COMUNE DI BARBERINO DI MUGELLO

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Sistemi di Videosorveglianza mobile per la prevenzione ed il sanzionamento di illeciti ambientali

NORMATIVA DI RIFERIMENTO

La normativa relativa alla materia della videosorveglianza comprende:
- Provvedimento in materia di videosorveglianza emanato dal Garante per la protezione dei dati personali in data 8 aprile 2010 (che sostituisce il Provvedimento generale del 29 aprile 2004), in particolare il paragrafo 5.2;
- Regolamento UE n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;
- D. Lgs. 30 giugno 2003, n. 196, recante: "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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" e successive modificazioni (D.Lgs. 10 agosto 2018, n. 101, D.L. 8 ottobre 2021, n. 139 conv. in L. 3 dicembre 2021, n. 205);
- Legge 24 novembre 1981, n. 689 in particolare l'art. 13, recante "Atti di accertamento", secondo cui gli organi addetti al controllo sull'osservanza delle disposizioni per la cui violazione è prevista la sanzione amministrativa del pagamento di una somma di denaro possono procedere, per accertare le violazioni di loro competenza, fra le altre cose, a rilievi segnaletici, descrittivi e fotografici e ad ogni altra operazione tecnica;
- D.P.R. 22 settembre 1988, n. 447, recante "Approvazione del codice di procedura penale" e in particolare l'art. 331, recante "Denuncia da parte di pubblici ufficiali e incaricati di un pubblico servizio";
- Linee guida n. 3/2019 del 10 Luglio 2019 del Comitato europeo per la protezione dei dati personali effettuati con apparecchiature video;
- Regolamento Comunale sulla Videosorveglianza.

I sistemi mobili di videosorveglianza rientrano nell'ambito della disciplina di cui al Regolamento U.E. 2016/679 e del D.Lgs. 196/2003.

Il **Provvedimento del Garante della Privacy in materia di videosorveglianza del 8 aprile 2010** stabilisce al **Punto 5.2** – "Deposito dei rifiuti" che "*In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l´utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad accertare l´utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi*".
Il trattamento operato dagli agenti di Polizia Locale dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza attivati nel territorio dell'Ente, avviene ai sensi del Reg. UE 2016/679, in osservanza delle disposizioni contenute nel Provvedimento in materia di videosorveglianza emanato dal Garante per la protezione dei dati personali in data 8 aprile 2010.

L'impatto è valutato con particolare attenzione ai diritti e alle libertà degli interessati e ha come obiettivo di verificare e garantire la protezione dei dati personali di tutti coloro che entrano in contatto o in relazione con l'attività di videosorveglianza mobile (fototrappole).
I sistemi mobili di videosorveglianza costituiscono supporto all'esercizio di compiti attuati dalla Polizia Locale di accertamento violazioni amministrative, ferma restando l'eventuale rilevazione, in via incidentale, di condotte che possono astrattamente assumere rilevanza sul piano penale, affinché le autorità di polizia e giudiziaria possano effettuare gli accertamenti e adottare i conseguenti provvedimenti di propria competenza.
I trattamenti, effettuati nell'esercizio delle ordinarie funzioni di polizia amministrativa sono finalizzati ad accertare condotte sanzionate prevalentemente in via amministrativa:

- art. 13 della L. 689/1981, avente ad oggetto “Atti di accertamento”;
- art. 192 del D.Lgs. 152/2006, avente ad oggetto “divieto di abbandono”;
- art. 255 del D.Lgs. 152/2006, avente ad oggetto “abbandono di rifiuti”
- artt. 19 e 80 del Regolamento per la gestione dei rifiuti e del servizio di gestione integrata dei rifiuti urbani, approvato con Delibera di Consiglio n. 10 del 15/02/2016.

Ai fini del presente documento si intende:
1. per **dato personale**, qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all’ubicazione, un identificativo online od a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2. per **trattamento**, qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione;
3. per **Titolare del trattamento**, la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell’Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell’Unione o degli Stati membri;
4. per **Responsabile (esterno) del trattamento**, la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
5. per **Autorizzato o Incaricato del trattamento**, la persona fisica che abbia accesso a dati personali e agisca sotto l’autorità del Titolare o del Responsabile interno del trattamento;
6. per **Interessato**, la persona fisica identificata o identificabile cui si riferiscono i dati personali oggetto di trattamento.

A - CONTESTO

PANORAMICA DEL TRATTAMENTO

Qual è il trattamento preso in considerazione?

Nel presente documento la valutazione di impatto concerne il trattamento dati svolto dal Comune di Barberino di Mugello attraverso il sistema di videosorveglianza con mezzi mobili di rilevamento (c.d. foto-trappole) forniti, a seguito di apposita procedura di affidamento, dalla ditta ILES S.r.l., con sede in via Franco Vannetti Donnini 81/1 – 59110 Prato.
Il trattamento consiste nella raccolta e registrazione di foto crittografate, decodifica, estrapolazione, gestione e versamento su una piattaforma informatica e, da PC della Polizia municipale, consultazione, archiviazione e cancellazione.

Quali sono le responsabilità connesse al trattamento?

Le responsabilità del trattamento sono connesse ai ruoli ricoperti in forza di appositi provvedimenti di designazione.

Titolare del Trattamento:
Comune di Barberino di Mugello, rappresentato dal Sindaco pro-tempore, con sede in Viale della Repubblica n. 24, pec barberino-di-mugello@postacert.toscana.it

Responsabile della protezione dei dati (RPD)/data protection officer (DPO):
Avv. Francesco Barchielli, francesco.barchielli@firenze.pecavvocati.it
email dpo@comune.barberino-di-mugello.fi.it

Designato/Responsabile del trattamento:
Il Responsabile del Settore Tecnico, Ing. Sebastiano Massimiliano Galasso, quale Responsabile del trattamento nominato con Decreto del Sindaco n. 18 del 22/08/2025, provvederà, a titolo esemplificativo e non esaustivo, a:
- individuare e nominare per iscritto i Responsabili esterni del trattamento, dando loro idonee istruzioni;
- vigilare sul rispetto delle istruzioni impartite ai Responsabili esterni del trattamento;
- adottare e rispettare le direttive e le misure di sicurezza tecniche e organizzative nel trattamento dei dati personali;
- evadere tempestivamente tutte le richieste e gli eventuali reclami degli Interessati;
- evadere le richieste di informazioni eventualmente pervenute da parte dell'Autorità garante in materia di protezione dei dati personali, nei termini e secondo le modalità contenute nelle richieste;
- interagire con i soggetti appositamente delegati ad eventuali verifiche, controlli o ispezioni;
- provvedere a supervisionare le procedure di cancellazione/distruzione dati raccolti per il tramite di sistemi di videosorveglianza, nel caso cui venga meno lo scopo del trattamento ed il relativo obbligo di conservazione;
- ogni ed altra qualsivoglia attività espressamente a lui delegata dal Sindaco.

Responsabili esterni del trattamento
I responsabili esterni del trattamento, autorizzati con atto scritto del Designato/Responsabile del trattamento, sono tutti i soggetti che effettuino in via principale o residuale un trattamento dati derivante dalla raccolta di immagini effettuate per il tramite della videosorveglianza, con specifica delimitazione dell'ambito di competenza.

In particolare, poiché il Comune di Barberino di Mugello ha conferito, come altri Comuni del Mugello, la funzione Polizia Amministrativa e Locale all'Unione Montana dei Comuni del Mugello, trasferendo a tale Ente già da marzo 2014 il proprio personale di Polizia Municipale, per la costituzione della Struttura Unica della Polizia Locale dell'Unione Mugello, il suddetto Responsabile del trattamento si avvarrà della Polizia Municipale Unione Mugello – Distretto di Barberino di Mugello, quale responsabile esterno al trattamento dei dati, limitatamente alle immagini trasferite su apposita piattaforma riservata alla Polizia Municipale, ai fini del sanzionamento degli episodi di abbandono che emergeranno da tali immagini, secondo le procedure indicate al punto 3) della sezione "DATI, PROCESSI E RISORSE DI SUPPORTO".

Saranno nominati, ciascuno per un ambito definito di trattamento, i seguenti soggetti:
Ditta ILES s.r.l. (per raccolta e registrazione dati);
Ditta GEOTECH ENGINEERING s.r.l. (sub responsabile per estrapolazione, pre-classificazione ed elaborazione, registrazione e cancellazione dati);
Polizia Municipale in servizio presso il Distretto di Barberino di Mugello (per gestione, elaborazione, archiviazione, cancellazione dati).

Ci sono standard applicabili al trattamento?

L'attività di videosorveglianza è disciplinata da specifico regolamento dell'ente per l'utilizzo del sistema di videosorveglianza ambientale nel territorio comunale.

Il trattamento fa riferimento principalmente a:
- Regolamento Europeo 679/2016 (GDPR) e D.Lgs 196/2003 come modificato dal D.Lgs 101/2018;
- Provvedimento del Garante Privacy dell'8 Aprile 2010 e s.m.i.;
- Pareri e provvedimenti generali del Garante Privacy;
- EDPB, Linee Guida 03/2019 dell'European Data Protection Board sul trattamento dei dati personali attraverso dispositivi video.

DATI, PROCESSI E RISORSE DI SUPPORTO

Quali sono i dati trattati?

I dati trattati consistono in immagini riportanti data, orario della rilevazione delle persone e delle targhe dei mezzi che transitano nel raggio d'azione delle fotocamere.

Qual è il ciclo di vita del trattamento dei dati?

Il ciclo di vita dei dati prevede i seguenti trattamenti:
- ripresa;
- registrazione;
- estrapolazione dei dati;
- gestione delle registrazioni;
- raccolta dati;
- elaborazione dati;
- cancellazione dei dati.

Quali sono le risorse di supporto dei dati?

1. Descrizione della videocamera mobile

Il sistema di videosorveglianza mobile è composto da n. 2 fotocamere modello AFC CAMERA, prodotto da Geotech Engineering S.r.l. e avente le seguenti caratteristiche: fotocamera automatica funzionante senza fili e senza collegamenti dati, con sistema di attivazione tramite PIR, con intensità e durata di rilevazione regolabile via software e capace di essere attiva stand by con 4 batterie litio per oltre 100 giorni, attiva in funzione per una durata di 7 giorni e dotata di un sistema opzionale di localizzazione GPS.

2. Registrazioni crittografate

Le immagini sono memorizzate su scheda SD allocata internamente alle fotocamere, dotata di Firmware con crittografia dati.
La chiave di crittografia è configurata in modo univoco da dispositivo a dispositivo.

3. Modalità di accesso al sistema di videosorveglianza

La ditta ILES s.r.l. è il soggetto affidatario della fornitura dei due dispositivi e del servizio di gestione. Effettua, previo sopralluogo, l'installazione delle fotocamere e dell'apposita segnaletica.

La ditta GEOTECH ENGINEERING s.r.l. effettua il monitoraggio settimanale con acquisizione dei dati crittografati, sostituzione batterie, eventuale ricollocazione delle fotocamere in postazioni diverse; esegue, con cadenza settimanale, la decriptazione delle SD card estratte dalle fotocamere; visiona le immagini e le pre-classifica, selezionando i fotogrammi riferiti a episodi di abbandono o non corretto conferimento dei rifiuti (in caso di incertezza seleziona comunque il materiale, riservando ogni valutazione alla Polizia Municipale); elabora le immagini selezionate, apponendo data e ora dell'evento rilevato; carica le sole foto inerenti ad episodi di abbandono su apposita piattaforma con accesso riservato alla Polizia Municipale; compila un report di scarico delle immagini riportando i riferimenti della fotocamera, i dati relativi al luogo e all'arco temporale di rilevazione, nonché il numero degli eventi documentati.

Gli agenti della Polizia Municipale Unione Mugello – Distretto di Barberino di Mugello, consultano le sole immagini caricate sull'apposita piattaforma dalla ditta GEOTECH ENGINEERING s.r.l., senza poter interagire sulle telecamere, al fine di verificare o meno la sussistenza di violazioni ed in caso positivo, la natura delle medesime (amministrativa o penale) per la successiva adozione degli atti consequenziali. L'accesso alla suddetta piattaforma, dedicata alla Polizia Municipale, avviene attraverso autenticazione informatica, collegandosi ad un'interfaccia web esclusivamente da

postazioni situate all'interno della sede del Comando di Polizia Municipale – Distretto di Barberino di Mugello.

4. Log di sistema

Gli accessi all'interfaccia web vengono salvati in una pagina di log, dalla quale si evincono gli orari di accesso – uscita dal sistema.

5. Caratteristiche tecniche

Le caratteristiche specifiche sono contenute nella scheda tecnica fornita dalla ditta installatrice, ed allegata al presente documento.
Come da contratto con la ditta ILES:
• le registrazioni vengono sovrascritte dopo sette giorni;
• le foto vengono protette da una codifica HASH che ne garantisce l'autenticità;
• le foto sono crittografate in modo che in caso di furto della SD CARD non possano essere lette;
• sulle foto sono riportate data, ora e nome della via dove è posizionata la fotocamera.

B - PRINCIPI FONDAMENTALI

La valutazione della DPIA deve uniformarsi ai valori e ai criteri generali del trattamento dei dati contenuti nel GDPR e in particolare verificare che siano attuati i principi di:
- liceità e correttezza (art. 5 par. 1 lett. a GDPR e art. 3 c. 1 lett. a D.LGS.51/2018);
- trasparenza (art. 5 par. 1 lett. a GDPR);
- limitazione delle finalità (art. 5 par. 1 lett. b GDPR e art. 3 c. 1 lett. b D.LGS.51/2018);
- minimizzazione dei dati (art. 25 par. 2 lett. c GDPR e art. 3 c. 1 lett. c D.LGS.51/2018);
- esattezza (art. 5 par. 1 lett. d GDPR e art. 3 c. 1 lett. c D.LGS.51/2018);
- diritto all'oblio (art. 5 par. 1 lett. e GDPR);
- integrità e riservatezza (art. 5 par. 1 lett. f GDPR e art. 3 c. 1 lett. f D.LGS.51/2018);
- responsabilizzazione (art. 5 par. 2 GDPR).

PROPORZIONALITA' E NECESSITA'

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento dei dati personali si svolge nel pieno rispetto dei principi di liceità, finalità, limitazione, pertinenza e proporzionalità, sanciti dal Codice Privacy novellato e dal Reg. UE 2016/679; il trattamento è effettuato dall'Ente esclusivamente per lo svolgimento delle funzioni istituzionali e per legittimo interesse.
In particolare, il trattamento è finalizzato ad accertare condotte sanzionabili prevalentemente in via amministrativa:
- art. 13 della L. 689/1981, avente ad oggetto "Atti di accertamento";
- art. 192 del D.Lgs. 152/2006, avente ad oggetto "divieto di abbandono";
- art. 255 del D.Lgs. 152/2006, avente ad oggetto "abbandono di rifiuti";
- artt. 19 e 80 del Regolamento per la gestione dei rifiuti e del servizio di gestione integrata dei rifiuti urbani, approvato con Delibera di Consiglio n. 10 del 15/02/2016.

In attuazione del principio di limitazione e pertinenza, gli impianti di videosorveglianza mobile e i programmi informatici di gestione sono configurati in modo da ridurre al minimo l'uso di dati personali ed identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere raggiunte mediante dati anonimi o con modalità che permettano di identificare l'interessato solo in caso di necessità, sono configurati in modo da raccogliere esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese ed evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti.

Principio di proporzionalità – La raccolta e l'uso delle immagini sono proporzionali agli scopi perseguiti. Nel commisurare la necessità del sistema di videosorveglianza al grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra una effettiva esigenza di deterrenza.

Principio di integrità e riservatezza - Il Titolare del trattamento tratta i dati personali in modo da garantire un'adeguata sicurezza degli stessi, compresa la protezione mediante misure tecniche ed organizzative adeguate, prevenendo trattamenti non autorizzati o illeciti oltre alla perdita, alla distruzione o al danno accidentale.
La piattaforma informatica, a cui avranno accesso gli agenti del Comando di Polizia Municipale, si limita a consentire, ai fini di controllo, la visualizzazione e lo scarico degli eventi (immagini) di abbandono o conferimento errato.
Il Provvedimento del 8 aprile 2010 del Garante, al punto 5, dispone che i soggetti pubblici in qualità di titolari del trattamento (art. 4, comma 1, lett. f), del Codice), possono trattare dati personali nel

rispetto del principio di finalità, perseguendo scopi determinati, espliciti e legittimi, soltanto per lo svolgimento delle proprie funzioni istituzionali.
Al punto 5.2 “Deposito dei rifiuti" il Garante precisa che "*In applicazione dei richiamati principi di liceità, finalità e proporzionalità, l´utilizzo di sistemi di videosorveglianza risulta lecito con riferimento alle attività di controllo volte ad accertare l´utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose solo se non risulta possibile, o si riveli non efficace, il ricorso a strumenti e sistemi di controllo alternativi.*
Analogamente, l´utilizzo di sistemi di videosorveglianza è lecito se risultano inefficaci o inattuabili altre misure nei casi in cui si intenda monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (art. 13, l. 24 novembre 1981, n. 689)”.
L'art. 13, comma 1, della L. 24 novembre 1981, n. 689 stabilisce che "*Gli organi addetti al controllo sull'osservanza delle disposizioni per la cui violazione è prevista la sanzione amministrativa del pagamento di una somma di denaro possono, per l'accertamento delle violazioni di rispettiva competenza, assumere informazioni [...] a rilievi segnaletici, descrittivi e fotografici e ad ogni altra operazione tecnica*".
L'art. 331 c.p.p. al comma 1 stabilisce che "[...] *i pubblici ufficiali e gli incaricati di un pubblico servizio che, nell'esercizio o a causa delle loro funzioni o del loro servizio, hanno notizia di un reato perseguibile di ufficio, devono fare denuncia per iscritto, anche quando non vi sia individuata la persona alla quale il reato è attribuito*". Al comma 4 aggiunge: "*Se, nel corso di un procedimento [...] amministrativo, emerge un fatto nel quale si può configurare un reato perseguibile di ufficio, l'autorità che procede redige e trasmette senza ritardo la denuncia al pubblico ministero*".
I sistemi mobili potranno essere installati in prossimità di zone pubbliche o private, in cui vi è una motivata esigenza di controllo, senza limitazioni geografiche su tutto il territorio cittadino, dove non si è rivelato efficace il ricorso a strumenti di controllo alternativi.
Le fototrappole, unitamente all'Informativa di primo livello, assumono, infatti, anche una funzione di deterrenza.

Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica che legittima il trattamento mediate videosorveglianza mobile è l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, par. 1, lett. e, del GDPR).
In particolare, il trattamento è necessario per l’esercizio delle ordinarie funzioni di polizia amministrativa, finalizzate ad accertare condotte sanzionate prevalentemente in via amministrativa:
- art. 13 della L. 689/1981, avente ad oggetto "Atti di accertamento";
- art. 192 del D.Lgs. 152/2006, avente ad oggetto "divieto di abbandono";
- art. 255 del D.Lgs. 152/2006, avente ad oggetto "abbandono di rifiuti";
- artt. 19 e 80 del Regolamento per la gestione dei rifiuti e del servizio di gestione integrata dei rifiuti urbani, approvato con Delibera di Consiglio n. 10 del 15/02/2016.

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 ed elaborati vengono costantemente minimizzati utilizzando unicamente le informazioni strettamente necessarie alla finalità.
Gli impianti mobili riprendono immagini che permettono di identificare in modo diretto o indiretto le persone riprese. Le ottiche utilizzate sulla fotocamera sono tali da ottenere un’ampiezza di campo minore al fine di rilevare solamente immagini relative all’area sottoposta ad indagine evitando di riprendere dati in eccesso non utili ai fini del controllo.
Le fotocamere non effettuano alcun trattamento di dati biometrici e non consentono il riconoscimento facciale.

Sono posizionate in area predefinite dove non è frequente il passaggio di persone. Il numero di interessati coinvolti nel trattamento è dunque limitato.
Come è precisato infatti nelle Linee guida n. 3/2019 del 10 Luglio 2019 del Comitato europeo per la protezione dei dati personali, l'uso della videosorveglianza in una zona isolata "*deve essere valutato in modo diverso rispetto alla videosorveglianza in una zona pedonale o in un centro commerciale*".

I dati sono esatti ed aggiornati?

I dati personali di persone fisiche eventualmente raccolti a seguito dell'attivazione della fotocamera che non riprendono fenomeni di abbandono rifiuti (quindi dati personali "inesatti") sono cancellati automaticamente nel termine di cui sopra.

Qual è il periodo di conservazione dei dati?

Le Linee guida n. 3/2019 del 10 Luglio 2019 precisano che "*La necessità o meno di conservare i dati personali dovrebbe essere valutata entro una tempistica ristretta. In via generale, gli scopi legittimi della videosorveglianza sono spesso la protezione del patrimonio o la conservazione di elementi di prova. Solitamente è possibile individuare eventuali danni entro uno o due giorni. Per facilitare la dimostrazione di conformità al quadro normativo in materia di protezione dei dati, è nell'interesse del titolare del trattamento organizzarsi proattivamente (ad esempio nominando, se necessario, un responsabile per lo screening e la protezione del materiale video). Tenendo conto dei principi di cui all'articolo 5, paragrafo 1, lettere c) ed e), del RGPD, vale a dire la minimizzazione dei dati e la limitazione della loro conservazione, i dati personali dovrebbero essere – nella maggior parte dei casi (ad esempio se la videosorveglianza serve allo scopo di rilevare atti vandalici) – cancellati dopo alcuni giorni, preferibilmente tramite meccanismi automatici*".
La totalità delle immagini catturate dalle fotocamere mobili vengono conservate (come da Regolamento comunale sulla videosorveglianza) soltanto per il tempo prestabilito pari a massimo 7 giorni successivi alla rilevazione, dopo di che verranno sovrascritte. Le sole immagini che saranno trasferite dalle telecamere alla piattaforma da parte della ditta incaricata, saranno conservate fino alla conclusione delle procedure sanzionatorie (amministrative o penali); fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o servizi, nonché nel caso in cui si debba adire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

Come sono informati del trattamento gli interessati?

L'utilizzo delle fotocamere mobili è soggetto ad Informativa Privacy attraverso cartellonistica apposta prima del raggio d'azione delle fotocamere o nelle immediate vicinanze delle stesse (**Informativa di primo livello**) in modo da permettere all'Interessato di riconoscere facilmente le circostanze della sorveglianza, prima di entrare nella zona sorvegliata (approssimativamente all'altezza degli occhi).
A tal fine i cartelli, recanti immagine informativa conforme alle indicazioni di cui al punto 7.1.2 n.114 delle Linee guida 3/2019,[1] contengono un'informativa sintetica indicante:

[1] *European Data Protection Board Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video. Punto 7.1.2 Contenuto delle informazioni di primo livello:* «114. Generalmente, le informazioni di primo livello (segnale di avvertimento) dovrebbero comunicare i dati più importanti, ad esempio le finalità del trattamento, l'identità del titolare del trattamento e l'esistenza dei diritti dell'interessato, unitamente alle informazioni sugli impatti più consistenti del trattamento. Si può fare riferimento, ad esempio, ai legittimi interessi perseguiti dal titolare (o da un soggetto terzo) e ai recapiti del responsabile della protezione dei dati (se applicabile). Occorre anche fare riferimento alle informazioni di secondo livello, più dettagliate indicando dove e come trovarle.».

- l'identità del titolare del trattamento: Comune di Barberino di Mugello Pec: barberino-di-mugello@postacert.toscana.it
- le finalità del trattamento: tutela della sicurezza urbana e del decoro del territorio comunale anche attraverso l'accertamento degli illeciti concernenti la gestione dei rifiuti avvalendosi della Polizia Locale dell'Unione Mugello (art. 5 L.65/1986 e art. 13 L.689/81);
- i diritti fondamentali degli interessati;
- indirizzo del sito internet del Comune di Barberino di Mugello su cui prendere visione della informativa completa (**Informativa di secondo livello** contenente tutte le informazioni richieste dall'art. 13 del GDPR con riferimento ai trattamenti di dati personali in questione).

Tutti gli interessati possono prendere visione e stampare copia dell'informativa completa sul trattamento dei dati personali dal sito del Comune di Barberino di Mugello, oppure ottenerne copia fisica accedendo agli uffici comunali.

Non necessità di consenso degli interessati

Il trattamento dei dati personali con riferimento alle fotocamere mobili non richiede il consenso dell'Interessato ai sensi dell'art. 6, par. 1, lett. a, del GDPR.
La base giuridica che legittima il trattamento mediate videosorveglianza mobile è l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, par. 1, lett. e, del GDPR).

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

In relazione al trattamento di dati personali che lo riguardano, l'Interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss., GDPR, può presentare apposita istanza al Titolare del trattamento dei dati personali, i cui dati di contatto sono espressamente indicati nell'informativa e pubblicati sul sito istituzionale del Comune di Barberino di Mugello, sezione Privacy.
L'Interessato ha diritto:
a) di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi;
b) ad essere informato sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali;
c) di richiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
d) di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano.

Il Titolare accerterà l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano.
Nel caso di esito negativo alla istanza di cui ai commi precedenti, l'Interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.
L'interessato potrà ricevere l'accesso ai dati e le informazioni ai sensi dell'art. 15 del GDPR se i dati sono ancora in corso di trattamento (visti i tempi di conservazione previsti e la successiva cancellazione).
Qualora sia già trascorso il tempo di conservazione dei dati previsto, l'Interessato sarà informato che i propri dati personali non sono più oggetto di trattamento al momento della richiesta in quanto cancellati.
Qualora la richiesta dell'interessato di ricevere una copia dei dati personali trattati (foto) possa ledere i diritti e le libertà di altri soggetti eventualmente ritratti nella foto, il Titolare del trattamento

metterà in atto misure tecniche per soddisfare la richiesta di accesso (modifica delle immagini tramite mascheramento-sfuocatura delle aree non di interesse).

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

Gli Interessati hanno diritto di ottenere dal Titolare la conferma o meno del fatto che i propri dati personali siano oggetto di trattamento, nonché la cancellazione dei dati personali ai sensi dell'art. 17 del GDPR.

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

Per esercitare il diritto di limitazione o opposizione, gli Interessati possono presentare istanza come da allegato 1 al Regolamento comunale sulla videosorveglianza. L'interessato ha il diritto di opporsi al trattamento in qualsiasi momento, per motivi connessi alla sua situazione particolare, ai sensi dell'articolo 21 del GDPR. A meno che il Titolare possa dimostrare l'esistenza di motivi legittimi cogenti che prevalgono sui diritti e sugli interessi dell'interessato, il trattamento dei dati della persona che vi si è opposta cesserà.

Il Responsabile del trattamento risponderà alle richieste dell'Interessato senza ritardo non oltre 15 giorni dalla data di ricezione della richiesta (o al massimo entro 30 giorni – dandone comunicazione all'Interessato - se ricorra giustificato motivo).

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

Gli obblighi di ogni singolo responsabile del trattamento sono definiti negli atti di nomina/designazione (agli atti del Comune).

I ruoli e i compiti dei responsabili sono inoltre definiti nel Regolamento comunale sulla videosorveglianza.

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

I dati non vengono trasferiti al di fuori dell'Unione Europea.

C – RISCHI - MISURE ESISTENTI O PIANIFICATE

Valutazione del sistema di rilevazione

Il sistema di rilevazione consiste di n. 2 dispositivi di monitoraggio abbandono rifiuti (fotocamere) con le caratteristiche tecniche di seguito riepilogate:

- Foto a colori di giorno e in bianco e nero di notte;
- Sensore video ottimizzato per notturno 2MegaPixel con parametri lettura targhe impostabili da file setpar.mep relativi a luminosità contrasto;
- Capacità di lettura delle targhe in qualunque situazione di veicolo fermo, in situazione diurna e notturna anche con fari auto puntati contro l'ottica per un range di 5-15 metri dal posizionamento del dispositivo;
- Resistente ad alta compressione fino a 20 N/mmq. Resistente agli effetti di corrosione atmosferica, mascheramento con cartello PVC;
- Ottica intercambiabile camera 6mm grandangolare 3-10m 8mm medio angolo 5-15 12mm 8-20 metri. Illuminatore IR integrato, illuminazione fino a 20 metri, con calendario mensile per accendere l'illuminatore solo ad orario prestabilito;
- Programmazione funzionamento per fasce orarie, per disabilitare il funzionamento in due fasce orarie programmabili;
- Registrazione su Sd Card fino a 256 GB;
- Sovrascrittura SD dopo 7 giorni;
- Crittazione SD: tramite crittatura con chiave a 128 bit (Nessun utente deve poter ottenere o dedurre dal sistema informazioni che non è autorizzato a conoscere) – Attivabile/disattivabile da software;
- Anticontraffazione: tramite codifica HASH SHA1 il sistema salva una stringa di caratteri univoca per ogni immagine – Attivabile/disattivabile da software.

Per maggiori dettagli, si rimanda alla scheda tecnica allegata.

La valutazione della sicurezza di questo sistema di acquisizione dei dati si è svolta sui seguenti punti (Linee guida videosorveglianza):

a) protezione dei dati, attraverso l'archiviazione remota delle immagini ovvero l'implementazione di sistemi di crittografia;

b) protezione antifurto (opzionale), attraverso idonei sistemi fisici, di segnalazione e localizzazione remota dello spostamento non autorizzato per impedire rischi di accesso illecito e sottrazione dei dati;

c) protezione della fotocamera, dagli agenti atmosferici, dalla polvere e dagli impatti di eventuali colpi con corpi contundenti per finalità illecite;

d) sicurezza informatica, attraverso sistemi di cybersicurezza che proteggano l'accesso remoto non autorizzato al sistema di trasmissione delle immagini (trasmissione sicura delle immagini tramite protocolli cifrati tramite crittografia).

Valutazione del sistema di archiviazione si è svolta sui seguenti piani:

a) **sicurezza fisica** (Linee guida videosorveglianza punto 9.3.2-132 p. 35), valutando la protezione e resilienza in caso di interferenze volontarie e involontarie sulla parte hardware e quindi sulle macchine elettroniche, quindi la protezione da furti, atti vandalici, calamità naturali, catastrofi provocate dall'uomo e danni accidentali;

b) **sicurezza del sistema e dei dati** (Linee guida videosorveglianza punto 9.3.2-134 p. 35), valutando la protezione e resilienza sulla parte software e quindi del contenuto informatico in caso di interferenze volontarie e involontarie nel suo normale funzionamento quindi la protezione accesso abusivo al sistema, sottrazione, utilizzo abusivo, danneggiamento, alterazione, blocco del sistema, come ad esempio virus, malware, spyware, ransomware, accessi abusivi al sistema informatico;

c) il **controllo degli accessi** (Linee guida videosorveglianza punto 9.3.2-135 p. 35-36), valutando i sistemi e le procedure per garantire che solo le persone autorizzate possano accedere al sistema e ai dati, impedendo a chiunque altro di farlo.

Quindi nella valutazione della sicurezza del sistema di archiviazione delle immagini si è tenuto conto del:

a) controllo dell'accesso fisico, verificando che non ci sia il rischio di accessi non autorizzati ai locali di archiviazione delle immagini, ricorrendo all'archiviazione in cloud;

b) controllo della sicurezza dei dati archiviati, verificando che non ci sia il rischio di accessi non autorizzati ai dati archiviati e che i monitor siano orientati in maniera da non permettere la visualizzazione ad altri soggetti estranei;

c) controllo degli accessi logici, verificando che non ci sia il rischio di accessi non autorizzati al sistema di videosorveglianza e che:

   - ogni utente disponga di una password univoca che rispetti i requisiti di sicurezza;
   - ogni utenza consenta l'accesso personalizzato solo ai dati e alle parti autorizzate.

d) verifica file log degli utenti, per poter verificare e accertare a posteriori:

   - chi abbia avuto accesso al sistema;
   - quali dati personali siano stati gestiti nell'archivio;
   - la cronodatazione di ogni accesso.

e) controllo della ridondanza, per garantire che i sistemi di archiviazione e i dati in essi contenuti possano essere ripristinati in caso di perdita;

f) controllo dell'affidabilità e integrità del sistema, per garantire che le funzioni del sistema siano sempre operative e che eventuali errori di funzionamento siano segnalati (affidabilità) e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema (integrità).

Alle misure sopra indicate, si aggiungono:

Cancellazione automatica dei dati

Le immagini catturate dalle fotocamere mobili vengono conservate soltanto per il tempo prestabilito pari a massimo 7 giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore

conservazione in relazione a festività o chiusura di uffici o servizi, nonché nel caso in cui si debba adire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

Sicurezza dei documenti cartacei

Il trattamento si svolge essenzialmente su strumenti elettronici/digitali.
Eventuali stampe o documenti cartacei sono conservati per il tempo strettamente necessario al procedimento a cui afferiscono, presso l'ufficio della Polizia Municipale – Distretto di Barberino di Mugello, in archivio chiuso a chiave.

Minimizzazione dei dati

Il principio di minimizzazione dei dati implica che siano trattati solo i dati realmente necessari per raggiungere le finalità del trattamento. I sistemi di rilevazione raccolgono le sole immagini di contesto, senza estrapolazione automatica di dati biometrici.

Manutenzione

L'attività è condotta in outsourcing: la manutenzione fisica dei sistemi di rilevazione viene effettuata, secondo quanto stabilito da contratto, dalla stessa ditta che li ha forniti.

Politica di tutela della privacy

L'Ente pone attenzione a tutti gli aspetti in tema di normativa sulla Privacy derivanti dai trattamenti di dati personali effettuati ed attua un adeguamento continuo alle prescrizioni vigenti. Ha approvato un Regolamento comunale relativo alla protezione dei dati personali oltre ad uno specifico Regolamento in materia di videosorveglianza. Ha designato i Responsabili dei trattamenti. Coinvolge e consulta il DPO nelle questioni attinenti alla normativa sulla privacy.

Gestione del personale

Il personale autorizzato al trattamento è formato in merito alla normativa sulla privacy.

Struttura, compiti e responsabilità dei soggetti

I compiti sono ripartiti in modo chiaro secondo competenze e ruoli. Le responsabilità del trattamento sono connesse ai ruoli ricoperti.

Gestione degli incidenti di sicurezza e le violazioni dei dati personali

L'Ente, in qualità di Titolare del trattamento, si è dotato di una procedura operativa interna per la gestione di eventuali incidenti di sicurezza o Data Breach, in conformità a quanto previsto dal Regolamento (UE) 2016/679 e dal Provvedimento del Garante del 30 luglio 2019.
I Responsabili esterni del trattamento che vengano a conoscenza, anche a seguito di segnalazione di terzi, di un incidente sulla sicurezza o di circostanze che facciano sospettare il verificarsi di un incidente, comunicano immediatamente tale circostanza al Designato Responsabile e al DPO dell'Ente.
Il Responsabile del Settore Tecnico, in qualità di Designato Responsabile del trattamento, ricevuta la segnalazione, effettua senza ritardo una valutazione preliminare congiuntamente al DPO, per determinare se si sia effettivamente verificato un incidente e se esso si configuri come violazione di dati personali.
In caso di violazione dei dati personali, il Titolare del trattamento notificherà la violazione al Garante per la Protezione dei Dati Personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche.

C – RISCHI – MINACCE E LIVELLI DI GRAVITA' E DI PROBABILITA' DEL RISCHIO

ACCESSO ILLEGITTIMO AI DATI

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Divulgazione, Distruzione/Perdita della disponibilità dei dati, perdita di integrità

Quali sono le principali minacce che potrebbero concretizzare il rischio?
Furto dispositivo, atto vandalico, attacco informatico

Quali sono le fonti di rischio?
Fonti umane esterne, fonti non umane, virus informatico

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?
Crittografia, controllo degli accessi logici, tracciabilità, minimizzazione, manutenzione, sicurezza dei canali informatici

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Trascurabile. La possibilità di accesso illegittimo ai dati appare remota.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?
Trascurabile. La probabilità di accesso illegittimo ai dati appare remota.

MODIFICHE INDESIDERATE DEI DATI

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

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?
Furto dispositivo, atto vandalico, attacco informatico, malfunzionamento dispositivo

Quali sono le fonti di rischio?
Fonti umane esterne, fonti umane interne, fonti non umane, virus informatico

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Crittografia, controllo degli accessi logici, tracciabilità, sicurezza dei documenti cartacei, minimizzazione, manutenzione, sicurezza dei canali informatici

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?
Trascurabile. La possibilità di modifiche indesiderate ai dati appare remota.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?
Trascurabile. Le modifiche indesiderate ai dati appaiono poco probabili.

PERDITA DI DATI

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?
Distruzione/ Perdita della disponibilità dei dati

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?
Accesso non autorizzato ai dati, Atto vandalico, Furto dispositivo, Guasto dispositivo, Malfunzionamento dispositivo

Quali sono le fonti di rischio?
Fonti umane esterne, fonti umane interne, fonti esterne non umane, virus informatico

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Crittografia, controllo degli accessi logici, tracciabilità, sicurezza dei documenti cartacei, minimizzazione, manutenzione, sicurezza dei canali informatici, prevenzione delle fonti di rischio

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Medio. Il rischio di perdita dati dovuto ad atto vandalico è presente e difficilmente eliminabile, ma in caso di furto della SD CARD, le foto non possono comunque essere lette, in quanto crittografate.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?
Medio. Esiste la probabilità di perdita dati connessa ad atto vandalico.

PANORAMICA DEI RISCHI

Rischi	1.Fonti di rischio	2.Principali impatti sugli interessati	3.Principali minacce	4.Probabilità di rischio , specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate	5.Gravità di rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate	6. Misure di mitigazione del rischio fra quelle sopra individuate
Accesso illegittimo ai dati	Fonti umane esterne, virus informatico	Divulgazione, Distruzione/ Perdita della disponibilità dei dati, perdita di integrità	Furto dispositivo, atto vandalico, attacco informatico	Trascurabile	Trascurabile	Crittografia, controllo degli accessi logici, tracciabilità, minimizzazione, manutenzione, sicurezza dei canali informatici
Modifiche indesiderate dei dati	Fonti umane esterne, fonti umane interne, fonti non umane, virus informatico	Perdita integrità	Furto dispositivo, atto vandalico, attacco informatico, malfunziona-mento dispositivo	Trascurabile	Trascurabile	Crittografia, controllo degli accessi logici, tracciabilità, sicurezza dei documenti cartacei, minimizzazione, manutenzione, sicurezza dei canali informatici
Perdita dei dati	Fonti umane esterne, fonti umane interne, fonti esterne non umane, virus	Distruzione/ Perdita della disponibilità dei dati	Furto dispositivo, atto vandalico, attacco informatico, malfunziona-	Medio	Medio	Crittografia, controllo degli accessi logici, tracciabilità, sicurezza dei documenti cartacei,

	informatico		mento dispositivo, accesso non autorizzato			minimizzazione, manutenzione, sicurezza dei canali informatici, prevenzione delle fonti di rischio

RISULTATI DELLA VALUTAZIONE D'IMPATTO

Le misure tecniche e organizzative individuate per mitigare l'impatto del trattamento sono ritenute ADEGUATE.

Sulla base degli elementi e criteri indicati in precedenza non sono state rilevate criticità e nei successivi aggiornamenti sarà verificata la permanenza di tale situazione.

Allegati:
Scheda tecnica sistemi di rilevazione (foto trappole)
Parere del Responsabile della protezione dei dati - DPO

Geotech Engineering S.r.l.

Via Vecchia Provinciale Lucchese 50 --
51030 Serravalle Pistoiese (PT)
Tel. 0573.51089 - CF e PI 01698450473
info@pec.geotechsrl.org

AFC FOTOCAMERA CONTROLLO AMBIENTALE

CARATTERISTICHE TECNICHE

Descrizione

AFC CAMERA, prodotto esclusivamente da Geotech Engineering Srl, è una fotocamera automatica funzionante senza fili e senza collegamenti dati, con sistema di attivazione tramite PIR, con intensità e durata di rilevazione regolabile via software e capace di essere attiva stand by con 4 batterie litio per oltre 100 giorni e attiva in funzione per una durata di 7 giorni. AFC può essere dotata di un sistema di allarmi (ha un accelerometro per allarmare in caso di furto) e/o di un sistema di localizzazione GPS.

AFC ha le seguenti caratteristiche tecniche :

- Capacità di lettura delle Targhe in qualunque situazione di veicolo fermo
- Foto a colori di giorno e in bianco e nero di notte
- Contenitore in materiale plastico PVC a MEMORIA, con alta resistenza alla compressione e piastra inox posteriore per fissaggio di dimensioni contenute simili ad un cartello di dimensione massima 34X23 e spessore max 4 cm
- Resistente ad alta compressione fino a 20 N/mmq. Resistente agli effetti di corrosione atmosferica, mascheramento con cartello PVC personalizzato con logo Comune
- Ottica intercambiabile camera 6mm grandangolare 3-10m 8mm medio angolo 5-15 12mm 8-20 metri. Illuminatore IR integrato, illuminazione fino a 20metri, con calendario mensile per accendere l'illuminatore sono ad orario prestabilito
- Sensore video ottimizzato per notturno 2MegaPixel con parametri lettura targhe impostabili da file setpar.mep relativi a luminosità contrasto e guadagno del sensore video (scelta per la lettura delle targhe e ridurre la pesantezza delle foto)
- Installazione su palo con possibilità di braccio snodato per l'orientamento del dispositivo nella zona di interesse.
- Programmazione funzionamento per fasce orarie, per disabilitare il funzionamento in due fasce orarie programmabili
- Registrazione su Sd Card fino a 256 GB
- Lettura delle targhe in situazione diurna e notturna anche con fari auto puntati contro l'ottica per un range di 5-15 metri dal posizionamento del dispositivo
- Sovrascrittura SD con tempo in giorni minuti e secondi
- Crittazione SD: tramite XTEA chiave a 128 bit (Nessun utente deve poter ottenere o dedurre dal sistema informazioni che non è autorizzato a conoscere) – Attivabile disattivabile da software
- Anticontraffazione: tramite codifica HASH SHA1 il sistema salva una stringa di caratteri univoca per ogni immagine – Attivabile disattivabile da software

Serravalle Pistoiese (PT) 24/03/2025

Il legale rappresentante

GEOTECH ENGINEERING srl
Via Vecchia Prov.le Lucchese, 50
51030 SERRAVALLE PISTOIESE (PT)
Tel. e Fax. 0573 51089
P.IVA 01698450473 - REA PT-171799

Comune di Barberino di Mugello. Valutazione d'impatto sulla protezione dei dati relativo ai sistemi di Videosorveglianza mobile per la prevenzione ed il sanzionamento di illeciti ambientali. Parere DPO

In merito alla Valutazione di impatto sulla protezione dei dati (D.P.I.A.) relativa al trattamento di videosorveglianza in oggetto, redatta dal Titolare del trattamento, Comune di Barberino di Mugello, ai sensi dell'articolo 35 del Regolamento (UE) 2016/679, trasmessa nella versione definitiva in data 02/09/2025, il sottoscritto, in qualità di Responsabile della Protezione dei Dati (R.P.D./D.P.O.) rilascia il parere di propria competenza così come previsto dall'articolo 39, paragrafo 1, lettera c).

La Valutazione di Impatto è stata redatta indicando tutte gli elementi necessari per un corretto inquadramento del trattamento oggetto di valutazione.

In particolare, il Titolare ha ben evidenziato le finalità perseguite dal sistema, i ruoli dei soggetti coinvolti nonché ha offerto una opportuna analisi del ciclo di vita del trattamento con indicazione delle misure in essere e pianificate e dei dispositivi utilizzati, comprendendo altresì nella valutazione la descrizione tecnica fornita dal Responsabile esterno.

Si rileva, poi, che il periodo di conservazione individuato per lo specifico trattamento è pari a 7 giorni.

A riguardo, il Titolare ha considerato attentamente il termine indicato. Il Titolare, infatti, ha richiamato opportunamente il Provvedimento del Garante in materia di videosorveglianza, dando atto dell'orientamento ivi indicato e delle diverse finalità a cui l'Autorità dà rilievo.

Dopo un'attenta valutazione sul periodo di conservazione che ha portato altresì il raffronto tra differenti soluzioni, il Titolare ha riscontrato l'impossibilità nel concreto di ridurre il termine di conservazione in esame in quanto – viene rappresentato – che l'adeguato monitoraggio delle immagini non potrebbe essere assicurato diversamente a causa delle risorse presenti attualmente nell'Ente.

Il Titolare ha ritenuto di dar altresì lettura ampia al concetto di sicurezza urbana, individuando quale componente della stessa anche il contrasto di situazioni di degrado ambientale particolarmente pericolose per la sicurezza dei cittadini.

Si dà atto, inoltre, che la DPIA è stata elaborata in un'ottica di collaborazione col D.P.O., il quale ha già preso visione di quanto indicato nella stessa.

A parere del DPO, il trattamento può essere implementato.

Si raccomanda una revisione periodica ad un anno dalla redazione finale della Valutazione, salvo modifiche al trattamento che impongano una integrazione e/o revisione in termini minori.