

DATA PROTECTION IMPACT ASSESSMENT

Valutazione d'impatto sistema di lettura targhe mobile

Titolare del Trattamento

COMUNE DI PALAU
Provincia di Sassari
Piazza Popoli d'Europa, 1 - 07020 Palau (SS)
Codice Fiscale: 82004530901
P.IVA: 01373510906
www.comune.palau.ss.it

SETTORE VIGILANZA - POLIZIA LOCALE

Redatto dal Responsabile del Settore Vigilanza, dr. Walter Nieddu, con la collaborazione del personale dell'Ufficio.

Data Protection Officer (D.P.O.)

Grafiche E. Gaspari Srl - privacy@gaspari.it - privacy@pec.egaspari.net

CONTESTO - Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento che viene preso in considerazione riguarda i dati personali acquisiti mediante l'utilizzo del sistema di lettura targhe mobile "Lince Traffic TIP-HK Patrol", installato sulle autovetture della Polizia Locale del Comune di Palau. Il sistema rileva automaticamente le targhe dei veicoli in transito e ne controlla lo stato consultando le banche dati istituzionali e liste personalizzate interne. Il titolare del trattamento dei dati è lo stesso Comune di Palau, il quale demanda al Responsabile del Settore Vigilanza la competenza su ogni decisione circa le modalità del trattamento e l'eventuale redazione di accordi sull'utilizzo del sistema da parte di altre Forze di Polizia statali o locali convenzionate.

Le finalità di utilizzo del sistema di lettura targhe mobile sono conformi alle funzioni istituzionali attribuite all'ente dalla Legge 7 marzo 1986, n. 65 - Legge Quadro sull'ordinamento della Polizia Municipale, dalla Legge Regionale Sardegna n. 9/2007 in materia di Polizia Locale, dallo Statuto e dai regolamenti comunali, dalla direttiva Polizia 2016/680 attuata con decreto lgs. 18 maggio 2018, n. 51, nonché dal decreto-legge n. 14 del 20 febbraio 2017 convertito in legge n. 48 del 13 aprile 2017 "disposizioni urgenti in materia di sicurezza delle città" e successive modificazioni ed integrazioni.

Quali sono le responsabilità connesse al trattamento?

Le responsabilità connesse al trattamento comprendono:

- La gestione delle attività di accesso al sistema di lettura targhe mobile
- La visualizzazione dei dati in tempo reale durante i controlli
- L'eventuale archiviazione dei dati relativi a veicoli segnalati
- La consultazione delle informazioni sui veicoli attraverso il collegamento alle banche dati
- La gestione degli allarmi generati dal sistema

Ci sono standard applicabili al trattamento?

- Provvedimento generale in materia di videosorveglianza in ambito pubblico e privato del 08 aprile 2010 del Garante della protezione dei dati personali (G.U. n. 99 del 29/04/2010);
- Circolare del Ministero dell'Interno inerente i Sistemi di videosorveglianza e relative specifiche tecniche per i Comuni del 02 marzo 2012 e successive indicazioni;
- Regolamento UE Generale sulla Protezione dei Dati 2016/679 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" (anche "RGPD/GDPR");
- Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali" come modificato e integrato dal D.Lgs 101/2018;
- Allegato 1 al provvedimento n. 467 dell'11 ottobre 2018, pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018, inerente all'elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto del Garante della protezione dei dati personali;
- Direttiva UE 2016/680 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", recepita con il D.lgs. 51/2018;
- DPR del 15 gennaio 2018, n. 15, recante "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";
- Decreto-legge 20 febbraio 2017, n. 14, convertito, con modificazioni, dalla legge 18 aprile 2017, n. 48, recante "Disposizioni urgenti in materia di sicurezza delle città" e successive

modificazioni ed integrazioni del D.L. 14.06.19 n. 53 convertito con modifiche con L. 8 agosto 2019 n. 77;

- Linee guida 03/2019 v.2 del 29 gennaio 2020 pubblicate dall'EDPB, inerenti al trattamento di dati personali attraverso dispositivi video;
- Le regole per installare telecamere del 05 dicembre 2020, il vademecum e le FAQ in materia di videosorveglianza del 03 dicembre 2020 del Garante della protezione dei dati personali.

CONTESTO - Dati, processi e risorse di supporto

Quali sono i dati trattati?

Attraverso il sistema di lettura targhe mobile "Lince Traffic TIP-HK Patrol" vengono rilevati e trattati i seguenti dati:

- Targhe dei veicoli in transito lungo le vie percorse dalle autovetture della Polizia Locale
- Fotografia del veicolo con dettaglio targa
- Data, ora e coordinate GPS del rilevamento
- Tipologia di allarme riscontrato (veicolo non assicurato, non revisionato, rubato, segnalato)
- Geolocalizzazione attraverso coordinate e mappa
- Classe ambientale di emissione (Euro) del veicolo

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Il sistema di lettura targhe è attivo esclusivamente durante i turni di servizio degli operatori di Polizia Locale e quando il veicolo è in movimento per attività istituzionali.

Le targhe vengono lette automaticamente dal sistema OCR che le confronta in tempo reale con:

- Banche dati istituzionali e liste personalizzate interne e Nazionali
- Black List personalizzate per identificare veicoli sospetti

In caso di riscontro positivo, l'operatore viene allertato da un allarme acustico e visivo. Il sistema associa automaticamente:

- Fotografia del veicolo con dettaglio targa
- Tipologia di allarme riscontrato
- Geolocalizzazione attraverso coordinate e mappa

I dati relativi ai veicoli non segnalati vengono automaticamente cancellati dal sistema entro 7 giorni.

I dati relativi ai veicoli oggetto di segnalazione possono essere conservati:

- Per attività di Polizia Giudiziaria: fino a sei mesi, salvo diverse disposizioni dell'A.G.
- Per illeciti amministrativi: fino a 5 anni o comunque fino al termine del procedimento

Le informazioni possono essere visualizzate in tempo reale su Tablet PC e/o Smartphone attraverso l'APP dedicata, nonché dalla centrale operativa tramite PC.

Quali sono le risorse di supporto ai dati?

Il personale autorizzato al trattamento dei dati viene individuato mediante apposito atto predisposto dal Responsabile del Settore Vigilanza e suddiviso in:

- **Incaricato del trattamento:** personale al quale è consentito l'accesso al sistema di lettura targhe mobile durante il servizio;
- **Responsabile del trattamento:** soggetto esterno all'organizzazione del Titolare che tratta dati per attività di manutenzione dell'impianto o in virtù di una eventuale convenzione (altro soggetto pubblico).

L'attivazione e disattivazione del sistema durante il servizio deve essere registrata su apposito registro, contenente:

- Data e ora di attivazione/disattivazione
- Identificativo del veicolo utilizzato
- Nominativo dell'operatore
- Zone percorse durante il servizio

Ogni operatore deve essere dotato delle proprie credenziali di accesso e relativa password per l'utilizzo del sistema.

PRINCIPI FONDAMENTALI - Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Gli scopi del trattamento dei dati sono specifici e legittimi in quanto finalizzati a:

- Prevenzione e repressione di reati
- Controllo del rispetto delle norme sulla circolazione stradale (assicurazione, revisione)
- Recupero veicoli rubati
- Controllo veicoli segnalati per motivi di sicurezza urbana
- Accertamento violazioni amministrative

Il sistema è chiaramente identificabile attraverso:

- Cartelli informativi agli ingressi della città
- Adesivi sui veicoli della Polizia Locale
- Segnalazione luminosa quando il sistema è attivo
- QR-Code per accesso all'informativa estesa

Quali sono le basi legali che rendono lecito il trattamento?

Il trattamento dei dati è effettuato nel pubblico interesse, per lo svolgimento di funzioni istituzionali di polizia locale e sicurezza urbana.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. minimizzazione) di cui all'art. 5 par. 1, lett. c) del GDPR, il sistema di lettura targhe mobile è configurato per:

- Rilevare esclusivamente le targhe dei veicoli in transito
- Cancellare automaticamente i dati dei veicoli non segnalati entro 7 giorni
- Conservare solo i dati strettamente necessari per le finalità istituzionali

I dati sono esatti e aggiornati?

I dati relativi ai veicoli sono aggiornati in tempo reale attraverso:

- Collegamento alle banche dati nazionali
- Aggiornamento costante delle Black List
- Sincronizzazione oraria del sistema (GMT +1 o GMT +2 per ora legale)

Qual è il periodo di conservazione dei dati?

- Veicoli non segnalati: cancellazione automatica entro 7 giorni
- Attività di Polizia Giudiziaria: fino a 6 mesi, salvo diverse disposizioni dell'A.G.
- Illeciti amministrativi: fino a 5 anni o comunque fino al termine del procedimento
- Veicoli rubati recuperati: fino a 90 giorni per rilevanza penale, salvo diverse disposizioni dell'A.G.

PRINCIPI FONDAMENTALI - Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati sono informati mediante:

1. Informativa "diffusa" sul territorio:

- Cartelli agli ingressi della città con dicitura: "Il Comune utilizza sistemi mobili di lettura targhe, installati sulle autovetture della polizia locale, per sicurezza urbana"
 - QR-Code sui cartelli che rimanda all'informativa estesa
2. **Identificazione visibile del veicolo:**
- Adesivi/scritte sul veicolo: "VEICOLO DOTATO DI SISTEMA LETTURA TARGHE"
 - QR-Code sul veicolo che rimanda all'informativa estesa
 - Segnalazione luminosa quando il sistema è attivo
3. **Pubblicazione online:**
- Informativa estesa sul sito web istituzionale del Comune

Come si ottiene il consenso degli interessati?

Essendo il sistema utilizzato per finalità di pubblico interesse e sicurezza urbana, con monitoraggio degli spazi pubblici, non è prevista la richiesta del consenso degli interessati.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

L'istanza per l'esercizio dei propri diritti da parte dell'interessato è presentata al Titolare del trattamento o al DPO (Grafiche E. Gaspari Srl - privacy@gaspari.it).

Nel caso specifico, potranno essere rilasciati all'interessato:

- I dati relativi al proprio veicolo se oggetto di rilevamento e conservazione
- Le informazioni sul trattamento effettuato
- La conferma dell'avvenuta cancellazione dei dati

Al fine di salvaguardare i diritti e le libertà altrui (art. 15 par. 4 del GDPR), non verranno forniti dati relativi ad altri veicoli o persone.

In caso di esito negativo all'istanza dell'interessato, quest'ultimo potrà rivolgersi al Garante della protezione dei dati personali per il reclamo, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

La cancellazione dei dati non oggetto di segnalazione avviene automaticamente entro 7 giorni. Per i dati conservati per fini istituzionali, gli interessati possono contattare:

- Il Titolare del trattamento (Comune di Palau)
- Il DPO: Grafiche E. Gaspari Srl - privacy@gaspari.it - privacy@pec.egaspari.net

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

I dati che vengono conservati riguardano determinati fatti illeciti che comportano l'irrogazione di una sanzione - amministrativa o penale -, pertanto la natura giuridica stessa del dato, quale fonte di prova, ne limita già l'utilizzo.

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

Il Responsabile del settore vigilanza, che supervisiona il sistema, abilita mediante credenziali il personale interno incaricato al trattamento dei dati e stipula accordi e convenzioni con altre forze di polizia per l'eventuale accesso ai dati, rilasciando le credenziali di accesso esclusivamente al personale indicato dall'amministrazione richiedente.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I server e i dispositivi di archiviazione sono collocati all'interno dell'Unione europea. Non è previsto alcun trasferimento di dati al di fuori dell'UE.

RISCHI - Misure esistenti o pianificate

Controllo degli accessi logici

- Ogni operatore autorizzato è dotato di username e password personale di accesso
- Le credenziali sono modificate periodicamente
- Le credenziali vengono disattivate in caso di cessazione del servizio o perdita della qualifica
- Registro dettagliato degli operatori autorizzati, costantemente aggiornato
- Sistema di tracciabilità degli accessi e delle operazioni effettuate

Archiviazione

- I dati sono archiviati in formato digitale su server protetto
- Accesso ai dati archiviati solo tramite credenziali autorizzate
- Cancellazione automatica dei dati non rilevanti dopo 7 giorni
- Backup periodici dei dati, nei limiti delle regole di conservazione

Incaricati e Responsabili del trattamento

- Nomina formale del personale incaricato del trattamento
- Definizione chiara di ruoli e responsabilità
- Accordi formalizzati con altre forze di polizia per eventuale accesso ai dati
- Contratto con la società fornitrice del sistema per assistenza e manutenzione

Controllo degli accessi fisici

- I dispositivi mobili (tablet/PC) sono custoditi presso il Comando di Polizia Locale quando non in uso.
- Accesso al Comando limitato al personale autorizzato
- I veicoli dotati del sistema sono parcheggiati in area protetta
- Rimozione delle apparecchiature dai veicoli al termine del servizio, se tecnicamente possibile

Sicurezza dell'hardware

- Dispositivi protetti da password di accesso
- Sistemi antivirus e antimalware aggiornati
- Crittografia dei dati archiviati
- Protezione fisica dei dispositivi contro furto o danneggiamento

Politica di tutela della privacy

- Il Responsabile del Settore Vigilanza supervisiona il rispetto delle policy
- Formazione specifica del personale sul trattamento dati
- Registro degli accessi e delle operazioni
- Audit periodici sull'utilizzo del sistema

Gestione del personale

- Formazione iniziale e aggiornamento periodico sul GDPR
- Istruzioni operative dettagliate per l'uso del sistema
- Responsabilizzazione del personale sulle conseguenze di un uso improprio
- Verifica periodica del rispetto delle procedure

Vigilanza sulla protezione dei dati

- Invio del DPIA al DPO per parere preventivo
- Aggiornamento annuale del DPIA
- Monitoraggio continuo dell'efficacia delle misure di sicurezza
- Collaborazione costante con il DPO per eventuali criticità

Anonimizzazione

I dati relativi alle targhe non vengono pubblicati né diffusi, pertanto non è necessaria l'anonimizzazione. In caso di utilizzo per finalità statistiche, i dati vengono aggregati e resi anonimi.

Vulnerabilità

- Sistema di protezione perimetrale del software
- Aggiornamenti di sicurezza installati tempestivamente
- Monitoraggio delle vulnerabilità note
- Piano di disaster recovery

Gestione dei terzi che accedono ai dati

- La società fornitrice del sistema e servizio di manutenzione accede solo per finalità di manutenzione, ed è formalmente nominata "Responsabile del Trattamento"
- Accesso remoto solo previa autorizzazione e sotto supervisione
- Tracciabilità di tutti gli accessi effettuati da terzi

Tracciabilità

Il sistema "Lince Traffic TIP-HK Patrol" registra automaticamente:

- Tutti gli accessi al sistema
- Le operazioni effettuate
- I veicoli controllati
- Gli allarmi generati
- Le estrazioni di dati effettuate

Backup

- Backup automatico dei dati rilevanti
- Conservazione dei backup in luogo sicuro
- Test periodici di ripristino
- Retention policy definita per i backup

Crittografia

- Crittografia dei dati in transito tra dispositivo mobile e server
- Crittografia dei dati archiviati
- Protocolli sicuri per la trasmissione dati
- Gestione sicura delle chiavi di crittografia

RISCHI - Accesso illegittimo ai dati

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

- Divulgazione non autorizzata di dati relativi agli spostamenti dei veicoli
- Possibile profilazione illegittima degli interessati
- Violazione della riservatezza degli spostamenti
- Utilizzo improprio dei dati per finalità non istituzionali

Quali sono le principali minacce che potrebbero concretizzare il rischio?

- Accesso non autorizzato ai dispositivi mobili
- Furto o smarrimento di tablet/smartphone
- Attacchi informatici al sistema
- Abuso d'ufficio da parte del personale

Quali sono le fonti di rischio?

- Fonti interne: personale non adeguatamente formato o malintenzionato
- Fonti esterne: criminali informatici, furti di dispositivi
- Vulnerabilità tecniche del sistema

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

- Controllo degli accessi logici con credenziali personali
- Crittografia dei dati
- Formazione del personale
- Tracciabilità delle operazioni
- Controllo degli accessi fisici ai dispositivi

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

La gravità del rischio è valutata come ELEVATO. L'accesso non autorizzato a un sistema di lettura targhe mobile potrebbe consentire la tracciatura sistematica degli spostamenti dei cittadini, con conseguente violazione grave della loro privacy e libertà di circolazione. I dati potrebbero essere utilizzati per profilazione, stalking, ricatti o altre attività illecite con impatti rilevanti sulla vita privata degli interessati.

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

La probabilità è valutata come TRASCURABILE, considerando:

- Il personale autorizzato ha qualifica di Agente/Ufficiale di P.G.
- I dispositivi sono protetti da multiple misure di sicurezza
- La cancellazione automatica dei dati non rilevanti dopo 7 giorni
- Il sistema di audit e tracciabilità

RISCHI - Modifiche indesiderate dei dati

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

- Alterazione dei dati probatori in procedimenti penali/amministrativi
- Cancellazione indebita di prove
- Inserimento di false segnalazioni
- Compromissione dell'affidabilità del sistema

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

- Manomissione del sistema da parte di personale interno
- Attacchi informatici mirati
- Malfunzionamenti del software
- Errori operativi

Quali sono le fonti di rischio?

- Personale interno non adeguatamente formato
- Vulnerabilità del software
- Attacchi esterni
- Errori procedurali

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

- Sistema di tracciabilità completa delle operazioni
- Backup periodici dei dati
- Controllo degli accessi con diversi livelli di autorizzazione
- Impossibilità di modifica dei dati acquisiti automaticamente
- Registro delle operazioni non modificabile

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

La gravità del rischio è valutata come ELEVATA. La modifica non autorizzata dei dati potrebbe compromettere l'integrità delle prove in procedimenti penali o amministrativi, con conseguenze gravi per gli interessati: condanne ingiuste, sanzioni illegittime, impossibilità di difendersi in giudizio. L'alterazione dei dati potrebbe anche portare a false segnalazioni di veicoli rubati o non in regola, causando fermi illegittimi e violazioni dei diritti fondamentali.

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

TRASCURABILE. La struttura del sistema e i controlli implementati rendono estremamente difficile la modifica non autorizzata dei dati.

RISCHI - Perdita di dati

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

- Perdita di prove in procedimenti penali o amministrativi
- Impossibilità di dimostrare la legittimità dei controlli effettuati
- Compromissione di indagini in corso
- Perdita di dati statistici per la sicurezza urbana

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

- Guasto hardware dei dispositivi
- Cancellazione accidentale dei dati
- Furto o danneggiamento dei dispositivi
- Disaster (incendio, allagamento) presso il Comando

Quali sono le fonti di rischio?

- Obsolescenza o guasto delle apparecchiature
- Eventi naturali o accidentali
- Errore umano
- Atti dolosi (furto, sabotaggio)

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

- Sistema di backup automatico
- Ridondanza dei sistemi di archiviazione
- Procedure di disaster recovery
- Manutenzione preventiva delle apparecchiature
- Formazione del personale sulle procedure di salvataggio

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

LIMITATA. I sistemi di backup e le procedure di recovery limitano significativamente l'impatto di eventuali perdite di dati.

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

TRASCURABILE. Le misure preventive e i sistemi di backup rendono molto improbabile la perdita definitiva di dati rilevanti.

RISCHI - Panoramica dei rischi

Tipo di Rischio	Gravità	Probabilità	Livello Complessivo
Accesso illegittimo ai dati	Elevata	Trascurabile	MEDIO
Modifiche indesiderate dei dati	Elevata	Trascurabile	MEDIO
Perdita di dati	Limitata	Trascurabile	BASSO

CONCLUSIONI

Il sistema di lettura targhe mobile "Lince Traffic TIP-HK Patrol" del Comune di Palau presenta un livello di rischio complessivamente MEDIO per i diritti e le libertà degli interessati, mitigato dalle misure tecniche e organizzative implementate.

Le misure di informativa adottate (cartellonistica, adesivi sui veicoli, QR-Code) garantiscono la trasparenza del trattamento nel rispetto del principio di accountability del GDPR.

Si raccomanda:

- Aggiornamento della presente DPIA in caso di modifiche al sistema
- Formazione continua del personale
- Verifica periodica dell'efficacia delle misure di sicurezza
- Mantenimento del dialogo con il DPO per eventuali criticità emergenti

Data di redazione: 09/07/2025

Il Titolare del Trattamento
Rappresentato dal Responsabile dell'Area Polizia Locale
Walter Nieddu

**PARERE DEL DATA PROTECTION OFFICER ai sensi dell'art. 39, par. 1, lett. c) del
Regolamento UE 2016/679**

Oggetto: Valutazione d'impatto sulla protezione dei dati (DPIA) relativa al sistema di lettura targhe mobile "Lince Traffic TIP-HK Patrol" del Comune di Palau

Data: _____

DPO: Grafiche E. Gaspari Srl **Contatti:** privacy@gaspari.it - privacy@pec.egaspari.net

PREMESSA

Il sottoscritto DPO, esaminata la Valutazione d'Impatto sulla Protezione dei Dati (DPIA) relativa al sistema di lettura targhe mobile "Lince Traffic TIP-HK Patrol" che il Comune di Palau intende implementare sui veicoli della Polizia Locale, esprime il seguente parere ai sensi dell'art. 35, par. 2 del GDPR e dell'art. 39, par. 1, lett. c) del medesimo Regolamento.

ANALISI DEL TRATTAMENTO

La DPIA sottoposta all'attenzione dello scrivente descrive un trattamento che, per sua natura, ambito di applicazione e finalità, presenta **rischi elevati** per i diritti e le libertà delle persone fisiche, come correttamente evidenziato nella valutazione dei rischi. In particolare:

1. **Sorveglianza sistematica su larga scala:** Il sistema consente la lettura automatica delle targhe di tutti i veicoli in transito nelle aree percorse dalle pattuglie
2. **Trattamento di dati sensibili:** Localizzazione e movimenti dei cittadini attraverso i loro veicoli
3. **Possibili effetti sulla libertà di circolazione:** Il monitoraggio potrebbe generare effetti dissuasivi sulla libera circolazione
4. **Rischio di profilazione:** I dati raccolti potrebbero consentire la ricostruzione di abitudini e spostamenti

VALUTAZIONE COMPLESSIVA

Nonostante i rischi intrinseci elevati del trattamento, il parere dello scrivente DPO è **FAVOREVOLE CON RACCOMANDAZIONI**, considerando che:

- ✓ Le finalità del trattamento sono legittime e proporzionate (sicurezza urbana, prevenzione reati, controllo circolazione stradale)
- ✓ La base giuridica è solida (esecuzione di compiti di interesse pubblico)
- ✓ Le misure di sicurezza tecniche e organizzative descritte sono adeguate
- ✓ Il sistema informativo adottato garantisce trasparenza verso i cittadini
- ✓ I tempi di conservazione sono proporzionati (7 giorni per dati non rilevanti)
- ✓ È prevista la nomina formale del fornitore come Responsabile del Trattamento ex art. 28 GDPR

RACCOMANDAZIONI PER IL MIGLIORAMENTO

Al fine di rafforzare ulteriormente il livello di protezione dei dati personali, si suggeriscono misure aggiuntive che potrebbero essere in futuro implementate:

1. Misure Tecniche

- **Segregazione dei dati:** Implementare un sistema di accesso differenziato che limiti la visualizzazione dei dati sensibili (GPS, orari) solo al personale strettamente necessario
- **Cifratura end-to-end:** Verificare che la trasmissione dati tra dispositivi mobili e server centrale utilizzi protocolli di cifratura robusti (minimo TLS 1.2)
- **Penetration test periodici:** Prevedere test di vulnerabilità sul sistema

2. Misure Organizzative

- **Formazione rafforzata:** Oltre alla formazione GDPR generale, prevedere:
 - Sessioni specifiche sul sistema di lettura targhe
 - Aggiornamenti in caso di modifiche procedurali
- **Audit interni:** Pianificare verifiche su:
 - Corretto utilizzo del sistema
 - Rispetto dei tempi di cancellazione
 - Gestione delle credenziali

3. Accountability e Governance

- **Procedura di data breach specifica:** Definire un protocollo specifico per gestire eventuali violazioni relative a questo sistema
- **Revisione periodica delle Black List:** Stabilire criteri oggettivi e documentati per l'inserimento/rimozione di targhe dalle liste personalizzate

4. Trasparenza Rafforzata

- **FAQ dedicate sul sito web:** Creare una sezione specifica con domande frequenti sul sistema
- **Comunicazione proattiva:** Considerare una campagna informativa sul funzionamento del sistema
- **Registro pubblico delle zone monitorate:** Pubblicare periodicamente le aree maggiormente interessate dal controllo (in forma aggregata)

MONITORAGGIO E AGGIORNAMENTO

Si raccomanda di:

- Aggiornare la DPIA in caso di modifiche significative al sistema
- Monitorare l'evoluzione normativa e giurisprudenziale in materia
- Valutare periodicamente l'efficacia delle misure implementate

DISPONIBILITÀ AL CONFRONTO

Il sottoscritto DPO resta a completa disposizione per:

- Chiarimenti interpretativi sulla normativa privacy
- Supporto nell'implementazione delle raccomandazioni
- Gestione di situazioni critiche o dubbi operativi

Si invita il Titolare del trattamento a non esitare nel contattare lo scrivente DPO per qualsiasi dubbio o incertezza nell'applicazione delle misure di protezione dati, anche attraverso confronti informali prima di procedere con modifiche al sistema o alle procedure.

CONCLUSIONI

Il sistema di lettura targhe mobile, se implementato secondo quanto descritto nella DPIA e integrato con le raccomandazioni sopra indicate, può rappresentare un valido strumento per le finalità di sicurezza urbana nel rispetto dei principi del GDPR.

L'approccio privacy by design adottato e le misure di trasparenza previste dimostrano l'impegno del Comune di Palau verso la protezione dei dati personali dei cittadini.

Si esprime pertanto **parere favorevole** all'implementazione del sistema, subordinatamente all'adozione delle misure raccomandate e al mantenimento di un dialogo costante con il DPO per la gestione di eventuali criticità emergenti.

Il presente parere viene reso ai sensi e per gli effetti dell'art. 35, par. 2 del GDPR.

Il Data Protection Officer
Grafiche E. Gaspari Srl

Firma: _____