere** comunque che tale documento venga periodicamente aggiornato ogni qualvolta si renda necessario e in funzione di eventuali criticità anche mediante un continuo dialogo con il DPO per garantire la tutela degli interessati;
5. adeguare di conseguenza le determinazioni, sia nella premessa che nel dispositivo di entrambe,
n.266 del 24.03.2026 di approvazione DPIA per per utilizzo telecamere finalizzate al rilievo infrazioni superamento velocità su SS 714 e SP2";
n.278 del 26.03.2026 di approvazione DPIA per utilizzo telecamere finalizzate al rilievo infrazioni semaforiche in località Cerratina di Pianella"
prevedendo al posto di "di integrare e migliorare la presente DPIA secondo le considerazioni del DPO entro il mese di giugno 2026"
la frase "**di integrare e migliorare la presente DPIA secondo le considerazioni del DPO nei mesi successivi e comunque nell'anno in corso**"
- 6. di disporre** che tutti i soggetti coinvolti nella gestione di tale sistema di videosorveglianza dell'Ente siano informati del presente provvedimento e osservino le prescrizioni presenti al suo interno;
- 7. di dare atto** che il documento allegato riguardante l'informativa sul trattamento dei dati personali dovrà essere pubblicato sul sito istituzionale della Provincia alla pagina dedicata alle informative privacy;
- 8. di dare atto** che avverso il presente atto è possibile il ricorso al T.A.R. Abruzzo ex art.119 del D.Lgs. n.104/2010 e art.120 comma 5 del c.p.a;
- 9. di dare atto** altresì che sarà verificato il rispetto delle disposizioni in materia di trasparenza mediante la pubblicazione dei dati obbligatori nella sezione **AMMINISTRAZIONE TRASPARENTE** del sito web dell'Ente.



PROVINCIA DI PESCARA

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

DPIA – Trattamento dati Sistemi rilevamento velocità

Il Regolamento UE 2016/679 (General Data Protection Regulation) relativo al trattamento dei dati personali nonché alla loro circolazione, e con l'applicazione del principio ispiratore della accountability, impone al Titolare e Responsabile del Trattamento:

l'adozione di tutte le misure necessarie finalizzate a garantire la protezione e la sicurezza dei dati trattati, tra cui, ai sensi dell'art. 35 del GDPR e del relativo Regolamento provinciale, lo svolgimento di una valutazione preventiva (Data Protection Impact Assessment - DPIA) sui trattamenti eseguiti e l'impatto di essi sulla libertà ed i diritti delle persone fisiche, specificamente nell'ambito dell'utilizzazione dei sistemi di videosorveglianza.

Il presente documento rappresenta l'esito della DPIA svolta nell'ambito dei sistemi di videosorveglianza sui misuratori di velocità utilizzati dalla Provincia di Pescara finalizzati al raggiungimento di obiettivi relativi a:

- a) tutelare e monitorare la sicurezza stradale, controllando la circolazione lungo le strade del territorio provinciale;
- b) verificare e sanzionare, attraverso gli appositi apparati omologati/approvati per l'accertamento delle infrazioni al codice stradale, violazioni della velocità;

DPIA

Informazioni sulla DPIA

Nome della DPIA: Valutazione sul sistema di Videosorveglianza della Provincia di Pescara per la tutela contro gli atti di vandalismo sulle telecamere facenti parte del sistema di rilevazioni delle violazioni al Codice della Strada.

Titolare del trattamento dati: è la Provincia di Pescara, da cui dipende l'organo di polizia provinciale che procede all'accertamento, nella persona del Presidente pro- tempore.

Nome autore:

Comandante Polizia Provinciale: Dott. Giulio Honorari(supporto/consulenza Maggioli Spa-Avv. Guido Paratico):

Data di creazione- aggiornamento: 16/04/2026

Nome del DPO/RPD: Ing. Aldo Lupi

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Non si ritiene opportuno procedere alla richiesta di alcun parere agli Interessati per impossibilità oggettiva.

Norme di riferimento:

Regolamento UE 2016/679 (GDPR) - art. 25

Articolo Privacy D. Lgs. 196/2003 e s.m.i.

Art. 105 C. C. P. D. L. 144/2000

DESCRIZIONE DEL TRATTAMENTO

Il trattamento dati effettuato dalla Provincia di Pescara nel tratto del proprio territorio ha finalità di:

- prevenzione dell'incidentalità stradale
- accertamento delle violazioni al Codice della Strada, superamento limiti di velocità,
D. Lgs 285/1992, art. 142.

Valutazione: Migliorabile

Commento di valutazione: Il nome della DPIA parla di *"tutela contro gli atti di vandalismo sulle telecamere facenti parte del sistema di rilevazioni delle violazioni al Codice della Strada"*. Poi la descrizione del trattamento si focalizza sull'accertamento delle violazioni al CdS. Si consiglia di dare maggiore coerenza ai contenuti, atteso che le telecamere sono a tutela del patrimonio, come di seguito descritto.

CONTESTO OPERATIVO:

La Provincia di Pescara ha installato due sistemi di rilevazione della velocità, di cui uno di rilevazione della velocità media ed uno di rilevazione della velocità puntuale, forniti dalla ditta Safety21. I sistemi di velocità media prevedono l'installazione di due portali di ingresso ed uscita dalla zona oggetto di rilevazione della velocità media. Il sistema della velocità puntuale prevede l'installazione di singole postazioni di rilevazione della velocità istantanea.

Ciò premesso, nella Provincia di Pescara per ogni punto di rilevazione sono installate anche delle telecamere di videosorveglianza, modello Hikvision DS-2CD2047G2-L o simile, preposte alla tutela del patrimonio e in particolare ad attestare e prevenire eventuali atti vandalici posti in essere sulle attrezzature che compongono i sistemi di rilevazione.

Le telecamere sono quindi posizionate in corrispondenza dei punti di rilevazione:

- **due sistemi** per il controllo della **velocità media** sulla Strada Statale S.S. 714 Tangenziale di Pescara, in corrispondenza del km 5+400 e del Km 6+500 in direzione Sud e in corrispondenza del km 6+500 e del km 5+400 in **direzione Nord**.
- **due postazioni** fisse di controllo elettronico della **velocità istantanea** al km 11+850, in direzione Pescara, ed al km 13+360, in **direzione Teramo**, sulla Strada Provinciale S.P. 2 Lungofino.

Le telecamere, sono poste sui pali di sostegni dei sistemi di rilevazione e riprendono solo l'area strettamente limitrofa al palo su cui sono state installate le postazioni di rilevazione della velocità, evitando la raccolta di immagini non pertinenti.

MODALITA' DI ACQUISIZIONE DELLE IMMAGINI:

Il sistema opera 24h/24h, e riprende solo l'area di installazione, senza riprendere veicoli o passanti. Vi è quindi possibilità di acquisizione di immagini solo nelle ipotesi in cui una persona fisica si avvicini al palo di installazione, laddove non è prevista la presenza di persone.

Le immagini acquisite vengono inviate con connessione sicura VPN.

Le immagini vengono trattate tramite una piattaforma software che consente agli utenti di visualizzare in tempo reale, registrare, riprodurre filmati e gestire i dispositivi di sorveglianza in modo centralizzato al server posizionato presso il Comando di Polizia Provinciale.

Sicurezza dell'hardware

La rete con la quale sono gestite le immagini e la verbalizzazione è connessa ad internet, che, oltre alle credenziali personali è presente una password sul PC di accesso al server.

CICLO DI VITA DEL TRATTAMENTO DEI DATI

Raccolta: I dati vengono raccolti in locale all'interno dei dispositivi e trasferiti, su richiesta del Titolare, verso il client software tramite una connessione sicura VPN. L'accesso ai dati è limitato ai soggetti puntualmente autorizzati.

Conservazione: I dati sono conservati in locale all'interno dei dispositivi su scheda di memoria crittografata per il tempo strettamente necessario alle finalità del trattamento (v. sezione "Periodo di conservazione"). In funzione dei privilegi concessi, gli utenti, autorizzati dal titolare del trattamento, possono memorizzare le registrazioni video sui dispositivi dove è installato il client software di gestione nei limiti della normativa

vigente in materia.

Eventuale cancellazione o anonimizzazione: Al termine del periodo di conservazione pari a 72 ore, i dati vengono sovrascritti in modo sicuro (processo di sovrascrittura automatica).

Valutazione: **Migliorabile**

Commento di valutazione: Si consiglia di descrivere in maniera più chiara il flusso di informazioni attraverso le componenti del sistema. Nei paragrafi successivi è specificato che la trasmissione avviene tramite router 4G: tali informazioni andrebbero menzionate anche nella descrizione del sistema. Si consiglia inoltre di specificare come si attiva la registrazione, cioè se vi sono dei sensori di movimento o se la registrazione è costante.

CATEGORIE DI PERSONE INTERESSATI DEL TRATTAMENTO E DATI PERSONALI TRATTATI:

Categoria di interessati: i dati trattati riguardano solo eventuali soggetti ripresi dalle telecamere perché avvicinati al palo di sostegno dei sistemi di rilevazione.

Categorie di dati trattati:

- Dati personali comuni anagrafici: non trattati
- Dati personali comuni di contatto: non trattati
- Dati personali comuni relativi alla posizione: ora e luogo

dell'infrazione PERIODO DI CONSERVAZIONE DATI E FOTOGRAMMI:

Le immagini sono conservate per un periodo non superiore a 72h, con sovrascrittura automatica.

La conservazione per un periodo di 72h risulta congruo in caso di atti vandalici nella giornata del sabato pomeriggio con visione delle immagini nella giornata di lunedì.

Valutazione: **Migliorabile**

Commento di valutazione: Tra i dati acquisiti andrebbero menzionati anche immagini/video che consentano la riconoscibilità dei soggetti che si avvicinano ai dispositivi. Il periodo di conservazione appare congruo.

Principi Fondamentali

PROPORZIONALITÀ E NECESSITÀ

La liceità è data dall'art. 6 par. 1 del GDPR 2016/679, in quanto "il trattamento è necessario per l'esecuzione del contratto" ovvero dell'esecuzione del contratto di affidamento del servizio di rilevazione delle violazioni della velocità nonché di un compito di interesse pubblico, relativo alla tutela di beni patrimoniali dell'Ente pubblico.

Il trattamento **proporzionato**, in quanto l'angolo di ripresa è limitato all'area immediatamente circostante il palo su cui sono installati i sistemi di rilevazione delle violazioni al CdS e la possibilità di ripresa di immagini di persone fisiche è limitata

all'ipotesi in cui le persone si avvicinino alla struttura in un'area in cui ciò non dovrebbe avvenire.

Valutazione: Migliorabile

Commento di valutazione: Il titolo del periodo parla di "proporzionalità e necessità", ma in realtà la proporzionalità non è in alcun modo menzionata. Sarebbe invece opportuno spiegare per quale motivo sia necessario installare delle telecamere per sorvegliare altri dispositivi di sorveglianza: ad esempio, la necessità potrebbe evincersi dal fatto che in passato si siano registrati atti di vandalismo verso i rilevatori fissi di velocità, che hanno portato l'ente a introdurre dei sistemi di dissuasione. L'esecuzione di un contratto non è una base di liceità in alcun modo sostenibile, poiché la norma esplicita che *"il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte"*: appare evidente che non vi sia alcun contratto in essere con eventuali vani

MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

Gli interessati che si trovano nelle vicinanze dei sistemi di rilevazione sono informati, attraverso un apposito cartello informativo, secondo il modello approvato dal Garante della Privacy (informativa di primo livello) della presenza delle telecamere in postazione fissa, prima del raggio di azione del controllo stesso.

La segnaletica ha un formato ed un posizionamento tale da essere chiaramente visibile.

Si specifica inoltre che nella sezione "privacy", o comunque nella sezione Polizia Provinciale, del sito web istituzionale della Provincia di Pescara viene riportata l'informativa completa sul trattamento dei dati di videosorveglianza ai sensi dell'art. 13 del GDPR UE 679/2016.

Valutazione: Migliorabile

Commento di valutazione: Si raccomanda molta attenzione, poiché l'informativa semplificata dovrebbe essere separata dall'informativa relativa ai rilevatori di velocità. In questo caso la finalità è dissuasiva verso eventuali vandali (e non di rilevazione violazioni al CdS), pertanto il cartello deve esplicitare tale circostanza ed essere posizionato prima dello spazio di ripresa. Si assume che l'informativa completa venga posizionata sul sito, in una zona facilmente raggiungibile.

CONSENSO DEGLI INTERESSATI

La base giuridica del trattamento è lo svolgimento di un compito connesso all'esercizio di un pubblico interesse che è di tutela del patrimonio per la prevenzione dei reati proprio contro il patrimonio.

Pertanto, non è richiesto il consenso dell'interessato.

Valutazione: Accettabile

Commento di valutazione: La descrizione risulta coerente, anche se andrebbero specificati anche i diritti esercitabili dell'interessato.

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

Gli obblighi del Responsabile del trattamento sono assunti mediante specifica determina di affidamento di incarico e successiva stipula di contratto, con nomina di responsabile del trattamento, ai sensi dell'art 28 del Reg U.E 2016/679.

Valutazione: Accettabile

Commento di valutazione: La descrizione risulta coerente con il contesto, atteso che la descrizione del servizio manutentivo deve essere dettagliata.

MISURE ESISTENTI O PIANIFICATE

Solo il personale autorizzato o i preposti possono accedere alle immagini conservate sul server attraverso dei propri username e delle proprie password. Il sistema segnala all'utente l'utilizzo di una password considerata troppo debole, invitandolo così ad utilizzarne una adeguata, di almeno 8 caratteri con maiuscola, minuscola, un carattere speciale.

I dati raccolti verranno archiviati localmente su scheda di memoria crittografata per il tempo strettamente necessario al raggiungimento delle finalità del trattamento (72 ore). Al termine del periodo di conservazione, i dati vengono eliminati in modo sicuro con sovrascrittura automatica.

Il dispositivo è connesso tramite LAN a un router 4G, il quale, attraverso una connessione sicura e protetta VPN, funge da punto di accesso per visualizzare le registrazioni della telecamera. Le registrazioni sono disponibili per la visione sia in modalità sincrona che asincrona, tramite un software di gestione nella disponibilità del Titolare del trattamento.

L'accesso alla piattaforma di gestione sarà strettamente controllato e monitorato dal Titolare del trattamento. I tecnici abilitati della Ditta Safety21 S.p.A. fornitrice degli strumenti saranno autorizzati all'accesso per operazioni di manutenzione, sia tramite la piattaforma di gestione che direttamente sui dispositivi.

Valutazione: Migliorabile

Commento di valutazione: sarebbe necessario chiarire le modalità di rilascio delle credenziali, quali sono i criteri per cui una password è considerata debole, la lunghezza prevista e l'eventuale scadenza delle password

Archiviazione

L'archiviazione sugli hard disk è fissata secondo i termini di conservazione dei dati dell'Ente, cioè di 72 ore con sovrascrittura automatica.

Valutazione: Migliorabile

Commento di valutazione: l'archiviazione non avviene sugli hard disk, bensì sulle schede di memoria posizionate sulle telecamere.

Vulnerabilità

I software e l'hardware sono aggiornati al bisogno durante l'attività di manutenzione

compiuta dal Responsabile del trattamento dei dati.

I pc in uso sono dotati di sistemi operativi e antivirus costantemente aggiornati.

L'accesso ai dati è consentito unicamente agli autorizzati, muniti di account personale.

Valutazione: Accettabile

Commento di valutazione: La descrizione risulta coerente con il contesto.

Crittografia

I dati memorizzati in locale sono protetti con crittografia Advanced Encryption Standard (AES).

Autenticazione a più fattori (MFA): predisposizione per l'accesso ai sistemi, mediante SPID/CIE, da parte del personale autorizzato, con controllo basato su ruoli e privilegi.

Anche la semplice visualizzazione di un'immagine è tracciata e non è possibile visualizzare un'immagine se non passando dal processo di autenticazione attraverso il programma di convalida delle infrazioni.

Valutazione: Migliorabile

Commento di valutazione: la descrizione non è coerente con le misure di gestione degli accessi logici precedentemente descritti. Inoltre, si fa menzione a sistemi di convalida delle infrazioni, che non sono oggetto della presente DI

Lotta contro il malware

L'anti malware è regolarmente installato e costantemente aggiornato.

Aggiornamenti e patch management: monitoraggio costante e applicazione di patch di sicurezza a sistemi operativi e software.

Firewall e protezione da malware: implementazione di firewall di rete per prevenire accessi non autorizzati e attacchi informatici

Valutazione: Accettabile

Commento di valutazione: La descrizione risulta coerente con il contesto.

Gestione postazioni

Il PC, sito nell'ufficio della polizia provinciale, è utilizzabile solo dal designato o dai preposti muniti di credenziali di accesso personali. Il server non necessita di accesso da parte del personale in loco.

Valutazione: Accettabile

Commento di valutazione: La descrizione risulta coerente con il contesto.

Politica di tutela della privacy

Si è proceduto alla nomina del Data Protection Officer-DPO. Si è proceduto alle autorizzazioni al trattamento dati personali, inserite e visibili sul sito web Provincia di Pescara-Polizia Provinciale. Vengono predisposte adeguate informative con cartellonistica sul luogo(I livello) e con informativa più estesa sul web istituzionale Provincia di Pescara- Polizia Provinciale(II livello).

Valutazione: Accettabile

Commento di valutazione: La descrizione risulta coerente con il contesto.

Gestione delle politiche di tutela della privacy

Il Titolare del trattamento ha approvato un Regolamento comunale relativo alla protezione dei dati personali oltre ad uno specifico regolamento in materia di videosorveglianza.

I dati non sono trasferiti in paesi al di fuori dell'Unione Europea.

Nel caso specifico non vi sono archivi cartacei.

Valutazione: Accettabile

Commento di valutazione: La descrizione risulta coerente con il contesto.

Gestione del personale

Il personale autorizzato al trattamento riceve annualmente dal DPO, in presenza, una formazione generale in merito alla protezione dei dati personali, così come prevista dal vigente regolamento europeo 2016/679, sessioni di formazione su specifici argomenti, all'occorrenza. La nomina del designato dà conto del dovere di riservatezza cui sono tenuti, in base alla normativa vigente.

Valutazione: Accettabile

Commento di valutazione: La descrizione risulta coerente con il contesto.

Accessi diversificati

La password è diversificata tra il Designato al trattamento, i preposti al trattamento ed il Responsabile del trattamento in modo da poter identificare chi accede al sistema.

Valutazione: Accettabile

Commento di valutazione: La descrizione risulta coerente con il contesto.

Misure antincendio

Il trattamento dei dati avviene nel pieno rispetto degli obblighi normativi in materia di prevenzione incendi.

Valutazione: Accettabile

Commento di valutazione: La descrizione risulta coerente con il contesto.

CARENZE DI FONDO SULLE MISURE ADOTTATE E DESCRITTE

Nel documento non si fa alcun riferimento a:

- la modalità di gestione dei data breach

- la tracciabilità dei log non è gestita

protezione fisica dei dispositivi da interventi umani e circostanze ambientali

Rischi

Accesso illegittimo ai dati

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

Perdita o alterazione, anche irreversibile dei dati.

Perdita o alterazione, anche irreversibile dei programmi. Impossibilità temporanea di accesso di dati.

Impossibilità temporanea di accesso ai programmi.

Per gli interessati: lesione del diritto d'immagine, lesione del diritto alla riservatezza, percezione di insicurezza.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Attacco da remoto ai sistemi da parte di hacker; Accesso non autorizzati; Visione dei monitor in diretta per una finalità illegittima se non illecita.

Quali sono le fonti di rischio?

Fonti umane interne; Personale non adeguatamente preparato; Fonti umane esterne; Hacker.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Anonimizzazione, Crittografia, Controllo degli accessi logici, Tracciabilità, Minimizzazione dei dati, Gestione postazioni, Lotta contro il malware, Politica di tutela della privacy, Vulnerabilità, Gestione del personale, Gestione delle politiche di tutela della privacy, Controllo degli accessi fisici, Sicurezza dei canali informatici, Manutenzione.

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

Accettabile: la gravità delle conseguenze di un ipotetico accesso non autorizzato può riguardare la visione, relativamente alle immagini riguardanti una persona avvicinata incidentalmente alla struttura di sostegno dei sistemi di rilevazione delle infrazioni al CdS.. Il numero di immagini di persone fisiche che possono essere rilevate è pertanto molto limitato. Pertanto anche in caso di attacco è improbabile che tra le immagini registrate vi siano persone fisiche.

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

Trascurabile: le misure di sicurezza paiono adeguate a proteggere i dati personali trattati da accessi non autorizzati in considerazione del contesto con il quale vengono effettuati i fotogrammi con l'apparecchiatura in uso. La probabilità di concretizzazione del rischio di accesso illegittimo ai dati è trascurabile, soprattutto per quanto concerne gli attacchi di soggetti esterni all'ente.

Valutazione: **Migliorabile**

Commento di valutazione: **Gli effetti descritti fanno riferimento più alla perdita di disponibilità**

(perdita o alterazione dei dati e dei programmi, impossibilità di accesso) piuttosto che di riservatezza. Tra le minacce non è menzionato lo sfruttamento di vulnerabilità informatiche in generale, che rappresenta un elemento rilevante. Alcune delle misure di mitigazione menzionate non sono state illustrate nel documento (anonimizzazione, tracciabilità, controllo degli accessi fisici, manutenzione).

Rischi

Modifiche indesiderate dei dati

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

Lesione al diritto all'immagine; Lesione all'integrità del dato personale; Impossibilità di tutela a seguito di un reato subito; Percezione di insicurezza.

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

Attacco da remoto ai sistemi da parte di hacker; Accesso non autorizzati alla sala di controllo; Visione dei monitor in diretta per una finalità illegittima se non illecita.

Quali sono le fonti di rischio?

Fonti umane interne; Personale non adeguatamente preparato; Fonti umane esterne; Hacker.

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

Anonimizzazione, Crittografia, Controllo degli accessi logici, Tracciabilità, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Gestione postazioni, Manutenzione, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Politica di tutela della privacy, Accessi diversificati, Gestione del personale.

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

Limitata: una modificazione indesiderata delle immagini comporterebbe un rischio limitato con riguardo al profilo psicologico dell'interessato. Il senso di violazione della propria riservatezza sarebbe apprezzabile, sebbene priva di danni irreparabili. Ciò potrebbe comportare un disturbo di contenuta gravità ma oggettivo, soprattutto nelle persone più suscettibili. Le immagini alterate potrebbero essere utilizzate, in linea teorica, per scherni, intimidazioni o ricatti verso gli interessati ad opera di malintenzionati.

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

Trascurabile: sebbene il rischio zero sia da considerarsi un'utopia a carattere precipuamente teorico, la modifica dell'immagine raccolta da una telecamera di videosorveglianza è un'operazione tecnicamente molto complessa. Il rapporto costi/benefici tra i mezzi impiegati ed i risultati ottenuti per compiere l'azione illecita

risulta davvero sproporzionato. In ogni caso, le misure di sicurezza che sono state adottate contribuiscono ad abbattere drasticamente la già scarsissima probabilità di verifica dell'evento.

Valutazione: **Migliorabile**

Commento di valutazione: Le minacce menzionate sarebbero più riferibili ad una perdita di riservatezza (Accesso non autorizzati alla sala di controllo; Visione dei monitor in diretta), piuttosto che di integrità. Alcune delle misure di mitigazione menzionate non sono state illustrate nel documento (Anonimizzazione, tracciabilità, controllo degli accessi fisici, manutenzione).

Rischi

Perdita dei dati

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

Lesione alla integrità del dato personale; Impossibilità di tutela a seguito di un reato subito; Percezione di insicurezza.

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

Attacco da remoto; Accesso non autorizzati alla sala di controllo; Malfunzionamenti fisici dei sistemi; Eventi naturalistici.

Quali sono le fonti di rischio?

Fonti umane interne; Personale non adeguatamente preparato; Fonti umane esterne; Hacker.

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

Anonimizzazione, Crittografia, Controllo degli accessi logici, Archiviazione, Sicurezza dei canali informatici, Controllo degli accessi fisici, Sicurezza dell'hardware, Gestione delle politiche di tutela della privacy, Gestione del personale, Accessi diversificati, Politica di tutela della privacy, Manutenzione, Backup, Gestione postazioni, Tracciabilità, Vulnerabilità, Lotta contro il malware, Misure antincendio.

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

Limitata: una perdita indesiderata delle immagini comporterebbe un rischio limitato con riguardo al profilo psicologico dell'interessato. La perdita del dato comporterebbe l'impossibilità di utilizzare le immagini per accertare gli autori di eventuali atti di vandalismo, ma senza conseguenze per i soggetti ripresi che hanno eseguito tali atti di vandalismo.

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

Trascurabile: le misure di sicurezza che sono state adottate contribuiscono ad abbattere drasticamente la probabilità di verifica di una perdita dei dati.

Valutazione: Migliorabile

Commento di valutazione: Alcune delle misure di mitigazione menzionate non sono state illustrate nel documento (Anonimizzazione, tracciabilità, controllo degli accessi fisici, manutenzione). Altre misure sono descritte più approfonditamente rispetto alla sezione dedicata (backup, misure antincendio): potrebbe essere opportuno procedere ad una descrizione più decisa nella sezione dedicata alla mitigazione.

Il Titolare del trattamento: Il Presidente della Provincia

Il Responsabile della Protezione dei dati è: Ing. Aldo Lupi

PARERE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

A seguito dell'esame della Valutazione d'Impatto sulla Protezione dei Dati (DPIA) relativa al sistema di videosorveglianza installato a protezione dei rilevatori di velocità presenti sul territorio comunale, si esprime parere favorevole in merito all'iniziativa proposta, ritenendo che il trattamento, così come configurato, persegua una finalità legittima riconducibile alla tutela del patrimonio pubblico e alla prevenzione di atti vandalici che potrebbero compromettere il corretto funzionamento dei dispositivi destinati al controllo del rispetto delle norme del Codice della Strada.

L'analisi svolta evidenzia infatti la presenza di misure organizzative e tecniche orientate alla protezione dei dati personali trattati e, in particolare, la previsione di un periodo di conservazione delle immagini che appare congruo rispetto alle finalità perseguite. Si ritiene tuttavia opportuno formulare alcune osservazioni migliorative che il Titolare del trattamento è invitato a valutare e recepire nell'ambito della documentazione definitiva, al fine di rafforzare ulteriormente la completezza della valutazione e garantire il più elevato livello di sicurezza e conformità del trattamento.

In primo luogo, si rileva l'opportunità di rendere maggiormente coerenti le diverse sezioni della DPIA. In particolare, il titolo del documento richiama espressamente la "tutela contro gli atti di vandalismo sulle telecamere facenti parte del sistema di rilevazione delle violazioni al Codice della Strada", mentre la descrizione del trattamento risulta prevalentemente focalizzata sulle attività di accertamento delle violazioni al Codice della Strada. Considerato che il sistema oggetto della valutazione è finalizzato alla protezione dei dispositivi e non all'accertamento delle infrazioni, si suggerisce di uniformare i contenuti del documento affinché emerga con chiarezza la reale finalità perseguita.

Si raccomanda inoltre di descrivere in modo più dettagliato il flusso delle informazioni

all'interno dell'architettura tecnologica adottata. Sebbene in altre sezioni del documento sia indicato che la trasmissione dei dati avviene mediante router 4G, tale informazione dovrebbe essere riportata anche nella descrizione generale del sistema, al fine di consentire una migliore comprensione delle modalità di trattamento. Nella medesima prospettiva, sarebbe opportuno chiarire le modalità di attivazione della registrazione, specificando se essa avvenga in maniera continua oppure a seguito dell'attivazione di sensori di movimento o di altri meccanismi di rilevazione.

Con riferimento alle categorie di dati trattati, si suggerisce di menzionare espressamente, oltre alle altre informazioni già indicate, anche le immagini e i filmati che consentono l'identificazione o la riconoscibilità dei soggetti che si avvicinano ai dispositivi oggetto di

tutela. Tale integrazione contribuirebbe a rappresentare in maniera più completa l'effettiva portata del trattamento.

Per quanto riguarda la sezione dedicata alla necessità e proporzionalità del trattamento, si osserva che il documento risulta prevalentemente concentrato sugli aspetti di necessità, senza sviluppare adeguatamente la valutazione di proporzionalità richiamata nel titolo del paragrafo. Sarebbe pertanto opportuno illustrare le ragioni che rendono necessario installare un sistema di videosorveglianza a protezione di altri dispositivi di controllo, evidenziando, ove esistenti, precedenti episodi di danneggiamento o vandalismo che abbiano interessato i rilevatori fissi di velocità e che abbiano indotto l'Ente ad adottare misure di protezione e deterrenza ulteriori. Nello stesso contesto si rileva che il riferimento all'esecuzione di un contratto quale base giuridica del trattamento non appare sostenibile, considerato che l'articolo 6, paragrafo 1, lettera b), del Regolamento (UE) 2016/679 presuppone l'esistenza di un contratto tra il titolare e l'interessato, circostanza evidentemente non configurabile nei confronti di eventuali soggetti responsabili di atti vandalici.

Particolare attenzione dovrà essere inoltre riservata agli obblighi di trasparenza. Si raccomanda che l'informativa semplificata relativa al sistema di videosorveglianza oggetto della presente DPIA sia distinta da quella concernente i rilevatori di velocità. Le finalità dei due trattamenti risultano infatti differenti: nel primo caso la videosorveglianza è finalizzata alla protezione del patrimonio e alla dissuasione di eventuali atti vandalici, mentre nel secondo caso il trattamento è diretto all'accertamento delle violazioni del Codice della Strada. Conseguentemente, il cartello informativo dovrà riportare chiaramente la specifica finalità di tutela dei dispositivi ed essere collocato prima dell'area sottoposta a ripresa. Si presume inoltre

che l'informativa completa venga resa disponibile sul sito istituzionale dell'Ente in una sezione facilmente individuabile dagli interessati.

Per quanto concerne le misure di sicurezza, si suggerisce di integrare la documentazione con una descrizione più dettagliata delle modalità di gestione delle credenziali di autenticazione, specificando le procedure di rilascio, i criteri utilizzati per individuare password deboli, la lunghezza minima richiesta e l'eventuale politica di scadenza periodica delle password.

Si segnala inoltre la necessità di correggere alcuni aspetti descrittivi relativi all'archiviazione dei dati. Dalla documentazione emerge infatti che la conservazione delle registrazioni non avviene mediante hard disk dedicati, bensì attraverso schede di memoria installate direttamente sulle telecamere; tale circostanza dovrebbe essere rappresentata correttamente nella DPIA.

Infine, la sezione dedicata alla crittografia presenta alcune incongruenze rispetto alle misure

di controllo degli accessi logici illustrate in precedenza e contiene riferimenti a sistemi di convalida delle infrazioni che non sembrano rientrare nell'oggetto del trattamento analizzato. Si suggerisce pertanto una revisione del testo finalizzata ad eliminare tali incoerenze e a circoscrivere la descrizione esclusivamente alle componenti effettivamente ricomprese nel sistema oggetto della presente valutazione.

Dal punto di vista organizzativo, pur risultando presenti gli elementi fondamentali, la DPIA non fornisce un quadro completo delle misure di governance della protezione dei dati, omettendo riferimenti a aspetti rilevanti quali la gestione dei data breach, la tracciabilità dei log, la protezione fisica dei dispositivi. Tali elementi devono essere integrati per assicurare una rappresentazione esaustiva del sistema di gestione della protezione dei dati.

Infine, con riguardo alla valutazione dei rischi, si rileva una non piena coerenza tra minacce, impatti e misure di mitigazione descritte. In più punti le categorie di rischio (riservatezza, integrità, disponibilità) risultano sovrapposte o non correttamente distinte, e alcune misure richiamate non trovano adeguata descrizione nelle sezioni precedenti. È pertanto opportuno rivedere l'analisi dei rischi secondo una logica più rigorosa e aderente agli standard metodologici, includendo anche il riferimento allo sfruttamento delle vulnerabilità informatiche come minaccia rilevante.

Fermo restando quanto sopra evidenziato, le osservazioni formulate assumono carattere migliorativo e non pregiudicano il giudizio complessivamente favorevole sull'iniziativa. Si auspica pertanto che il Titolare del trattamento tenga conto delle

raccomandazioni sopra riportate in sede di aggiornamento della documentazione, al fine di incrementare ulteriormente il livello di trasparenza, sicurezza e conformità del trattamento rispetto ai principi stabiliti dal Regolamento (UE) 2016/679.

TUTTO CIÒ PREMESSO IL DPO - esprime parere POSITIVO, fermo restando le prescrizioni sopra evidenziate.

Firma Responsabile protezione dati (DPO) Ing. Aldo Lupi

VISTO DI REGOLARITÀ DELL'ISTRUTTORIA

Il Responsabile del Procedimento, valutati, ai fini istruttori, le condizioni di ammissibilità, i requisiti di legittimazione e i presupposti per l'emanazione del provvedimento, attesta la regolarità dell'istruttoria della proposta n.ro 804 del 03/06/2026.

Visto di regolarità dell'istruttoria firmato digitalmente dal Responsabile del Procedimento HONORATI GIULIO in data 03/06/2026.

VISTO DI REGOLARITÀ TECNICA

Il Dirigente, ai sensi dell'art. 147/bis del TUEL 267/2000 e del Regolamento sui controlli interni, in ordine alla proposta n.ro 804 del 03/06/2026, esprime parere **FAVOREVOLE**.

Visto di regolarità tecnica firmato digitalmente dal Dirigente SCORRANO MARCO in data 03/06/2026.

Non rilevante sotto il profilo contabile

NOTA DI PUBBLICAZIONE N. 683

Il 04/06/2026 viene pubblicata all'Albo Pretorio la Determinazione n.ro 542 del 03/06/2026 con oggetto: **Approvazione DPIA ex art.35 Regolamento UE 679/2016 per sistema di videosorveglianza per la tutela delle postazioni di rilevamento infrazioni superamento velocità in SS714-SP2 e adeguamento determinazioni n. 266/2026-278/2026**

Resterà affissa per giorni 15 ai sensi dell'art 124 del T.U. 267/2000.

Esecutiva ai sensi delle vigenti disposizioni di legge.

Nota di pubblicazione firmata digitalmente da CAPPOLA FRANCA il 04/06/2026.