PROVINCIA DI PESCARA

SETTORE I - TECNICO

REGISTRO GENERALE N. 278 del 26/03/2026

Determina del Dirigente di Settore N. 204 del 26/03/2026
PROPOSTA N. 442 del 23/03/2026

OGGETTO: Approvazione DPIA ex art. 35 Regolamento UE 679/2016 per utilizzo telecamere finalizzate al rilievo infrazioni semaforiche in località Cerratina del Comune di Pianella

Il Comandante della Polizia Provinciale, Dott. Giulio Honorati, in qualità di R.U.P del provvedimento in oggetto, giusto atto di 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"

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 semaforiche in località Cerratina del Comune di Pianella 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 semaforiche da attivare in località Cerratina di Pianella e precisamente in corrispondenza dell'intersezione tra viale S.Vincenzo e via Trieste in direzione ovest e in contrada Vicenne sud in corrispondenza dell'intersezione con via Trieste direzione est

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 "*parere complessivamente favorevole fermo restando l'opportunità di procedere alle integrazioni e ai chiarimenti indicati al fine di migliorare la completezza e la chiarezza del documento (NDR -DPIA) e di rappresentare in modo più puntuale le misure tecniche e organizzative adottate dall'amministrazione per garantire la protezione dei dati personali trattati*"

Preso atto delle indicazioni del DPO e cioè:
-*fornire maggiori dettagli sull'architettura di rete che collega i dispositivi installati sul territorio, il server centrale di gestione dei dati e le postazioni utilizzate dal personale autorizzato per la validazione delle infrazioni*
- *maggiore chiarezza sulla permanenza delle immagini nella memoria locale dei dispositivi di rilevazione*
- *criteri e modalità con cui tali dati vengono cancellati o sovrascritti una volta trasferiti nel sistema centrale o decorso il periodo di conservazione*
- *chiarezza sulle modalità di accesso ai dati conservati sul server centrale*
- *indicare se il server sia collocato in infrastruttura informatica segregata o comunque separata dalla rete ordinaria dell'amministrazione*
- *rivedere il quadro delle basi giuridiche richiamate nel documento*
- *opportunità di dedicare una specifica sezione relativa alla descrizione delle modalità di accesso degli interessati*

- descrizione più dettagliata delle modalità di gestione delle credenziali di accesso ai sistemi informatici ed eventuale implementazione di ulteriori misure di sicurezza
- eventuale integrazione sulla descrizione delle misure adottate per l'integrità e disponibilità dei dati, specificando le modalità con cui vengono effettuate le copie di sicurezza, le misure di protezione del backup e le procedure di ripristino dati in caso di incidente
- descrizione più dettagliata delle misure adottate per la protezione dei locali che ospitano le apparecchiature informatiche e le postazioni di lavoro(comprese eventuali misure di prevenzione e protezione antincendio e controllo accessi fisici)
- indicazione dei rapporti con i fornitori dei sistemi tecnologici e dei software utilizzati per la gestione delle sanzioni, di eventuale presenza di archivi cartacei collegati al trattamento delle procedure adottate per la gestione e notifica di eventuali violazioni dei dati personali(data breach) e delle modalità di registrazione e conservazione dei log di accesso ai sistemi;

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 semaforiche, 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 sinteticamente 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 semaforiche in località Cerratina del Comune di Pianella;

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 infrazioni semaforiche

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/Delibera Consiliare n. 35 del 28.11.2025), 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/**numero 2 apparecchiature AGUIA RED modello AGUIA RED-T5-5 per la rilevazione delle infrazioni semaforiche in località Cerratina di Pianella**, 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 infrazioni semaforiche;

DPIA
Informazioni sulla DPIA

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: 10/01/2026
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. 35
Codice Privacy D. Lgs 196/2003 e s.m.i.
Codice della Strada D. Lgs 285/1992 - art. 146 controllo semaforo
Regolamento provinciale "Regolamento per dispositivi di acquisizione immagini e trattamento dati" Delibera Consiliare n. 35 del 28.11.2205
Decreto Ministeriale n. 47 del 01.03.2021 di approvazione del dispositivo AGUIA Red modello AGUIA-T5-5 di accertamento infrazioni semaforiche

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. 146**.**

CONTESTO OPERATIVO:

Il controllo elettronico delle infrazioni semaforiche è identificato nei seguenti punti:

- installazione di una postazione di controllo elettronico delle infrazioni semaforiche su Viale S.Vincenzo in corrispondenza dell'intersezione con con Via Trieste in direzione Ovest, nel centro abitato di Cerratina (frazione del Comune di Pianella).
- installazione di una postazione di controllo elettronico delle infrazioni semaforiche su Contrada Vicenne Sud in corrispondenza dell'intersezione con Via Trieste in direzione Est, nel centro abitato di Cerratina (frazione del Comune di Pianella).

Il controllo dell'infrazione avviene per il tramite di un'apparecchiatura automatica, senza la presenza dell'organo accertatore, la quale acquisisce un fotogramma solo in caso di accertata violazione dell'art. 146, non vi è videoripresa continua e massiva, ma solo rilevazione puntuale di veicoli che superano l'incrocio con lanterna semaforica rossa.

Il sistema è un dispositivo approvato dal Ministero delle Infrastrutture e dei Trasporti (MIT) per il rilevamento delle infrazioni semaforiche.
Il rilievo delle infrazioni semaforiche avviene attraverso algoritmi di elaborazione delle immagini;

l'elaborazione è effettuata da vari algoritmi con anche il supporto del sistema OCR integrato (Sistema di riconoscimento targa).
Per il rilievo delle infrazioni, l'apparato valuta la posizione della targa del veicolo rispetto alle linee di arresto virtuali impostate. Nel caso siano presenti più targhe nel campo di riconoscimento dell'apparato, è garantito che la documentazione dell'infrazione risulti chiara e corretta anche in caso di infrazioni commesse da parte di più veicoli. Dal punto di vista privacy è inoltre 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 e supporta la gestione di corsie con verso di marcia opposto in modalità FreeFlow.
Le principali funzionalità dell'apparato sono:
- Rilievo infrazioni semaforiche e superamento linea di arresto;

È possibile configurare ogni corsia con funzionalità indipendenti ed è possibile anche configurare ogni corsia con modalità di funzionamento multiple (esempio rilievo infrazioni semaforiche e FreeFlow).
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.

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.
I dati dell'infrazione possono anche essere aggiunti in sovra impressione ad ogni immagine. È possibile selezionare quali dati stampare in sovra impressione attraverso l'interfaccia web di configurazione dell'apparato.
Nel fotogramma, le immagini contengono i seguenti dati:

- Targa di immatricolazione del veicolo.
- Marca – modello del veicolo ove possibile.
- Luogo, data ed ora dell'infrazione.
- Colore della lanterna semaforica

L'organo di Polizia Locale, il solo autorizzato a visionare le immagini, fa un collegamento diretto dall'ufficio di polizia locale, all'apparecchiatura con una connessione protetta su rete UMTS/HSDPA e un accesso protetto da password, 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. 146 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: Nella descrizione del sistema non è specificata l'architettura di rete dei client e dei server coinvolti.

CATEGORIE DI PERSONE INTERESSATI DEL TRATTAMENTO:

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).**

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 non sono specificati i tempi di conservazione delle immagini acquisite nella SSD card sul dispositivo. Non è inoltre chiarita la modalità di accesso ai dati riversati sul server e se il server è segregato. La descrizione funzionale risulta carente.

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.

Valutazione: Migliorabile
Commento di valutazione: Il riferimento al D.Lgs. 51/2018 non appare pertinente nel caso in esame.
La violazione dell'art. 146 del Codice della Strada (passaggio con semaforo rosso) costituisce infatti un illecito amministrativo e non un reato. L'attività di accertamento e gestione della sanzione rientra pertanto nell'ambito della polizia amministrativa stradale e non nelle attività di prevenzione, indagine o repressione di reati.
Di conseguenza, il trattamento dei dati personali connesso alla rilevazione dell'infrazione non ricade nell'ambito applicativo del D.Lgs. 51/2018, ma nel regime ordinario di protezione dei dati personali previsto dal GDPR e dal Codice Privacy. Si suggerisce quindi di eliminare il riferimento al D.Lgs. 51/2018 tra le basi normative del trattamento nella DPIA, in quanto non applicabile alla fattispecie.

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 sugli incroci nelle posizioni sopra indicate sono informati, attraverso una preventiva segnaletica stradale secondo il modello approvato dal Garante della Privacy (informativa di primo livello), 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 è confusa e non distingue la gestione del consenso (giustamente non necessaria) dall'esercizio degli altri diritti (che dovrebbero avere 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 la descrizione del servizio manutentivo deve essere dettagliata.

RISCHI
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 della gestione degli accessi logici, 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 come sopra indicato specificamente. 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: Posto che, quando un'immagine riferibile ad una sanzione viene acquisita nel software per la gestione delle sanzioni al CdS rientra nel trattamento del procedimento sanzionatorio, non viene specificato l'elemento più critico in termini di

conservazione, cioè secondo quali criteri le immagini vengono rimosse dall'SSD card localizzate 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. 146 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 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: Accettabile
Commento di valutazione: La descrizione risulta coerente con il contesto
Valutazione: Migliorabile
Commento di valutazione: Se il software per la gestione delle sanzioni al Codice della Strada, insieme ai PC e al relativo server, rientra nella gestione del sistema informatico dell'ente, i dispositivi costituiscono invece un elemento distinto che richiede interventi manutentivi specifici. È pertanto opportuno precisare espressamente se tale manutenzione sia svolta internamente, a cura della struttura informatica dell'ente, oppure affidata a soggetti esterni, come il fornitore. In quest'ultima ipotesi, si raccomanda inoltre di dettagliare le condizioni previste dal contratto di manutenzione.

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

Lotta contro il malware
L'anti malware è regolarmente installato e costantemente aggiornato.

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: 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.

Backup
I backup vengono effettuali quotidianamente con procedure automatiche centralizzate incrementali e a rotazione.

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 andrebbe accompagnata con le altre misure di tutela presenti nella Provincia (registro dei trattamenti, autorizzazione al trattamento, informative, designazione responsabili).

Gestione delle politiche di tutela della privacy
Il Titolare del trattamento ha approvato uno specifico Regolamento provinciale relativo alla protezione/trattamento dei dati personali in materia di videosorveglianza (Delibera consiliare n. 35 del 28.11.2025).

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 2016/679, 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: L'affermazione è corretta e la descrizione è coerente.

Accessi diversificati
La password di accesso è diversificata tra il personale esplicitamente autorizzato e il Responsabile al trattamento in modo da poter identificare chi accede al sistema; inoltre l'accesso avviene attraverso web browser su protocolli https protetti da cifrature.

Valutazione: Migliorabile
Commento di valutazione: Trattandosi di accessi web, si invita a ragionare sull'adozione di sistemi di autenticazione multifattore, o quantomeno sul filtraggio degli indirizzi da cui sia possibile effettuare l'accesso ai dati.

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?
Accettabile: 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 plixato 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.

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. Le misure antincendio, sebbene non soggette ad automatismi, sono proporzionate alle dimensioni del server ospitato. La politica di memorizzazione consente di salvare i dati con il backup nativo della banca dati oltre al backup completo dei nodi(utilizzo di meccanismi di replica stretched - doppia ridondanza applicativa e backup su siti differenti dal primario) garantendo una continuità operativa anche nel caso venisse meno uno dei supporti e prima che esso sia sostituito. Le misure informatiche e fisiche paiono adeguate a prevenire la perdita dei dati trattati. 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 – mappe e descrizione degli impianti ubicati sul territorio

Il Titolare del trattamento è: Il Presidente della Provincia pro-tempore
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 trattamento dei dati personali connesso all'utilizzo del sistema di rilevazione delle infrazioni semaforiche installato nel territorio provinciale, si esprime il seguente parere, con indicazione delle principali osservazioni e degli elementi suscettibili di miglioramento.
In primo luogo, appare opportuno integrare la descrizione dell'infrastruttura tecnologica utilizzata per il funzionamento del sistema di rilevazione delle infrazioni, fornendo maggiori dettagli sull'architettura di rete che collega i dispositivi installati sul territorio, il server centrale di gestione dei dati e le postazioni utilizzate dal personale autorizzato per la validazione delle infrazioni. Una descrizione più puntuale delle modalità di connessione, dei protocolli di comunicazione e delle eventuali misure di segmentazione o separazione della rete consentirebbe di rappresentare in modo più completo le misure tecniche adottate per garantire la sicurezza dei dati trattati.
Con riferimento alle politiche di conservazione dei dati e delle immagini acquisite, si ritiene opportuno specificare con maggiore chiarezza i tempi di permanenza delle immagini nella memoria locale dei dispositivi di rilevazione, nonché i criteri e le modalità con cui tali dati vengono cancellati o sovrascritti una volta trasferiti nel sistema centrale o decorso il periodo di conservazione necessario alla gestione del procedimento sanzionatorio. In tale ambito sarebbe inoltre utile chiarire le modalità di accesso ai dati conservati sul server centrale e indicare se il server sia collocato in un'infrastruttura informatica segregata o comunque separata dalla rete ordinaria dell'amministrazione, al fine di ridurre i rischi di accessi non autorizzati o di propagazione di eventuali minacce informatiche.
Sotto il profilo normativo, si suggerisce di riconsiderare il quadro delle basi giuridiche richiamate nel documento, eliminando eventuali riferimenti a normative non pertinenti rispetto alla natura del trattamento. L'attività di accertamento delle violazioni semaforiche costituisce infatti un'attività amministrativa riconducibile alla polizia stradale e, pertanto, il trattamento dei dati personali deve essere ricondotto al regime ordinario di protezione dei dati previsto dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali.
Con riferimento ai diritti degli interessati, si rileva l'opportunità di dedicare una specifica sezione alla descrizione delle modalità attraverso cui gli interessati possono esercitare i propri diritti, indicando le procedure adottate dall'amministrazione per la gestione delle richieste e i canali di contatto disponibili.
Per quanto riguarda le misure di sicurezza logica, si suggerisce di fornire una descrizione più dettagliata delle modalità di gestione delle credenziali di accesso ai sistemi informatici, specificando i criteri adottati per la creazione e la gestione delle password, le eventuali politiche di scadenza periodica delle credenziali e le procedure di rilascio degli account agli utenti autorizzati. Considerato che l'accesso ai sistemi avviene mediante interfacce web, potrebbe inoltre essere valutata l'adozione di ulteriori misure di sicurezza, quali sistemi di autenticazione multifattore o meccanismi di limitazione degli indirizzi IP dai quali è consentito l'accesso.
Ulteriori integrazioni potrebbero riguardare la descrizione delle misure adottate per garantire l'integrità e la disponibilità dei dati, in particolare con riferimento alle politiche di backup e di ripristino dei dati. In tale ambito appare opportuno specificare le modalità con cui vengono effettuate le copie di sicurezza, le eventuali misure di protezione dei backup (quali la separazione delle reti o l'adozione di sistemi di backup immutabili) e le procedure di ripristino dei dati in caso di incidente.
Dal punto di vista della sicurezza fisica delle infrastrutture, sarebbe inoltre utile fornire una descrizione più dettagliata delle misure adottate per la protezione dei locali che ospitano le apparecchiature informatiche e le postazioni di lavoro, comprese eventuali misure di prevenzione e protezione antincendio e di controllo degli accessi fisici.

Infine, si ritiene opportuno integrare il documento con alcune informazioni di carattere organizzativo e procedurale che risultano attualmente richiamate solo in misure parziale. In particolare, sarebbe utile fornire indicazioni più precise in merito ai rapporti con i fornitori dei sistemi tecnologici e dei software utilizzati per la gestione delle sanzioni, all'eventuale presenza di archivi cartacei collegati al trattamento, alle procedure adottate per la gestione e la notifica di eventuali violazioni dei dati personali (data breach) e alle modalità di registrazione e conservazione dei log di accesso ai sistemi.
Alla luce delle considerazioni sopra esposte, si esprime parere complessivamente favorevole sulla DPIA, fermo restando l'opportunità di procedere alle integrazioni e ai chiarimenti sopra indicati al fine di migliorare la completezza e la chiarezza del documento e di rappresentare in modo più puntuale le misure tecniche e organizzative adottate dall'amministrazione per garantire la protezione dei dati personali trattati.

Firma Responsabile protezione dati (DPO) Ing. Aldo Lupi

Firmato digitalmente da: ALDO LUPI
Data: 19/03/2026 14:34:29

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 442 del 23/03/2026.

Visto di regolarità dell'istruttoria firmato digitalmente dal Responsabile del Procedimento HONORATI GIULIO in data 25/03/2026.

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 26/03/2026

IL DIRIGENTE
SCORRANO MARCO