Città di Palmanova

Regione Friuli-Venezia Giulia
Servizio Associato di Polizia Locale
"Palma Torre"
Comuni di Palmanova, Chiopris-Viscone e Visco
Sede Comando
Piazza Grande n. 1- 33057 Palmanova - tel. 0432/928710 fax 0432/923346
E-mail: polizia.municipale@comune.palmanova.ud.it
PEC: comune.palmanova@certgov.fvg.it
C.F. - P. IVA 00249070301

COMUNE DI VISCO

DATA PROTECTION IMPACT ASSESTMENT (DPIA)

Nome della PIA: Valutazione sul sistema di videosorveglianza cittadino

Nome autore: dott. Roberto Fazio

Data di creazione: 17.01.2024

Nome del DPO/RDP: dott. Gilberto Ambotta

Richiesta del parere degli interessati: non è stato chiesto il parere degli interessati

Motivazione della mancata richiesta del parere degli interessati: non si ritiene opportuno procedere alla richiesta di alcun parere agli interessati

INTRODUZIONE

A partire dalla data del 25 maggio 2018 il nuovo Regolamento UE 2016/679 *("General Data Protection Regulation"* o "*GDPR*") relativo al trattamento dei dati personali nonché alla loro circolazione è pienamente applicabile. Il Regolamento, nella piena applicazione del nuovo principio ispiratore della *"accountability"* impone al titolare del trattamento l'azione di tutte le misure necessarie finalizzate a garantire la protezione e la sicurezza dei dati trattati.

Fra esse, vi è la previsione dell'art. 35 del GDPR dello svolgimento di una valutazione preventiva (Data Protection Impact Assestment – DPIA) sui trattamenti eseguiti e l'impatto di essi sulla libertà e i diritti delle persone fisiche, specificamente nell'ambito di utilizzazione dei sistemi di videosorveglianza.

Il presente documento rappresenta gli esiti della DPIA svolta nell'ambito dei sistemi di videosorveglianza utilizzati dal Comune di Visco finalizzati al raggiungimento di obiettivi relativi a **SICUREZZA MOBILITA' VEICOLARE E PEDONALE, SICUREZZA STRADALE, PUBBLICA SICUREZZA, PREVENZIONE REATI ED ILLECITI AMBIENTALI, POLIZIA GIUDIZIARIA.**

CONTESTO

PANORAMICA DEL TRATTAMENTO

Quale è il trattamento in considerazione?

Le operazioni di trattamento dati che il Comune di Visco esegue sul territorio attraverso i diversi sistemi di videosorveglianza, perseguono le seguenti finalità:

- Vigilanza sulla sicurezza stradale e della mobilità veicolare e pedonale;
- Svolgimento di funzioni di pubblica sicurezza;
- Vigilanza e prevenzione reati ed illeciti ambientali;
- Attività di Polizia Giudiziaria.

L'attività di videosorveglianza eseguita dal Comune di Visco è esercitata per lo svolgimento di funzioni e poteri pubblici, e il raggiungimento delle finalità istituzionali come sopra rappresentate e precisate, consentendo quindi di garantire ai cittadini il rispetto delle regole civili, penali ed amministrative nonché di civile educazione che consentono la normale convivenza e coabitazione nella condivisione di uno spirito di reciproco rispetto e di rispetto per le istituzioni e le loro funzioni.
I sistemi di videosorveglianza utilizzati dal Comune di Visco sono infatti proporzionati ed efficaci rispetto alle finalità prefissate, e sono tali da non comportare rischi ultronei rispetto a quelli inseriti nel contesto di normale funzionalità dei sistemi tecnologici delle tipologie in uso, avuto anche riguardo alla utilizzazione dei medesimi strumenti anche in altri contesti urbani, considerazione che consente di accrescere la fiducia e la credibilità degli strumenti stessi.
Gli strumenti tecnologici in uso sono i seguenti:

1) Sistema di videosorveglianza con telecamere fisse posizionate sul territorio, finalizzato al presidio del territorio stesso nonché alla vigilanza del traffico veicolare e pedonale, anche con dispositivi idonei alla lettura targhe;
2) Sistema di sorveglianza ambientale con "fototrappole" amovibili posizionate in prossimità dei luoghi destinati al gettito di rifiuti ovvero in aree presso le quali è stato rilevato ovvero potrebbe verificarsi il gettito irregolare e abusivo di rifiuti;

In aggiunta a quelli attualmente in uso, si prevede la possibilità di aggiungere in futuro una o più delle seguenti strumentazioni:
1) "dash cam" posizionate all'interno dei veicoli di servizio della Polizia Locale;
2) "body cam" sui giubbotti di servizio del personale della Polizia Locale;
3) Droni.

Quali sono i soggetti coinvolti e le responsabilità connesse al trattamento?
I soggetti coinvolti nell'attività di trattamento sono:

a) il referente privacy verrà individuato con apposito atto formale da parte del Titolare del trattamento;
b) tutti gli operatori designati al trattamento dei dati;
c) la società esterna titolare del contratto di manutenzione dell'impianto.

Ci sono standard applicabili al trattamento?

Attualmente non esistenti per la videosorveglianza

DATI, PROCESSI E RISORSE DI SUPPORTO

Quali sono i dati trattati?

I dati trattati consistono in immagini e video registrati sul piano operativo; la registrazione è attiva sulle 24 ore e le immagini registrate vengono salvate dal personale incaricato solamente qualora vi sia una situazione di particolare criticità che necessita la documentazione video degli eventi.

Qual è il ciclo di vita del trattamento dei dati?

Il trattamento dei dati personali è effettuato a seguito dell'attivazione di tutti gli impianti/sistemi/presidi di videosorveglianza presenti installati sul territorio comunale.

Le immagini vengono registrate su un server ubicato all'interno della sede comunale di Visco. L'accesso al server, tramite una connessione protetta, potrà essere reso possibile anche ad Enti terzi, previa sottoscrizione di specifici accordi di contitolarità.

La disponibilità tempestiva di immagini costituisce uno strumento di prevenzione e di razionalizzazione dell'azione del personale dislocato sul territorio comunale, anche in raccordo con altre Forze dell'Ordine; attraverso tali strumenti l'Ente persegue l'intento di tutelare la popolazione ed il patrimonio comunale, garantendo quindi un elevato grado di sicurezza nel centro storico e nelle strade ad intenso traffico veicolare.

A tal fine il Comune, previa intesa o su richiesta della Autorità di Pubblica Sicurezza e degli organi di Polizia, dispone l'utilizzo del sistema di videosorveglianza in dotazione, compresi i sistemi di lettura targa, ai fini di prevenzione e repressione di atti delittuosi anche nell'ambito del più ampio concetto di "sicurezza urbana", così individuata secondo il Decreto Ministero Interno 5 agosto 2008 e dal Decreto Legge 20 febbraio 2017, n. 14 recante "Disposizioni urgenti in materia di sicurezza delle città" convertito con Legge n. 48/2017.

Tutto il sistema di videosorveglianza comporterà esclusivamente il trattamento di dati personali rilevati mediante le riprese video e che, in relazione ai luoghi di installazione delle videocamere, interessano i soggetti ed i mezzi di trasporto che transiteranno nell'area interessata.

L'attività di videosorveglianza raccoglie esclusivamente i dati strettamente necessari per il raggiungimento delle finalità succitate, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando quando non indispensabili immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza.

L'uso dei dati personali nell'ambito di cui trattasi non necessita del consenso degli interessati in quanto viene effettuato per lo svolgimento di funzioni istituzionali che sono assoggettate alla normativa vigente in materia di "privacy" con un'apposita regolamentazione.

Quali sono le risorse di supporto ai dati?

Sistema di videosorveglianza urbana e sistema di lettura targhe: le immagini vengono gestite da un server collegato ad internet, ma con specifiche regole di accesso alle porte fissate da INSIEL che ne impediscono la fruizione ordinaria.

Fototrappole: le immagini vengono salvate all'interno della fototrappola su una SD-card.

PRINCIPI FONDAMENTALI

PROPORZIONALITA' E NECESSITA'

Gli scopi del trattamento sono specifici, espliciti e legittimi?

La liceità è data dall'art. 6 par. 1 del GDPR in quanto "il trattamento 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".

Il trattamento avviene altresì a fini di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, ai sensi dell'art. 1 comma 2 del D. Lgs. 18 maggio 2018, n. 51 "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2106, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

Il Comune di Visco effettua il trattamento di dati personali mediante impianti di videosorveglianza urbana, sia di osservazione che di contesto, ed altri sistemi di ripresa immagini di dati personali quali telecamere per lettura targhe e fototrappole; possono essere altresì previsti altri sistemi di videosorveglianza come sopra specificato.

In particolare, l'uso di tutti i sistemi e tipologie di videosorveglianza del territorio comunale è finalizzato a:

a) tutelare la sicurezza urbana di cui alle Legge n. 38/2009 e ss.mm.ii., Decreto del Ministero dell'Interno del 5 agosto 2008 e Decreto Legge 20 febbraio 2017, n. 14 nonché secondo le modalità previste dal capitolo n. 5.1 del provvedimento del Garante Privacy in materia di videosorveglianza datato 08.04.2010;
b) prevenire e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale secondo le modalità previste dal capitolo n. 5.1 del provvedimento del Garante Privacy in materia di videosorveglianza datato 08.04.2010;
c) tutelare gli immobili di proprietà o in gestione dell'Amministrazione Comunale ed a prevenire eventuali atti di vandalismo o danneggiamento;
d) controllare determinate aree e/o specifici siti comunali potenzialmente esposti a rischio di vandalismo o danneggiamento quali, a mero titolo esemplificativo, parchi, impianti sportivi e strutture ludico-ricreative;
e) al monitoraggio del traffico veicolare, al fine di prevenire o gestire problematiche inerenti la viabilità;
f) a tutelare in particolare coloro che più necessitano di attenzione: bambini, giovani e anziani, garantendo un elevato grado di sicurezza nelle aree urbane anche per le finalità previste dal "Decreto Sicurezza" approvato con Decreto Legge 23 febbraio 2009, n. 11 e convertito con Legge 23 aprile 2009, n. 38 (atti sessuali con minorenni, violenza sessuale di gruppo e atti persecutori);
g) controllare ad accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose nonché per monitorare il rispetto delle disposizioni concernenti modalità, tipologie di rifiuti scaricati ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (art. 13 Legge 24 novembre 1981, n. 689), secondo le previsioni di cui al capitolo n. 5.2 del Provvedimento del Garante Privacy in materia di videosorveglianza datato 08.04.2010;
h) prevenire eventuali atti di vandalismo e/o danneggiamento ovvero spaccio di sostanze stupefacenti presso istituti scolastici in casi di stretta indispensabilità ed attivando gli impianti interni esclusivamente negli orari di chiusura degli istituti secondo le modalità previste dal capitolo n. 4.3 del Provvedimento del Garante Privacy in materia di videosorveglianza datato 08.04.2010;
i) rilevare violazioni al Codice della Strada, contestate nella immediatezza, mediante l'uso di sistemi OCR (Optical Character Regognition) per riconoscimento delle targhe veicolari;
j) tutelare l'ordine e la sicurezza pubblica e prevenire, accertare e reprimere i reati mediante il controllo dei veicoli in transito; le informazioni delle targhe inserite in "liste di controllo" particolari potranno essere condivise con altre Forze dell'Ordine;
k) supportare operazioni di protezione civile;

Quali sono le basi che rendono lecito il trattamento?

Sulla base di quanto sopra indicato la liceità del trattamento è individuabile ex art. 6 par. 1 lett. E del GDPR, art. 5 del D. Lgs. 18 maggio 2018, n- 51 e art. 23, comma 1, del D.P.R. n. 15 del 2018.

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

In dati vengono raccolti solo per l'attivazione di misure di prevenzione e di tutela della pubblica sicurezza in ambito comunale e per la ricostruzione, in tempo reale, della dinamica di atti vandalici o fatti criminosi o azioni di teppismo nei luoghi pubblici, anche a tutela del patrimonio comunale

I dati sono esatti e aggiornati?

Sì

Qual è il periodo di conservazione dei dati?

Il termine massimo di durata della conservazione dei dati è limitato "ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di conservazione" ai sensi del paragrafo 3.4.3 del provvedimento del 08.04.2010 del Garante Privacy. In relazione alla capacità di immagazzinamento dei dati forniti sui server, in condizioni di normale

funzionamento le immagini riprese in tempo reale si sovrascrivono a quelle registrate, in piena osservanza della normativa vigente sulla privacy.

MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

Come sono informati del trattamento gli interessati?

In ottemperanza al Decreto Legislativo n. 101 del 10.08.2018 nelle zone in cui sono posizionate le telecamere è affissa adeguata segnaletica permanente (cartelli informatori) muniti di pittogramma e recanti la dicitura prevista dallo schema allegato al Provvedimento Generale del Garante per la protezione dei dati personali del 08.04.2010.

È prevista la graduale sostituzione della segnaletica esistente ai sensi delle novità del GDPR e delle linee guida n. 3/2019 EDPB con cartelli conformi alle indicazioni dell'Autorità Garante. Si specifica inoltre che sul sito istituzionale del Comune sarà resa disponibile una informativa di secondo livello relativa al trattamento di dati effettuato tramite l'impianto di videosorveglianza comunale e tramite fototrappole.

Gli interessati sono messi in grado di esercitare i diritti di cui agli artt. 15 e seguenti del GDPR?

In relazione al trattamento dei dati personali è assicurato agli interessati, indentificati o identificabili, l'effettivo esercizio dei propri diritti, in particolare quello di accedere ai dati che li riguardano, di verificarne le finalità, le modalità del trattamento e di ottenere l'interruzione nel caso di utilizzo illecito, in particolare per la carenza dell'adozione delle idonee misure di sicurezza o per l'uso indebito da parte di soggetti non autorizzati.

I diritti di cui al presente articolo riferiti a dati personali concernenti persone decedute possono essere esercitati dagli eredi, da chi abbia un interesse proprio, da chi agisca a tutela dell'interessato o per ragioni familiari considerate particolarmente meritevoli di protezione.

Nell'esercizio dei diritti di cui al primo paragrafo l'interessato può conferire per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da persona di fiducia.

Nel caso di esito negativo alle istanze di cui al presente articolo, 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.

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

Gli obblighi del referente privacy, del responsabile esterno del trattamento, degli incaricati e dei preposti dovranno essere esplicitamente definiti in apposito "Regolamento per la disciplina della videosorveglianza nel territorio comunale di Visco"

I dati sono trasferiti al di fuori del territorio UE?

No

RISCHI

INDISPONIBILITA' DEI DATI (DISTRUZIONE, PERDITA, FURTO)

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

Sistema di videosorveglianza urbana: in caso di sottrazione le immagini potrebbero essere modificate in quanto non crittografate.

Sistema di lettura targhe: in caso di sottrazione le immagini potrebbero essere modificate in quanto non crittografate.

Fototrappole: in caso di sottrazione le immagini potrebbero essere modificate in quanto non crittografate.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Sistema di videosorveglianza urbana: il sistema è connesso ad internet, sebbene siano accessibili solo alcune delle porte con specifiche regole, quindi ci possono essere vulnerabilità sia "logiche" che fisiche, dovute all'ingresso presso l'ambiente in cui si trova il server, presso i locali server di eventuali enti terzi con i quali siano stati sottoscritti accordi di contitolarità per il trattamento dati o presso un armadietto stradale.

Sistema di lettura targhe: il sistema è connesso ad internet, sebbene siano accessibili solo alcune delle porte con specifiche regole, quindi ci possono essere vulnerabilità sia "logiche" che fisiche, dovute all'ingresso presso l'ambiente in cui si trova il server, presso i locali server di eventuali enti terzi con i quali siano stati sottoscritti accordi di contitolarità per il trattamento dati o presso un armadietto stradale.

Fototrappole: qualora la fototrappola venisse trafugata, verrebbero perse anche le immagini salvate sulla SD-card.

Quali sono le fonti di rischio?

Vedi capo precedente

Quali misure tra quelle individuate contribuiscono a mitigare il rischio?

I soggetti "autorizzati" a trattare i dati di videosorveglianza sono nominati con specifici atti, come da Regolamento comunale, e sono istruiti e formati sul corretto trattamento.

L'accesso al locale server all'interno del palazzo municipale di persone non dipendenti è permesso solo dopo l'identificazione, e queste sono accolte da un dipendente in servizio. Per i locali server di enti terzi con i quali dovessero essere stati sottoscritti accordi di contitolarità varranno le misure di mitigazione previste dai propri regolamenti interni.

Molte delle funzionalità di controllo degli accessi possono essere abilitate o disabilitate in base alle esigenze o possono essere modificate per soddisfare un livello specifico di rischio. Le impostazioni predefinite per queste funzionalità di sicurezza sono state scelte per fornire un forte livello di sicurezza, pur mantenendo flessibilità e praticità.

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

Si ritiene il livello di rischio **Basso.**

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

Si ritiene la circostanza **Improbabile.**

INTEGRITA' DEI DATI (ALTERAZIONE, MODIFICA)

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

Sistema di videosorveglianza urbana: le immagini NON sono soggette a crittografazione.

Sistema di lettura targhe: le immagini NON sono soggette a crittografazione.

Fototrappole: le immagini NON sono soggette a crittografazione.

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

Per poter modificare i video le persone che si volessero cimentare dovrebbero possedere una tecnologia molto avanzata.

Quali sono le fonti di rischio?

Sistema di videosorveglianza urbana: le fonti di rischio sono legate ad un accesso abusivo presso il locale server nel palazzo municipale o presso un armadio stradale oltre che ad un accesso tramite internet. In caso di accordo di contitolarità dei dati, esiste una fonte di rischio collegata all'ente terzo cui viene eventualmente concesso l'accesso ai dati trattati.

Sistema di lettura targhe: le fonti di rischio sono legate ad un accesso abusivo presso il locale server nel palazzo municipale o presso un armadio stradale oltre che ad un accesso tramite internet. In caso di accordo di contitolarità dei dati, esiste una fonte di rischio collegata all'ente terzo cui viene eventualmente concesso l'accesso ai dati trattati.

Fototrappole: le fonti di rischio sono legate alla trafugazione dell'intera fototrappola con annessa SD-Card.

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

Per impedire a potenziali malintenzionati l'accesso al server ubicato nei locali del sottotetto del palazzo municipale, verrà realizzato un ambiente con pareti in cartongesso con una porta chiusa a chiave, che sarà messa nella disponibilità del referente privacy e dei suoi delegati.

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

Il rischio viene valutato come **Basso.**

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

La stima individua l'evento come **Improbabile.**

RISERVATEZZA DEI DATI (ACCESSO ABUSIVO, TRATTAMENTO NON CONFORME)

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

In caso di accesso illegittimo alle immagini si ritiene che il danno sarebbe limitato, in quanto il soggetto prenderebbe semplicemente visione delle immagini registrate.

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

Accesso abusivo al server o accesso abusivo presso il palazzo municipale.

Quali sono le fonti di rischio?

Accesso tramite internet o accesso abusivo presso il palazzo municipale.

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

Il locale server è chiuso a chiave. Restano validi i normali strumenti predisposti dal Comune per impedire l'accesso alla sede municipale a soggetti non autorizzati.

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

Il rischio viene valutato come **Basso.**

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

La stima individua l'evento come **Improbabile**.

PIANO D'AZIONE

MISURE E PROCEDURE ADOTTATE O PROGRAMMATE PER LA MITIGAZIONE DEI RISCHI

Attualmente si ritiene che le misure di mitigazione dei rischi attualmente adottate siano adeguate.

Parere del DPO:

L'analisi di cui sopra risulta conforme alle caratteristiche del trattamento ed adeguata.

L'autore

Il Comandante

Dott. Roberto FAZIO

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: FAZIO ROBERTO
CODICE FISCALE: FZARRT78A19L483K
DATA FIRMA: 20/03/2024 12:59:42
IMPRONTA: 4968460482F0247D43E8E5333FD7F49E6C26C6B926749A454C36BB805CFE92F7
6C26C6B926749A454C36BB805CFE92F7FC3521445838EF5CBA358EE06FB53AF5
FC3521445838EF5CBA358EE06FB53AF59C9B89C420124A0562D6592AB14C3363
9C9B89C420124A0562D6592AB14C336327989602662O3B998081011FAD06E02A

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: GORI MARICA
CODICE FISCALE: GROMRC70B44G284T
DATA FIRMA: 28/05/2024 13:28:50
IMPRONTA: 5DB6A899155343F6A1C04ED238E82E29C56372CBA5EE6C5D4EF4B0A0905AE90D
C56372CBA5EE6C5D4EF4B0A0905AE90D96CD5E5FB67EEFECED6F7526216F0250
96CD5E5FB67EEFECED6F7526216F0250FB6E8A824D4BDA0FEAA9A5B5484AD480
FB6E8A824D4BDA0FEAA9A5B5484AD4804D4F1A6803CAC35A0C0EC31BCD5186F8