PROVINCIA DI PESCARA

SETTORE I - TECNICO

REGISTRO GENERALE N. 266 del 24/03/2026

Determina del Dirigente di Settore N. 198 del 24/03/2026
PROPOSTA N. 457 del 24/03/2026

OGGETTO: Approvazione DPIA ex art. 35 Regolamento UE 679/2016 per utilizzo telecamere finalizzate al rilievo infrazioni superamento limiti velocità su SS714 e su SP2

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 font-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 Assesment- 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."

DATO ATTO 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 il sistema di videosorveglianza provinciale finalizzato al rilievo delle infrazioni del superamento limiti di velocità con:

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, 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 al rilievo di infrazioni del superamento limiti di velocità da attivare:
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 19.03.2026 il DPO della Provincia di Pescara, ai sensi dell'art. 39 comma 1 lett. c) del GDPR, ha espresso *"Alla luce dell'analisi complessiva della DPIA trasmessa, delle osservazioni puntuali formulate nel corso dell'istruttoria e delle integrazioni suggerite, si esprime un parere complessivamente favorevole sul trattamento in oggetto, ritenendo che esso, nella sua configurazione generale, risulti coerente con le finalità istituzionali perseguite e fondato su idonea base giuridica. Permangono tuttavia alcune criticità e ambiti di miglioramento che, pur non inficiando la correttezza del trattamento, incidono sul livello di accountability documentale e sulla piena dimostrazione di conformità al quadro normativo vigente..omissis. Il parere favorevole deve pertanto intendersi subordinato all'adozione delle integrazioni e dei chiarimenti sopra richiamati, che si consiglia di recepire in una versione aggiornata della DPIA. TUTTO CIÒ PREMESSO IL DPO - esprime parere POSITIVO, fermo restando le prescrizioni sopra evidenziate"*

Preso atto delle osservazioni del DPO e cioè:
- *Sotto il profilo della **descrizione del trattamento e del perimetro normativo**, maggiore precisione e coerenza - ricondurre con esattezza le fattispecie trattate alle corrette disposizioni del Codice della Strada, evitando riferimenti a violazioni non pertinenti rispetto all'oggetto della DPIA. chiarire in modo netto il quadro giuridico applicabile, distinguendo il trattamento amministrativo connesso all'accertamento delle infrazioni – correttamente riconducibile al GDPR – da eventuali trattamenti di natura penale. - evitare sovrapposizioni normative e garantire una corretta qualificazione giuridica del trattamento;*
- *Con riferimento al **flusso dei dati e all'architettura del sistema**, migliorare il profilo descrittivo con adeguato livello di dettaglio per la catena di trattamento che intercorre tra dispositivi di rilevazione, sistemi di trasmissione e software di gestione delle sanzioni.- necessario esplicitare le modalità tecniche di trasmissione dei dati, le caratteristiche dei file generati, la gestione dei metadati, nonché l'infrastruttura sottostante (server, eventuale cloud, segmentazione della rete). Descrivere i rapporti tra i diversi fornitori coinvolti, anche sotto il profilo delle responsabilità e delle interfacce tecnologiche;*
- *In relazione alla **conservazione dei dati** permane una lacuna significativa riguardo alle modalità operative di cancellazione, in particolare sui dispositivi di rilevazione- specificare quali dati permangono localmente, per quanto tempo e con quali procedure vengano eliminati o sovrascritti per il rispetto del principio di limitazione della conservazione e della sicurezza dei dati;*

*-Per quanto concerne i **diritti degli interessati**, distinguere adeguatamente la non necessità del consenso dalla disciplina degli altri diritti previsti dagli artt. 15 e ss. del GDPR- necessario separare concettualmente i due ambiti e fornire una descrizione più strutturata delle modalità di esercizio dei diritti;.*
*-Sul piano delle **misure tecniche e organizzative**, definizione più puntuale della gestione degli accessi logici, includendo criteri di robustezza delle credenziali, politiche di scadenza e modalità di assegnazione.-la trattazione della crittografia deve essere distinta da quella relativa all'autenticazione - chiarire separatamente i meccanismi di protezione dei dati e quelli di controllo degli accessi - approfondimento tecnico-documentale in merito alla segmentazione della rete, alla localizzazione dei server, alla gestione dei backup e alle garanzie di integrità degli stessi;*
*- Necessità di una maggiore trasparenza circa la **gestione della manutenzione dei server**, specificando se essa sia interna o affidata a fornitori esterni e, in tal caso, secondo quali condizioni contrattuali. Analogamente, le misure di sicurezza fisica, incluse quelle antincendio, dovrebbero essere meglio articolate con riferimento ai diversi ambienti coinvolti (sala server, postazioni operative).*
*- Quadro più completo delle **misure di governance della protezione dei dati** quali la gestione dei data breach, la tracciabilità dei log, l'eventuale presenza di trattamenti extra UE e la gestione di archivi cartacei. Tali elementi devono essere integrati per assicurare una rappresentazione esaustiva del sistema di gestione della protezione dei dati.*
*-Con riguardo alla **valutazione dei rischi**, senza sovrapposizione e adeguata distinzione e descrizione, è 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 entro il mese di giugno 2026;

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), e i relativi allegati, tutti parte integrante e sostanziale del presente provvedimento, per il sistema di rilevazione immagini catturate attraverso l'utilizzo delle telecamere di videosorveglianza 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 entro il mese di giugno 2026;

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. **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;

6. **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;

7. **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;

8. **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.

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/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 Provincia di Pescara per le rilevazioni delle violazioni al Codice della Strada (violazione della velocità) tramite due sistemi di rilevazione composti da due dispositivi ciascuno, di cui un sistema di rilevazione della velocità media.

Titolare del trattamento dati: 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 Honorati (supporto/consulenza Maggioli Spa- Avv.Guido Paratico)
Data di creazione - aggiornamento: 06/03/2025
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. 35
Codice Privacy D. Lgs 196/2003 e s.m.i.
Codice della Strada D. Lgs 285/1992 art. 142 controllo velocità

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, passaggio con lanterna semaforica rossa, D. Lgs 285/1992, art. 142.

Valutazione: Migliorabile
Commento di valutazione: Il passaggio con il semaforo rosso è sanzionato dall'articolo 146 del Codice della Strada. Non è oggetto della presente analisi di impatto.

CONTESTO OPERATIVO:

Il sistema di rilevazione comprende l'ubicazione di due sistemi di rilevazione della velocità, di cui uno
di rilevazione della velocità media ed uno di rilevazione della velocità puntuale:

- 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.

Il controllo dell'infrazione avviene per il tramite di un'apparecchiatura automatica, senza la presenza dell'organo accertatore. Il sistema quale acquisisce un fotogramma solo in caso di accertata violazione dell'art. 142, sia con riferimento alla velocità puntuale che a quella media**, non vi è videoripresa continua e massiva, ma solo rilevazione puntuale di veicoli che superano i limiti di velocità puntuale o media**.

I sistemi sono composti da n. 6 dispositivi approvati dal Ministero delle Infrastrutture e dei Trasporti (MIT) per il rilevamento delle infrazioni ai limiti della velocità.
Il rilievo delle infrazioni ai limiti della velocità avviene attraverso sensori radar.
In caso di violazione ai limiti di velocità il sistema elabora il riconoscimento della targa con il supporto del sistema OCR integrato (Sistema di riconoscimento targa).
Dal punto di vista privacy è garantito l'offuscamento automatico di altre targhe presenti nella scena
dell'infrazione. Non è mai possibile identificare i passeggeri.

MODALITA' DI ACQUISIZIONE DELLE IMMAGINI:

L'apparato è in grado di monitorare più corsie stradali contemporaneamente come emerge dai progetti tecnici che si allegano alla DPIA. I sistemi consentono anche il rilievo dei veicoli in modalità FreeFlow però tale modalità operativa non viene utilizzata per l'accertamento del rilievo della velocità e per la contestazione.
L'apparato integra i seguenti sistemi di comunicazione:
- WEB Server: Per la configurazione e manutenzione
- Notifiche PUSH via FTP e WebServices: Notifiche real time di dati e immagini;
- FTP Server: Per l'accesso a dati e immagini salvati all'interno della memoria SSD integrata nell'apparato;
- WebServices: Per l'accesso remoto ai dati e per la supervisione remota dell'apparato.

Per ogni evento rilevato e quindi anche per il transito di ogni singolo veicolo è possibile inviare in tempo reale i dati verso uno o più server remoti attraverso web services. Il software VSP di centrale operativa è in grado di gestire la ricezione di questi messaggi in tempo reale.

I dati relativi ad ogni infrazione sono inseriti all'interno delle immagini utilizzate per documentare l'infrazione stessa. Questo processo avviene in modo completamente automatico.
Questa modalità di gestione dei dati garantisce l'autenticità dei dati stessi. Non è utilizzato il nome del file per veicolare dati dall'apparato verso il server centrale di gestione dei dati.

L'organo di Polizia Locale, il solo autorizzato (ad eccezione della società Safety 21 designata Responsabile del Trattamento dei dati) a visionare le immagini, fa un collegamento diretto dall'ufficio di polizia locale verifica che i dati di cui sopra siano correttamente acquisiti e procede con la validazione della violazione di cui il fotogramma costituisce la fonte di prova.

L'organo di polizia sempre tramite una procedura inserita nel gestionale, consulta la banca dati della Motorizzazione Civile e aggancia i dati della targa con l'intestatario al quale sarà notificato l'atto amministrativo relativo alla violazione dell'art. 142 del codice della strada (D.lgs. 285/1992).

Il programma di convalida delle infrazioni in centrale operativa contiene nella sua configurazione interna la password necessaria per la decodifica delle immagini.

Quindi l'unico modo per visualizzare un'immagine di un'infrazione è passare attraverso il programma di convalida delle infrazioni. L'accesso a questo programma richiede sempre l'autenticazione inserendo username e password. Questo consente di tracciare tutte le operazioni eseguite dall'operatore compresa la semplice visualizzazione di un'immagine.

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.

Valutazione: Migliorabile
Commento di valutazione: Si consiglia di descrivere in maniera più chiara il flusso di informazioni attraverso le componenti del sistema. Da quanto si evince, i dispositivi acquisiscono le immagini che sono trasmesse altri sistemi, per poi essere consultate dal software di gestione delle contravvenzioni. I dispositivi di rilevazione della velocità – da quanto è dato di capire – sono forniti da Safety 21, mentre il software di gestione sanzioni al CdS è di un'altra società. Sarebbe opportuno chiarire come dialogano questi sistemi, in che modo sono trasmessi i dati (se la connessione è radio Hiperlan o con trasmissione cellulare UMTS, se vi è lo scarico tramite chiavetta USB o con collegamento wifi con tablet nelle vicinanze, se le immagini sono scaricate in un unico file cifrato o sono tanti file cifrati, se i metadati si trovano in un file separato, ecc). Si consiglia inoltre di dettagliare l'architettura informatica tramite la quale sono trattati i dati (PC, server interni/esterni, ecc).

CATEGORIE DI PERSONE INTERESSATI DEL TRATTAMENTO E DATI PERSONALI TRATTATI:

I dati trattati riguardano solo i proprietari e aventi diritto dei veicoli che commettono infrazioni. **Non vengono mai trattati i dati dei passeggeri (non identificabili).**
Categorie di dati trattati:

- Dati personali comuni anagrafici:
- Dati personali comuni di contatto:
- Dati personali comuni relativi alla posizione: ora e luogo dell'infrazione
- Altre tipologie di dati: targa, modello e categoria veicolo.

PERIODO DI CONSERVAZIONE DATI E FOTOGRAMMI:

Le immagini sono conservate solo per il periodo di tempo strettamente necessario alla definizione del procedimento amministrativo: applicazione delle sanzioni, pagamento, definizione dell'eventuale contenzioso in conformità a quanto previsto dal Titolo VI del Nuovo codice della strada. Il verbale è conservato come da norme su archiviazione atti pubblici.

Al termine di tale periodo le risultanze fotografiche saranno eliminate e i dati non saranno più utilizzabili. La documentazione fotografica non viene mai inviata al domicilio dell'intestatario del veicolo unitamente al verbale di contestazione, l'intestatario, tuttavia, può visionare il fotogramma su richiesta del destinatario del verbale nel rispetto delle norme previste dalla Legge 7 agosto 1991, n. 241. **In nessun caso è consentito identificare gli occupanti** in quanto le immagini, frontali, sono sempre oscurate/pixelatura.

Valutazione: Migliorabile

Commento di valutazione: Nella descrizione manca un elemento rilevante, cioè la modalità di cancellazione dei dati sui dispositivi. Occorre specificare quali informazioni rimangono residenti sui dispositivi una volta che i dati sono trasmessi al software di gestione sanzioni al CdS e per quanto vi rimangono.

Principi Fondamentali
PROPORZIONALITÀ E NECESSITÀ

La liceità è data dall'art. 6 par. 1 del GDPR, e del GDPR, art. 5 del Dlgs 18 maggio 2018, n. 51 e art. 23, comma 1, del d.P.R. n. 15 del 2018, in quanto "il trattamento è necessario per l'esecuzione di un compito di interesse pubblico, connesso all'esercizio di istituto della polizia stradale, previsto dalla Legge, il D.Lgs 285/1992 Codice della Strada.

E' **proporzionato,** poiché le immagini riprendono solo i veicoli che commettono illecito al codice della strada, **chi non commette infrazione, non viene ripreso**. La pixelatura frontale impedisce un trattamento eccedente e solo personale di polizia locale può

accedere alle immagini. Inoltre l'ottica delle telecamere, come emerge dal progetto esecutivo, è limitata alle sole corsie su cui transitano i veicoli.

Valutazione: Migliorabile
Commento di valutazione: La violazione dei limiti di velocità accertata ai sensi dell'art. 142 del Codice della Strada, in linea generale, non rientra nel perimetro applicativo del D.Lgs. 51/2018, in quanto quest'ultimo disciplina il trattamento dei dati personali effettuato per finalità di prevenzione, indagine, accertamento e perseguimento di reati. L'eccesso di velocità, salvo ipotesi particolari in cui assuma rilievo penale (ad esempio quando si inserisce in condotte più gravi), costituisce tipicamente un illecito amministrativo e non un reato. Ne consegue che il trattamento dei dati connesso all'accertamento di tale violazione trova la propria base giuridica nel Regolamento (UE) 2016/679 (GDPR) e nelle norme nazionali di settore, piuttosto che nel regime speciale previsto per il settore penale dal D.Lgs. 51/2018. Solo laddove l'accertamento della velocità si inserisca in un'attività di polizia giudiziaria finalizzata alla repressione di un reato potrebbe astrattamente profilarsi l'applicazione di tale decreto, ma si tratterebbe di un'ipotesi eccezionale e non della regola.

MINIMIZZAZIONE DEI DATI

I dati raccolti sono esatti, aggiornati quali risultano dalla banca dati della Motorizzazione civile, adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati:
• attivazione di misure di accertamento e sanzione della violazione al Codice della Strada.
I dati raccolti ed elaborati vengono minimizzati, sono solo di coloro che commettono infrazioni, non v'è acquisizione massiva di dati, le informazioni che si utilizzano sono strettamente necessarie all'applicazione della sanzione.

MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

Gli interessati che si trovano in transito sono informati, attraverso una preventiva segnaletica stradale secondo il modello approvato dal Garante della Privacy (informativa di primo livello) come viene indicato anhe nei progetti esecutivi, ovvero nelle sue immediate vicinanze, della collocazione dell'apparecchiatura in postazione fissa, prima del raggio di azione del controllo stesso. La registrazione delle immagini **avviene solo se vi è violazione alle norme** del c.d.s come sopradetto.
La segnaletica ha un formato ed un posizionamento tale da essere chiaramente visibile, in ogni condizione di illuminazione ambientale, anche quando il sistema di rilevazione è attivo in orario notturno. Si specifica inoltre che nella sezione "privacy" 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: Accettabile
Commento di valutazione: La descrizione risulta coerente con il contesto

CONSENSO DEGLI INTERESSATI

La base giuridica del trattamento è lo svolgimento di un compito connesso all'esercizio di un pubblico interesse che, in particolare interessa la tutela della sicurezza stradale veicolare e pedonale.
Pertanto, non è richiesto il consenso dell'interessato.

Il diritto di aggiornamento, rettificazione o integrazione non è in concreto esercitabile, in riferimento alle immagini registrate data la natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte per un determinato fatto: non aver rispetto i limiti di velocità stabiliti dall'Ente proprietario della strada.

Valutazione: Migliorabile
Commento di valutazione: La descrizione e non distingue la gestione del consenso (giustamente non necessaria) dallèsercizio degli altri diritti, i quali dovrebbero essere esplicitati un paragrafo a parte).

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 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.

Valutazione: Migliorabile
Commento di valutazione: Non è chiarito a quale misura si fa riferimento; se si sta parlando de gestione degli accessi logici, sarebbe necessario chiarire le modalità di rilascio delle credenziali, qu sono i criteri per cui una password è considerata debole, la lunghezza prevista e l'eventua scadenza delle
pa

Archiviazione
L'archiviazione sugli hard disk è fissata secondo i termini di conservazione dei dati dell'Ente. Salvo divers indicazione della Provincia attualmente vengono conservati per una durata di 5 anni. Il tempo di mantenimento delle immagini e registrazioni è **per il periodo**

di tempo strettamente necessario all'applicazione delle sanzioni e alla definizione dell'eventuale contenzioso.

Valutazione: Migliorabile
Commento di valutazione: Considerato che l'acquisizione, nel software deputato alla gestione delle sanzioni al Codice della Strada, di un'immagine connessa a una violazione si inserisce nel più ampio trattamento relativo al procedimento sanzionatorio, non risulta tuttavia chiarito l'aspetto più delicato sotto il profilo della conservazione, ossia in base a quali criteri le immagini vengano cancellate dalle schede SSD installate sui dispositivi.

Minimizzazione dei dati
Nel rispetto del principio di minimizzazione dei dati, sono raccolte e memorizzate le immagini (veicolo targa parte posteriore o Targa parte anteriore con oscuramento automatico degli occupanti) solo in caso di infrazione dell'art. 142 del c.d.s decreto legislativo del 16 dicembre 1992 n. 285, senza estrapolazione di altri dati biometrici o altre categorie particolari di dati.
Sono lette in automatico i dati relativi alle targhe dei veicoli in infrazione che transitano nel raggio
d'azione del radar di cui è composta l'apparecchiatura.

Valutazione: Accettabile
Commento di valutazione: La descrizione risulta coerente con il contesto

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:MigliorabilCommentodi Valutazione:

Mentre il software per la gestione delle sanzioni al CdS, i PC e il server relativo

sono gestiti allìnterno del sistema informatico, i dispositivi sono una componente a sé stante, che necessitano di una manutenzione ad hoc. Si consiglia di menzionare espressamente se la manutenzione di dei dispositivi è gestita internamente (dalla struttura informatica dellènte) o esternamente (dal fornitore). N secondo caso, si chiede di esplicitare le condizioni di fornitura del contratto manutentivo.

Crittografia

Per proteggere i dati da accessi indesiderati è presente una cifratura di tutte le immagini e i video generati. Ogni file è inserito in un archivio zip protetto da password. Lo standard

zip supporta molti algoritmi di cifratura dei dati. Quello utilizzato dall'apparato è l'algoritmo Advanced Encryption Standard (AES).
Per i dati in transito viene utilizzato un sistema SSL.
Premesso che l'accesso alle immagini presenti sul server centrale non è possibile se non attraverso il software di convalida delle infrazioni, il fatto di avere le immagini criptate rappresenta una garanzia ulteriore che non consente la visualizzazione delle immagini se non in possesso della password usata per eseguire la cifratura delle stesse.

Il programma di convalida delle infrazioni in centrale operativa contiene nella sua configurazione interna la password necessaria per la decodifica delle immagini.
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: In questo paragrafo è menzionato, seppur marginalmente, il passaggio dati tra i dispositivi e il software di gestione delle sanzioni al CdS (non è ancora chiaro in che modo effettuata la trasmissione). La parte dell'autenticazione multifattore rientra nella gestione de accessi logici e non nelle misure di crittografia; sarebbe opportuno chiarire se detto sistema autenticazione sia applicato al
software di gestione sanzioni al CdS. Non è ancora chiarita la modalità in cui i file cifrati sor trasmessi
dai dispositivi al server (1 file cifrato per ogni immagine, un set di immagini con
cifratura ed hash, ecc).

Lotta contro il malware
L'anti malware è regolarmente installato e costantemente aggiornato.
Vulnerability assessment e penetration test: esecuzione periodica di test per identificare e risolvere tempestivamente eventuali vulnerabilità.
Aggiornamenti e patch management: monitoraggio costante e applicazione di patch di sicurezza a sistemi operativi e software

Valutazione: Accettabile
Commento di valutazione: La descrizione risulta coerente con il contesto. Si presume che i Vulnerability assessment e penetration test siano effettuati sul software di gestione sanzioni al CdS.

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: Migliorabile
Commento di valutazione: Non è chiarito se il PC e il server si trovano in una rete separata dal resto della rete della Provincia (partizionamento), che ridurrebbe fortemente i rischi di propagazione di programmi malevoli. Sarebbe opportuno esplicitare se il server sia localizzato presso la rete della Provincia o se in cloud (il dettaglio dell'autenticazione con SPID/CIE propenderebbe verso tale ipotesi, ma con le informazioni fornite non è dato di saperlo):

Backup

Backup e piani di disaster recovery: backup periodici dei dati e piani per il ripristino in caso di incidente o attacco informatico.

Valutazione: Migliorabile
Commento di valutazione: Sarebbe necessario chiarire quali misure sono adottate per garantire l'integrità dei backup (es. backup immutabile, separazione della rete su cui si effettuano i salvataggi rispetto alla rete di produzione, ecc).

Politica di tutela della privacy
Si è proceduto alla nomina del Data Protection Officer. DPO.

Valutazione: Accettabile
Commento di valutazione: L'affermazione è corretta, ma si consiglia di integrarla con le altre misura di carattere organizzativo fissate dalla Provincia (registro dei trattamenti, autorizzazione al trattamento, informative, designazione responsabili).

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.

Valutazione: Accettabile
Commento di valutazione: L'affermazione è corretta

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 2016/678, 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: L'affermazione è corretta e la descrizione è coerente.

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: L'affermazione è corretta e la descrizione è coerente, attesco che tutti i soggetti che accedono ai sistemi siano dotati di credenziali personali.

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

Valutazione: Migliorabile
Commento di valutazione: Sarebbe opportuno chiarire quali sono le misure applicate alla sala server e quali ai locali relativi alle postazioni di lavoro.
CARENZE DI FONDO SULLE MISURE ADOTTATE E DESCRITTE
Nel documento non si fa alcun riferimento a:
la presenza o meno di trattamenti effettuati al di fuori dell'Unione Europea
il rapporto con i fornitori dei dispositivi e dei sistemi di gestione delle sanzioni, che risultano un elemento chiave ma che sono appena menzionati
l'eventuale gestione di archivi cartacei
la modalità di gestione dei data breach
la tracciabilità dei log è appena menzionata

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.
Impossibilita temporanea di accesso di dati.
Impossibilita temporanea di accesso si 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, Accessi diversificati, 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?

Limitata: la gravità delle conseguenze di un ipotetico accesso non autorizzato può riguardare la visione, relativamente alle immagini riguardanti un determinato veicolo ovvero del veicolo che ha commesso l'infrazione in precise circostanze di tempo e di luogo. Non è possibile mai in nessun caso associare quell'immagine a nessuna figura umana fisica perché l'immagine con l'oscuramento pixelato non identifica mai le persone a bordo dei veicoli. È invece possibile, in via ipotetica, riscontrare passaggi di veicoli attraverso una ricerca mirata per targa ma solo in relazione ai veicoli in infrazione di cui sia stato registrato il passaggio.

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, Gestione delle politiche 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 verificazione 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. 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. La perdita del dato comporterebbe l'impossibilità di utilizzare le immagini per reprimere i reati commessi, con conseguente danno materiale e morale per l'interessato che accresce in relazione alla gravità del reato subito.

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 verificazione di una perdita dei dati. Inoltre l'adozione periodica di Vulnerability assessment e penetration test e l'esecuzione periodica di test per identificare e risolvere tempestivamente eventuali vulnerabilità riduce il rischio. La politica di memorizzazione consente un backup delle immagini anche in caso di disastro in applicazione dello specifico piano di disaster recovery. La politica di manutenzione periodica contribuisce a prevenire la probabilità di verificazione della perdita indesiderata di dati a causa di malfunzionamento degli apparati tecnici.

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.

Allegato: Regolamento per la disciplina della videosorveglianza nel territorio comunale – Progetti di installazione dei sistemi contenenti mappa e descrizione degli impianti ubicati sul territorio

Il Titolare del trattamento: Il Presidente della Provincia

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

PARERE DEL RESPONSABILE DELLA PROTEZIONE D EI DATI PERSONALI

Alla luce dell'analisi complessiva della DPIA trasmessa, delle osservazioni puntuali formulate nel corso dell'istruttoria e delle integrazioni suggerite, si esprime un parere complessivamente favorevole sul trattamento in oggetto, ritenendo che esso, nella sua configurazione generale, risulti coerente con le finalità istituzionali perseguite e fondato su idonea base giuridica. Permangono tuttavia alcune criticità e ambiti di miglioramento che, pur non inficiando la correttezza del trattamento, incidono sul livello di accountability documentale e sulla piena dimostrazione di conformità al quadro normativo vigente.

Sotto il profilo della **descrizione del trattamento e del perimetro normativo**, si rileva l'esigenza di una maggiore precisione e coerenza. In particolare, è necessario ricondurre con esattezza le fattispecie trattate alle corrette disposizioni del Codice della Strada, evitando riferimenti a violazioni non pertinenti rispetto all'oggetto della DPIA. Parimenti, occorre chiarire in modo netto il quadro giuridico applicabile, distinguendo il trattamento amministrativo connesso all'accertamento delle infrazioni – correttamente riconducibile al GDPR – da eventuali trattamenti di natura penale, che rappresentano ipotesi residuali e

non tipiche. Tale chiarimento è essenziale per evitare sovrapposizioni normative e per garantire una corretta qualificazione giuridica del trattamento.

Con riferimento al **flusso dei dati e all'architettura del sistema**, la documentazione risulta i parte carente sotto il profilo descrittivo. Non emerge con adeguato livello di dettaglio la catena di trattamento che intercorre tra dispositivi di rilevazione, sistemi di trasmissione e software di gestione delle sanzioni. È necessario esplicitare le modalità tecniche di trasmissione dei dati, le caratteristiche dei file generati, la gestione dei metadati, nonché l'infrastruttura sottostante (server, eventuale cloud, segmentazione della rete). Analoga esigenza di chiarimento riguarda i rapporti tra i diversi fornitori coinvolti, che costituiscono un elemento centrale del trattamento e devono essere pienamente descritti anche sotto il profilo delle responsabilità e delle interfacce tecnologiche.

In relazione alla **conservazione dei dati**, pur essendo correttamente individuato il principio di limitazione temporale connesso al procedimento sanzionatorio, permane una lacuna significativa riguardo alle modalità operative di cancellazione, in particolare sui dispositivi di rilevazione. È necessario specificare quali dati permangono localmente, per quanto tempo e con quali procedure vengano eliminati o sovrascritti. Tale aspetto assume rilievo determinante ai fini del rispetto del principio di limitazione della conservazione e della sicurezza dei dati.

Per quanto concerne i **diritti degli interessati**, la DPIA evidenzia correttamente la non necessità del consenso, ma non distingue adeguatamente tale profilo dalla disciplina degli altri diritti previsti dagli artt. 15 e ss. del GDPR. Si rende pertanto necessario separare concettualmente i due ambiti e fornire una descrizione più strutturata delle modalità di esercizio dei diritti, compatibilmente con la natura del trattamento e con i limiti derivanti dal procedimento amministrativo.

Sul piano delle **misure tecniche e organizzative**, il documento presenta un impianto complessivamente adeguato, ma con descrizioni spesso generiche o non pienamente coerenti. In particolare, la gestione degli accessi logici necessita di una definizione più puntuale, includendo criteri di robustezza delle credenziali, politiche di scadenza e modalità di assegnazione. Analogamente, la trattazione della crittografia deve essere distinta da quella relativa all'autenticazione, chiarendo separatamente i meccanismi di protezione dei dati e quelli di controllo degli accessi. Permangono inoltre elementi di incertezza in merito alla segmentazione della rete, alla localizzazione dei server, alla gestione dei backup e alle garanzie di integrità degli stessi, che richiedono un approfondimento tecnico- documentale.

Sempre in ambito sicurezza, si evidenzia la necessità di una maggiore trasparenza circa la **gestione della manutenzione dei server**, specificando se essa sia interna o affidata a fornitori esterni e, in tal caso, secondo quali condizioni contrattuali. Analogamente, le misure di sicurezza fisica, incluse quelle antincendio, dovrebbero essere meglio articolate con riferimento ai diversi ambienti coinvolti (sala
server, postazioni operative).

Dal punto di vista organizzativo, pur risultando presenti gli elementi fondamentali (designazioni, formazione, regolamenti), 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, l'eventuale presenza di trattamenti extra UE e la gestione di archivi cartacei. 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.

In conclusione, il trattamento oggetto della DPIA può ritenersi lecito e, in linea generale, proporzionato rispetto alle finalità perseguite. Tuttavia, le carenze evidenziate riguardano principalmente il livello di dettaglio e la qualità della documentazione, aspetti che incidono sulla capacità dell'Ente di dimostrare pienamente la conformità al GDPR secondo il principio di accountability. Il parere favorevole deve pertanto intendersi subordinato all'adozione delle integrazioni e dei chiarimenti sopra richiamati, che si consiglia di recepire in una versione aggiornata della DPIA.

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

Firma Responsabile protezione dati (DPO) Ing. Aldo Lupi

Firmato digitalmente da: ALDO LUPI
Data: 19/03/2026 14:35:32

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 457 del 24/03/2026.

Visto di regolarità dell'istruttoria firmato digitalmente dal Responsabile del Procedimento HONORATI GIULIO in data 24/03/2026.

VISTO DI REGOLARITÀ TECNICA

Il Dirigente dichiara che la sottoscrizione della presente determinazione contiene in sé l'espressione del parere favorevole di regolarità tecnica ai fini dell'avvenuto controllo preventivo, ai sensi dell'art. 147/bis del TUEL 267/2000 e del Regolamento sui controlli interni.

Pescara, lì 24/03/2026

IL DIRIGENTE
SCORRANO MARCO