

Anteprima

INFORMAZIONI GENERALI



modifica pia

100%

Anteprima

Modifica : Comune di Montalcino
Stato : Validata
Valutazione : Marcucci Giulio
Validazione : Team DPO

Validazione

Mappatura dei rischi

Gravità del rischio



- **Misure pianificate o esistenti**
- **Con le misure correttive implementate**
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

Probabilità del rischio

23/06/26

Validazione

Piano d'azione

Panoramica

Principi fondamentali

Finalità
Basi legali
Adeguatezza dei dati
Esattezza dei dati
Periodo di conservazione
Informativa
Raccolta del consenso
Diritto di accesso e diritto alla portabilità dei dati
Diritto di rettifica e diritto di cancellazione
Diritto di limitazione e diritto di opposizione
Responsabili del trattamento
Trasferimenti di dati

Misure esistenti o pianificate

Crittografia
Minimizzazione dei dati
Controllo degli accessi fisici
Protezione contro fonti di rischio non umane
Controllo degli accessi logici

Rischi

Accesso illegittimo ai dati
Modifiche indesiderate dei dati
Perdita di dati

Misure Migliorabili

Misure Accettabili

Principi fondamentali

Nessun piano d'azione registrato.

Misure esistenti o pianificate

Nessun piano d'azione registrato.

Rischi

Nessun piano d'azione registrato.

Validazione

Opinioni del DPO/RPD e degli interessati

Nome del DPO/RPD

Il Team DPO

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

Il Team DPO ha preso visione della DPIA elaborata il 23/06/2026 relativa al trattamento in oggetto e la suddetta Valutazione analizza in modo esaustivo la natura, le finalità e i tempi di conservazione del trattamento. A fronte delle misure di sicurezza previste il rischio residuo è limitato ed il trattamento

può procedere. In data 03/07/2026 il Team DPO valida la suddetta Valutazione d'Impatto.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Il Titolare non ritiene che sia necessario raccogliere il parere per questo trattamento oggetto della Valutazione d'Impatto.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Trattamento dati personali raccolti tramite sistemi di videosorveglianza mobile all'interno del Comune di Montalcino. L'uso di impianti di videosorveglianza mobile è strumento indispensabile per la lotta all'abbandono di rifiuti.

Quali sono le responsabilità connesse al trattamento?

Titolare (Ente), Responsabile del Trattamento (Comandante PM) e addetti al trattamento (Personale del Comando di Polizia Locale o altri soggetti eventualmente individuati, per sole motivazioni di assistenza o manutentive).

Ci sono standard applicabili al trattamento?

Il trattamento viene svolto per le esclusive finalità in precedenza riportate in ottemperanza a quanto stabilito dal regolamento per la disciplina ed utilizzo degli impianti di videosorveglianza; GDPR, poi il codice della Privacy e le Linee guida del Garante.

Valutazione : Accettabile

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati trattati sono principalmente video ed immagini di persone o veicoli, con comportamenti e movimenti.

I destinatori sono la Polizia Giudiziaria, le autorità di PG e PS e la Procura della Repubblica.

Personae che possono accedervi: Responsabile del trattamento, altri responsabili del trattamento e addetti/incaricati nominati, per soli motivi manutentivi e di assistenza.

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

Raccolta, Registrazione, Utilizzo, Condivisione, Conservazione, Estrazione, Consultazione, Comunicazione mediante trasmissione, Limitazione e Cancellazione o Distruzione.

Periodo conservazione limitato allo stretto necessario e comunque come fissato dalla normativa di settore, salvo speciali esigenze di ulteriore conservazione ad es. specifiche richieste investigative dell'autorità giudiziaria o della polizia giudiziaria.

Quali sono le risorse di supporto ai dati?

Tutti i dati video vengono scritti sulla microSD interna utilizzando crittografia avanzata AES-256,

impedendo la lettura da parte di soggetti non autorizzati anche in caso di accesso fisico al dispositivo. La chiave crittografica è univoca per ogni dispositivo e non è accessibile dall'esterno. Il dispositivo è dotato di una gabbia in acciaio inox, doppio lucchetto e catena antisabotaggio. La microSD non è accessibile dall'utente, che può interagire con il sistema solo tramite interfaccia software sicura. Per ridurre l'inquadratura di zone non rilevanti o sensibili, si utilizzano ottiche strette (non grandangolari) e si possono applicare maschere di privacy su aree specifiche, che verranno oscurate e non registrate. Tutte le comunicazioni tra client e dispositivo avvengono tramite connessione end-to-end crittografata AES-256. I log sono sempre attivi e consultabili.

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Scopi del trattamento sono la prevenzione di illeciti ambientali con riferimento particolare al contrasto dell'abbandono dei rifiuti.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Regolamento Generale sulla Protezione dei Dati GDPR 2016/679 Direttiva UE 2016/680.
DPR n. 15 del 15/01/2018 e D. Lgs. n. 196 del 30/06/2003 come modificato dal D. lgs. n. 101 del 10/08/2018, D.Lgs. n. 51 del 18/05/2018, Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza dell'8 aprile 2010, Decreto-legge 20 febbraio 2017, n. 14 convertito con modificazioni dalla legge 18 aprile 2017 n. 48, Decreto-Legge 23 febbraio 2009, n. 11 convertito con modificazioni nella legge 23 aprile 2009 n. 38, Direttiva Ministeriale n. 300-A-5620-17-144-5-20-3 del luglio 2017, Legge 147/2025, TUA;

Valutazione : Accettabile

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

I dati raccolti sono strettamente necessari per le attività istituzionali.
Le telecamere riprendono solo aree pubbliche o di interesse pubblico a rischio e non sono dotate di identificazioni biometriche avanzate. Non vengono raccolti dati audio. I sistemi utilizzati sono configurati per ridurre al minimo l'utilizzazione di dati personali e identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi od opportune modalità che permettono di identificare l'interessato solo in caso di necessità. E' infatti possibile visualizzare solamente i frammenti di video sospetti.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

I dati sono periodicamente verificati ed aggiornati dagli operatori incaricati. I sistemi sono estremamente affidabili, vengono effettuati periodicamente aggiornamenti e manutenzioni. Personale della Polizia Locale controlla periodicamente il funzionamento delle telecamere e l'allineamento temporale.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

I dati vengono conservati al massimo per 24 ore, salvo speciali esigenze di ulteriore conservazione ad es. specifiche richieste investigative dell'Autorità Giudiziaria o della Polizia Giudiziaria.

Valutazione : Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati sono informati della presenza di fototrappole attraverso l'informativa di I livello (cartellonistica) posizionata nelle vicinanze alle postazioni e quella di II livello pubblicata all'interno del sito istituzionale del Comune di Montalcino.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Il trattamento di dati personali da parte di soggetti pubblici è lecito allorquando è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento in ottemperanza al disposto di cui all'art. 5 par. 1 lett. a) e all'art. 6 par. 1 lett. e) del GDPR. La videosorveglianza mobile pertanto è consentita senza necessità di consenso da parte degli interessati.

Valutazione : Accettabile

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

In ossequio alle disposizioni di cui agli artt. 15 e ss. del GDPR gli interessati potranno esercitare i propri diritti su presentazione di apposita istanza da presentare al Responsabile della Protezione dei dati dell'Ente ai sensi dell'art. 38 par. 4 del GDPR (i cui dati di contatto sono disponibile sulla home page del sito istituzionale dell'Ente nella sezione "\\\"Privacy\\\"") ovvero al Responsabile del trattamento dei dati individuato nel Comandante della Polizia Locale. L'informativa è disponibile sul sito istituzionale del Comune di Montalcino.

Valutazione : Accettabile

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

In ossequio alle disposizioni di cui agli artt. 15 e ss. del GDPR gli interessati potranno esercitare i propri diritti su presentazione di apposita istanza da presentare al Responsabile della Protezione dei dati dell'Ente ai sensi dell'art. 38 par. 4 del GDPR (i cui dati di contatto sono disponibile sulla home page del sito istituzionale dell'Ente nella sezione "\\\"Privacy\\\"") ovvero al Responsabile del trattamento dei dati individuato nel Comandante della Polizia Locale.

Valutazione : Accettabile

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

In ossequio alle disposizioni di cui agli artt. 15 e ss. del GDPR gli interessati potranno esercitare i propri diritti su presentazione di apposita istanza da presentare al Responsabile della Protezione dei

dati dell'Ente ai sensi dell'art. 38 par. 4 del GDPR (i cui dati di contatto sono disponibile sulla home page del sito istituzionale dell'Ente nella sezione "\\\"Privacy\\\"") ovvero al Responsabile del trattamento dei dati individuato nel Comandante della Polizia Locale.

Valutazione : Accettabile

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

I dati possono essere conosciuti dai responsabili del trattamento, individuati per iscritto con atto di nomina ed ai quali sono state date specifiche istruzioni scritte.

Le immagini sono visionate e trattate esclusivamente da personale appartenente al Comando di Polizia Locale del Comune di Montalcino in possesso della qualifica di APS e APG/UPG.

Valutazione : Accettabile

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

Non ricorre tale ipotesi

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Crittografia

Registrazioni crittografate AES 256-bit Tutti i dati video vengono scritti sulla microSD interna utilizzando crittografia avanzata AES-256, impedendo la lettura da parte di soggetti non autorizzati anche in caso di accesso fisico al dispositivo. La chiave crittografica è univoca per ogni dispositivo e non è accessibile dall'esterno. Accessi sicuri (locale e remoto)

Locale: connessione Wi-Fi 2.4 GHz protetta WPA2-PSK con password sicura e accesso filtrato per MAC address.

Remoto (2 modalità):

1. VPN tra router e client.
2. IP statico con accesso diretto configurabile, porte dedicate e logging.

Protezione da accessi non autorizzati

- Blocco temporaneo di 5 minuti dopo tentativi falliti.
- Notifica e-mail in caso di più accessi errati.
- Logging attivo: accessi tracciati per orario, IP, credenziali.

Connessioni criptate e logging

Tutte le comunicazioni tra client e dispositivo avvengono tramite connessione end-to-end crittografata AES-256. I log sono sempre attivi e consultabili.

Valutazione : Accettabile

Minimizzazione dei dati

Vengono visualizzati solamente gli spezzoni di video sospetti, tralasciando completamente le parti di non interesse. Per ridurre l'inquadratura di zone non rilevanti o sensibili, si utilizzano ottiche strette (non grandangolari).

Valutazione : Accettabile

Controllo degli accessi fisici

Protezione fisica dei dati: Il dispositivo è dotato di una gabbia in acciaio inox, doppio lucchetto e catena antisabotaggio. La microSD non è accessibile dall'utente, che può interagire con il sistema solo tramite interfaccia software sicura.

Le immagini vengono visualizzate esclusivamente all'interno del Comando di Polizia Locale, salvo limitate operazioni di assistenza e manutenzioni.

Valutazione : Accettabile

Protezione contro fonti di rischio non umane

Grado di protezione IP 66

Temperatura operativa: -20° / +50°

Valutazione : Accettabile

Controllo degli accessi logici

Profilazione degli accessi

Accesso differenziato per ruolo: utenti con solo visualizzazione, operatori per gestione limitata, amministratori con accesso completo. L'accesso è sempre protetto da credenziali univoche.

Le immagini possono essere visualizzate esclusivamente nel comando di Polizia Locale da personale appartenente al comando di polizia locale del Comune di Montalcino in possesso della qualifica di APS e APG/UPG.

Valutazione : Accettabile

Rischi

Accesso illegittimo ai dati

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

Diffusione delle immagini dei movimenti di veicoli o persone", Diffusione delle immagini, modifiche indesiderate dei dati, perdita delle videoregistrazioni, ricostruzione dei movimenti di veicoli o persone

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Furto dello strumento con conoscenza dei dati relativi alla crittografia., Errore umano, attacco informatico, evento accidentale, guasto tecnico

Quali sono le fonti di rischio?

Furto da parte di malintenzionati, eventi esterni

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Minimizzazione dei dati, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane, Controllo degli accessi logici

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

Limitata,

limitata a fronte delle misure tecnico-organizzative esistenti o pianificate

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

Limitata,

limitata a fronte delle misure tecnico-organizzative esistenti o pianificate

Valutazione : Accettabile

Rischi

Modifiche indesiderate dei dati

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

Diffusione delle immagini, modifiche indesiderate dei dati, perdita delle videoregistrazioni, ricostruzione dei movimenti di veicoli o persone

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

Furto dello strumento con conoscenza dei dati relativi alla crittografia., Errore umano, attacco informatico, evento accidentale, guasto tecnico

Quali sono le fonti di rischio?

Furto da parte di malintensionati, eventi esterni

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

Crittografia, Minimizzazione dei dati, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane, Controllo degli accessi logici

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

Limitata,

limitata a fronte delle misure tecnico-organizzative esistenti o pianificate

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

Limitata,

limitata a fronte delle misure tecnico-organizzative esistenti o pianificate

Valutazione : Accettabile

Rischi

Perdita di dati

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

perdita delle videoregistrazioni

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

Errore umano, evento accidentale, guasto tecnico

Quali sono le fonti di rischio?

eventi esterni

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

Controllo degli accessi fisici, Protezione contro fonti di rischio non umane, Controllo degli accessi logici

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

Limitata,

limitata a fronte delle misure tecnico-organizzative esistenti o pianificate

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

Limitata,

limitata a fronte delle misure tecnico-organizzative esistenti o pianificate

Valutazione : Accettabile

Rischi

Panoramica dei rischi

Impatti potenziali

Diffusione delle immagini ...
Diffusione delle immagini
modifiche indesiderate dei ...
perdita delle videoregistra...
ricostruzione dei movimenti...

Minaccia

Furto dello strumento con c...
Errore umano
attacco informatico
evento accidentale
guasto tecnico

Fonti

Furto da parte di malintens...
eventi esterni

Misure

Crittografia
Minimizzazione dei dati
Controllo degli accessi fis...
Protezione contro fonti di ...

Accesso illegittimo ai dati

Gravità : Limitata

Probabilità : Limitata

Modifiche indesiderate dei dati

Gravità : Limitata

Probabilità : Limitata

Perdita di dati

Gravità : Limitata

Probabilità : Limitata