COMUNE DI MARANO DI NAPOLI

Città Metropolitana di Napoli

DELIBERAZIONE DELLA GIUNTA COMUNALE

ORIGINALE

Numero 104 del 27.12.2024

Oggetto: Approvazione della valutazione di impatto sulla protezione dei dati (DPIA) ai sensi del Regolamento UE n. 679/2016,in relazione al trattamento dei dati tramite sistemi videosorveglianza.

L'anno 2024 il giorno **ventisette** del mese di **DICEMBRE** alle ore **11:20** nella sede municipale si è riunita la Giunta Comunale, nelle forme di legge, nelle persone dei sigg.ri:

COGNOME	NOME	QUALIFICA	P	A
MORRA	Matteo	Sindaco	x	
CARANDENTE	Luigi	Vice Sindaco	x	
ALBANESE	Carlo	Assessore	x	
BOCCHETTI	Carmela	Assessore		x
CARANDENTE	Carmine	Assessore	x	
LIBERTI	Giuseppina	Assessore	x	
POLICHETTI	Gennaro	Assessore	x	
RUSSO	Concetta	Assessore	x	

Il Presidente constatata la legalità dell'adunanza, dichiara aperta la seduta ed invita i presenti a deliberare sulla proposta di cui all'oggetto.

Partecipa alla seduta il Segretario Generale dott.ssa Giovanna Imparato

Proposta di Delibera di Giunta Comunale

Su proposta dell'Assessore alla Sicurezza Urbana, dott. Carlo Albanese

Rilevato che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale é un diritto fondamentale e che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;

Considerato che le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche, tenuto conto che la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali in considerazione, in particolare, di quanto segue:

- la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo;
- la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano;
- la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali;

Tenuto presente che tale evoluzione ha indotto l'Unione europea ad adottare il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito solo "GDPR");

Dato atto che il 24 maggio 2016 è entrato ufficialmente in vigore il GDPR, il quale è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;

Rilevato che, con il GDPR, è stato richiesto agli Stati membri:

- un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, data l'importanza di creare il clima di fiducia funzionale allo sviluppo dell'economia digitale in tutto il mercato interno;

Visto il D. lgs 196/2003, modificato dal D.Lgs. 10 agosto 2018 n. 101;

Dato atto che, quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il GDPR obbliga i titolari a svolgere:

- una "determinazione preliminare della possibilità che il trattamento possa presentare un rischio elevato" in base alla quale stabilire se un trattamento può, anche solo teoricamente, presentare un rischio elevato;
- una valutazione di impatto nel caso in cui la determinazione preliminare restituisca l'accertamento della teorica possibilità che il trattamento possa presentare un rischio elevato;

Tenuto presente che la DPIA è una procedura prevista dall'art. 35 del Regolamento UE 206/679 (RGDP) che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonchè i relativi rischi, allo scopo di approntare misure idonee ad affrontarli;

Tenuto presente l'obbligo, in capo ai titolari, di consultare l´Autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato;

Rilevato che la DPIA deve essere condotta prima di procedere al trattamento e che, deve comunque essere previsto un riesame continuo della DPIA, ripetendo la valutazione a intervalli regolari;

Dato atto che la responsabilità della DPIA spetta al titolare, anche se la conduzione materiale della valutazione di impatto può essere affidata ad un altro soggetto, interno o esterno all'organizzazione;

Tenuto presente che, ferma restando la discrezionalità dell'amministrazione nell'effettuare la determinazione preliminare e la valutazione di impatto, il Garante, con provvedimento n. 467 dell'11 ottobre 2018, ha reso pubblico l'Elenco delle tipologie di trattamenti da sottoporre OBBLIGATORIAMENTE a valutazione d'impatto, tra cui si menzionano:

1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato";

2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi);

3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.;

4. Trattamenti su larga scala di dati aventi carattere estremamente personale: si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti);

5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8);

6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo);

7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01;

8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.

9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment);

10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.

11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento

Tenuto presente che, ai sensi dell'art. 29 delle linee guida elaborate dal Gruppo di Lavoro 29 per la protezione dei dati, la DPIA, non è necessaria per i trattamenti che:

- non presentano rischio elevato per diritti e libertà delle persone fisiche
- hanno natura, ambito, contesto, e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni non hanno subito modifiche
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA
- fanno riferimento a norme e regolamenti per la cui definizione è stata condotta una DPIA

Rilevato che, per quanto sopra, e' necessario istituire:

1. una "Determinazione preliminare della possibilità che il trattamento possa presentare un rischio elevato" in base alla quale stabilire se un trattamento può, anche solo teoricamente, presentare un rischio elevato;
2. una valutazione di impatto nel caso in cui la determinazione preliminare restituisca l'accertamento della teorica possibilità che il trattamento possa presentare un rischio elevato;

Dato atto che il responsabile del procedimento, relativamente al trattamento dei dati tramite sistemi di videosorveglianza è il Comandante della Polizia Municipale, e che lo stesso, al fine di garantire la massima diffusione interna ed esterna e la massima conoscibilità dei trattamenti oggetto di DPIA, nonché delle misure tecniche e organizzative individuate dai titolari per mitigare l´impatto del trattamento, è tenuto a garantire la conoscibilità della Valutazione d'impatto sulla protezione dei dati (DPIA) a tutti i dipendenti dell'Ente;

Dato atto che il procedimento di adozione e approvazione della Valutazione d'impatto sulla protezione dei dati (DPIA) e il presente provvedimento, risultano mappati dal PTPC e che sono stati

effettuati i controlli previsti dal Regolamento Sistema controlli interni ed è stato rispettato quanto previsto dal Piano Triennale di Prevenzione della corruzione e dal Programma per la trasparenza;
Visti:

- D.Lgs. 267/2000;
- Legge 241/1990;
- D.Lgs. 196/2003;
- Legge 190/2012;
- D.Lgs. 33/2013;
- Regolamento (UE) n. 679/2016;
- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
- Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida sul diritto alla "portabilità dei dati" - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e pro lazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Parere del WP29 sulla limitazione della finalità - 13/EN WP 203;
- Statuto Comunale;
- Regolamento di organizzazione degli uffici e dei servizi;
- Regolamento sul trattamento dei dati sensibili;
- Codice di comportamento interno dell'Ente;
- Circolari e direttive del RPC;

Propone

per le ragioni indicate in narrativa, e che qui si intendono integralmente richiamate:
1. di approvare la Valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi del Regolamento (UE) n.679/2016, allegata alla presente, per formarne parte integrante e sostanziale;
2. Di disporre che al presente provvedimento venga assicurata:
a) la pubblicità legale con pubblicazione all'Albo Pretorio;
b) la trasparenza mediante la pubblicazione sul sito web istituzionale, secondo criteri di facile accessibilità, completezza e semplicità di consultazione nella sezione "Amministrazione trasparente", sezione di primo livello "Disposizioni generali" sezione di secondo livello "Atti generali";
3. Di dare atto che, oltre quanto già previsto in ordine alla pubblicazione del provvedimento de quo, chiunque ha diritto, ai sensi dell'art. 5 comma 2 D.Lgs. 33/2013, di accedere ai dati e ai documenti ulteriori rispetto a quelli oggetto di pubblicazione, ai sensi del citato D.Lgs. 33/2013, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis del medesimo decreto.
4. Di disporre che la pubblicazione dei dati, delle informazioni e dei documenti avvenga nella piena osservanza delle disposizioni previste dal D.Lgs. 196/2003 e, in particolare, nell'osservanza di

quanto previsto dall'articolo 19, comma 2 nonché dei principi di pertinenza, e non eccessività dei dati pubblicati e del tempo della pubblicazione rispetto ai fini perseguiti.
5. Di dichiarare, con separata ed unanime votazione, il presente provvedimento immediatamente eseguibile ai sensi dell'articolo 134, comma 4, del decreto legislativo 18 agosto 2000, n. 267, in ragione dell'esigenza di celerità correlate dei procedimenti amministrativi.

L'Assessore alla Sicurezza Urbana

dott. Carlo Albanese

LA GIUNTA COMUNALE

Visti i pareri favorevoli espressi dall'Ing. Giovanni Napoli in qualità di Responsabile del Settore Lavori Pubblici e dalla dott.sa Maria Silvia De Luca, in qualità di Comandante della Polizia Municipale, in ordine alla regolarità tecnica nonché dal dott. Renato Spedaliere, in qualità di Responsabile dei Servizi Finanziari, in ordine alla regolarità contabile del presente atto (art. 49, 1° comma, D.Lgs. 267/2000);

DELIBERA

1. di approvare la Valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi del Regolamento (UE) n.679/2016, allegata alla presente, per formarne parte integrante e sostanziale;
2. Di disporre che al presente provvedimento venga assicurata:
a) la pubblicità legale con pubblicazione all'Albo Pretorio;
b) la trasparenza mediante la pubblicazione sul sito web istituzionale, secondo criteri di facile accessibilità, completezza e semplicità di consultazione nella sezione "Amministrazione trasparente", sezione di primo livello "Disposizioni generali" sezione di secondo livello "Atti generali";
3. Di dare atto che, oltre quanto già previsto in ordine alla pubblicazione del provvedimento de quo, chiunque ha diritto, ai sensi dell'art. 5 comma 2 D.Lgs. 33/2013, di accedere ai dati e ai documenti ulteriori rispetto a quelli oggetto di pubblicazione, ai sensi del citato D.Lgs. 33/2013, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis del medesimo decreto.
4. Di disporre che la pubblicazione dei dati, delle informazioni e dei documenti avvenga nella piena osservanza delle disposizioni previste dal D.Lgs. 196/2003 e, in particolare, nell'osservanza di quanto previsto dall'articolo 19, comma 2 nonché dei principi di pertinenza, e non eccessività dei dati pubblicati e del tempo della pubblicazione rispetto ai fini perseguiti.
5. Di dichiarare, con separata ed unanime votazione, il presente provvedimento immediatamente eseguibile ai sensi dell'articolo 134, comma 4, del decreto legislativo 18 agosto 2000, n. 267, in ragione dell'esigenza di celerità correlate dei procedimenti amministrativi.

COMUNE DI MARANO DI NAPOLI
Città Metropolitana di Napoli

PROPOSTA DI DELIBERAZIONE
(X) GIUNTA COMUNALE ( ) CONSIGLIO COMUNALE

Proponente:
Assessore alla Sicurezza Urbana

Oggetto: **Approvazione della valutazione di impatto sulla protezione dei dati (DPIA) ai sensi del Regolamento UE n. 679/2016, in relazione al trattamento dei dati tramite sistemi di videosorveglianza**

Ai sensi dell'art.49 del D.Lgs. 267/00, che testualmente recita:
1. Su ogni proposta di deliberazione sottoposta alla Giunta e al Consiglio che non sia mero atto di indirizzo deve essere richiesto il parere, in ordine alla sola regolarità tecnica, del responsabile del servizio interessato e, qualora comporti riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'ente, del responsabile di ragioneria in ordine alla regolarità contabile. I pareri sono inseriti nella deliberazione.
2. Nel caso in cui l'ente non abbia i responsabili dei servizi, il parere è espresso dal segretario dell'ente, in relazione alle sue competenze.
3. I soggetti di cui al comma 1 rispondono in via amministrativa e contabile dei pareri espressi.
Sulla proposta di deliberazione i sottoscritti esprimono il parere di cui al seguente prospetto:

IL RESPONSABILE SETTORE LL.PP. Ing. Giovanni Napoli	Per quanto concerne **la regolarità tecnica** esprime parere: ☒ **FAVOREVOLE** ☐ **CONTRARIO** Data _____ Il Responsabile
IL COMANDANTE UNITA' DI STAFF - COMANDO POLIZIA MUNICIPALE Cap. De Luca Dott.ssa Maria Silvia	Per quanto concerne **la regolarità tecnica** esprime parere: ☒ **FAVOREVOLE** ☐ **CONTRARIO** Data _____ Il Responsabile
IL RESPONSABILE SETTORE Servizi economico-finanziario Dr. Renato Spedaliere	Per quanto concerne **la regolarità contabile** esprime parere: ☒ **FAVOREVOLE** ☐ **CONTRARIO** Data _____ Il Responsabile

COMUNE DI MARANO DI NAPOLI

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

- Ente: Comune di Marano di Napoli
- Titolare: Sindaco Dott. Matteo Morra
- Responsabile Trattamento Dati: Comandante Polizia Municipale, Dott.ssa Maria Silvia De Luca
- Responsabile Trattamento Dati: Responsabile LLPP, Ing. Giovanni Napoli
- Responsabile Protezione Dati: Ing. Armando Lucci

Maggio 2024

INDICE

INTRODUZIONE

A partire dalla data del 25 maggio 2018 il nuovo Regolamento UE 2016/679 ("General Data Protection Regulation") 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'adozione di tutte le misure necessarie finalizzate a garantire la protezione e la sicurezza dei dati trattati.

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

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

DEFINIZIONI

Probabilità: valutazione della frequenza con la quale si verifica una minaccia funzionalmente alle vulnerabilità presenti e delle eventuali misure di contenimento adottate;

Impatto: rappresentazione del grado di gravità dell'incidente che comporta compromissione della riservatezza, integrità e disponibilità dei trattamenti e dei dati ad essi relativi;

Minaccia: evento potenziale, cagionato ovvero accidentale, che comporterebbe il danno all'interessato;

Vulnerabilità: elemento di debolezza presente all'interno del sistema informativo o informatico sfruttabile dalla minaccia per la produzione del danno;

Contromisure: soluzioni organizzative, tecnologiche o procedurali finalizzate alla diminuzione del rischio;

PREVISIONE NORMATIVA E CONTENUTI DELLA DPIA

La presente valutazione viene svolta in conformità alle disposizioni del reg. UE 2016/679 e da quelle contenute dal D.Lgs.n.196/2003 così come modificate dal D.Lgs. n.101/2018.

L'art. 35 del Reg. UE 2016/679 prevede lo svolgimento della DPIA il cui contenuto minimo deve essere (par.7 art.35):

1. descrizione dei trattamenti previsti, delle loro finalità incluso l'interesse legittimo del Titolare, ove applicabile ai trattamenti da eseguirsi;

2. valutazione della necessità e proporzionalità dei trattamenti eseguiti in relazione alle finalità perseguite;

3. valutazione dei rischi per le libertà ed i diritti degli interessati;

4. misure previste/approntate per le prevenzioni dei rischi.

La presente valutazione viene svolta dal Titolare del trattamento del Comune di Marano di Napoli, il Sindaco Dott. Matteo Morra con il supporto del Responsabile per la Protezione Dati del Comune di Marano di Napoli, Ing. Armando Lucci e si riferisce alla valutazione dei rischi in cui potrebbero incorrere le libertà ed i diritti dei cittadini nel corso dell'utilizzazione da parte del Comune dei sistemi di videosorveglianza da esso complessivamente attivati.

AMBITO DEI TRATTAMENTI E TRATTAMENTI ESEGUITI

Le operazioni di trattamento dati che il Comune di Marano di Napoli 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 Marano di Napoli è esercitata per lo svolgimento di funzioni e poteri pubblici ed 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 delle Istituzioni e delle loro funzioni.

I sistemi di videosorveglianza utilizzati dal Comune di Marano di Napoli sono, infatti, proporzionati ed efficaci rispetto alle finalità prefissate e sono tali da non comportare rischi ultronei rispetto a quelli inseriti in un 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 questa che consente di accrescere la fiducia e la credibilità degli strumenti stessi.

Gli strumenti tecnologici in uso sono i seguenti così come meglio rappresentati nelle schede tecniche allegate:

1) sistema di videosorveglianza con telecamere fisse posizionate agli accessi all'area urbana e nel territorio, finalizzata al presidio del territorio stesso nonché alla vigilanza del traffico veicolare e pedonale, anche con dispositivi idonei alla lettura targhe;

2) sistema di videosorveglianza 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;

SOLUZIONI TECNOLOGICHE ADOTTATE

Gli strumenti adottati per l'esecuzione della videosorveglianza sono quelli le cui schede tecniche sono allegate al presente documento, fatta eccezione per la videosorveglianza partecipata la cui valutazione di impatto verrà successivamente eseguita. Le schede tecniche allegate al presente documento sono le seguenti:

1) HIKVISION DS-2CD1743G0-I(Z) 4 MP Varifocal Dome Network Camera;

2) HIKVISION DS-2CD2646G2-IZS 4 MP AcuSense Powered-by-DarkFighter Motorized Varifocal Bullet Network Camera;
3) VIGILATE V-LANE A2B 2MP@60fps 250 Km/h (1 Corsia).

DURATA DEL TRATTAMENTO

Il trattamento dei dati rilevati attraverso i sistemi di videosorveglianza saranno conservati per il termine massimo di giorni 7 (sette) salvo il caso in cui, per atto delle AA.GG. competenti, venga disposta la proroga del predetto termine di conservazione. La previsione del termine di giorni 7 (sette) per la conservazione dei dati raccolti, è stata determinata sulla base dei criteri di necessità, proporzionalità, pertinenza e non eccedenza ed anche sulle modalità organizzative dell'orario lavorativo e dell'impiego del personale del Settore Polizia Locale del Comune di Marano di Napoli avuto riguardo all'efficienza ed efficacia dell'azione amministrativa di cui all'art. 97 Cost. it.

DATI INTERESSATI AL TRATTAMENTO

I dati interessati dal trattamento eseguito dai sistemi di videosorveglianza utilizzati dal Comune di Marano di Napoli sono le immagini, i video e le registrazioni degli interessati.

Trattasi, dunque, di dati comuni raccolti esclusivamente per le finalità qui di sopra rappresentate e soggette a cancellazione decorsi i 7 (sette) giorni salvo proroga disposta dalle AA.GG.

MISURE GIURIDICHE DI CONTENIMENTO

1. LIMITAZIONE DELLE FINALITA' il trattamento dei dati acquisiti mediante i sistemi di videosorveglianza in uso al Comune di Marano di Napoli avverrà per le finalità che sono espressamente manifestate nelle informative, nel Regolamento ed in tutti gli altri atti e documenti in cui verranno successivamente rappresentate e ciò in ossequio all'art.5 comma 1 lett.b del Regolamento UE 2016/679;

2. MINIMIZZAZIONE DEI DATI saranno trattati solo ed esclusivamente i dati personali necessari e sufficienti per il raggiungimento delle finalità alla base del trattamento così come previsto dall'art.5 comma 1 lett. c del predetto Regolamento europeo;

3. ESATTEZZA DEI DATI i dati trattati sono esatti d, ove necessario, il Titolare procederà ad eventuale rivisitazione ed aggiornamento;

4. PREVISIONE DI UNA DURATA DELLA CONSERVAZIONE ciò consente all'interessato di maturare la certezza che i propri dati personali sono soggetti ad automatica cancellazione in caso di mancato utilizzo e, comunque, non potranno essere conservati oltre i 7 (sette) giorni previsti salvo proroghe disposte dalle AA.GG.;

5. INFORMATIVA E CAMPAGNE DI SENSIBILIZZAZIONE oltre all'informativa semplificata presente sul sito del Comune di Marano di Napoli, in esso sarà presente anche l'informativa specifica sui sistemi di videosorveglianza. Sarà presente un'informativa succinta contenente i dati essenziali ed il rinvio ai link del sito del Comune di Marano di Napoli ove trovare i documenti completi, anche in ciascuno dei nuovi cartelli appositamente approntati per l'adeguamento dei sistemi di videosorveglianza. Il Comune di Marano di Napoli provvederà con apposita campagna di informazione e sensibilizzazione rivolta alla

cittadinanza per renderla edotta e consapevole della presenza e del funzionamento dei sistemi di videosorveglianza adottati in uso nonché dei propri diritti all'opposizione, all'accesso, alla rettifica nonché tutti gli altri così come previsti dal regolamento europeo.

6. REGOLAMENTI E DISCIPLINARI D'USO tra le misure giuridiche di contenimento, non potrà non trovare luogo l'adozione di nuovo Regolamento comunale adatto ed idoneo a gestire il funzionamento dei sistemi di videosorveglianza anche nelle sue nuove ed innovative formule nonché la relazione tecnica ed il disciplinare vigente per l'utilizzo futuro di "dash cam" e "body cam". All'interno del Regolamento comunale saranno disciplinate le procedure volte ad individuare ed autorizzare il personale che dovrà eseguire i trattamenti, le modalità di accesso ai locali ove sono posizionati i monitor di controllo ed i server posti a servizio dei sistemi di videosorveglianza nonché le modalità di accesso degli interessati ai propri dati personali. Il personale della Polizia Locale autorizzato riceverà atto formale di individuazione con annesse istruzioni impartite e specifica formazione sulla tematica della videosorveglianza.

7. NOMINA DEL RESPONSABILE DEL TRATTAMENTO il Titolare ha provvederà con apposito atto formale alla designazione del Responsabile del Trattamento Dati relativo ai sistemi della videosorveglianza nella persona del Comandante della Polizia Locale Capitano Costa Brigida Aurelia e del Responsabile Lavori Pubblici Ing. Giovanni Napoli, ciascuno per quanto di competenza.

8. REVISIONE RISULTANZE DPIA La DPIA verrà svolta ogniqualvolta venga ad essere sostituito un sistema di videosorveglianza o parti di esso nonché nel caso di ogni modifica al sistema. Verrà, altresì, svolta la Dpia ogni qualvolta il sistema complessivo di videosorveglianza del Comune di Marano di Napoli dovesse essere implementato con sistemi di videosorveglianza privati. In ogni caso, la DPIA dei sistemi di videosorveglianza del Comune di Marano di Napoli verrà eseguita in ragione di anno così da garantire la migliore aderenza e più idonea del sistema alle esigenze di tutela dei dati personali degli interessati nel rispetto delle finalità prefissate ed istituzionali del Comune di Marano di Napoli.

METODOLOGIA DI VALUTAZIONE DELL'IMPATTO PRIVACY

Per la valutazione dell'impatto del trattamento dei dati dell'interessato sulle libertà ed i diritti del medesimo, si è partiti dai contenuti (criteri) del Registro dei trattamenti ex art.30 Reg.UE 2016/679 attribuendo specifiche categorie di rischio:

Criteri	Livello di impatto		
	Alto	**Medio**	**Basso**
Tipologia dati	Dati ex art.9 GDPR	Cittadini Utenti Dipendenti	Fornitori
Categorie interessati	Minori o soggetti svantaggiati		
Finalità trattamento		Videosorveglianza	
Numerosità dati trattati	Maggiore 500K	Tra 500k e 300k	Minore 300k
Trasferimento paesi extra UE	Non previsto	Non previsto	Non previsto
Soluzioni tecnologiche adottate	Immagini ad alta risoluzione	Immagini a bassa risoluzione	Dati anonimizzati

Conseguenza del trattamento	Inibizione dell'esercizio di un diritto o all'utilizzo di un servizio		

RISULTANZE DI SINTESI

Sulla base di quanto sopra, può affermarsi come il Comune di Marano di Napoli attraverso i sistemi di videosorveglianza di cui alla presente DPIA, esegua il trattamento di:

1. categorie di dati personali: comuni

2. categoria di soggetti: cittadini

3. finalità del trattamento: 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;

4. trasferimento verso paesi extra UE: non previsto;

5. conseguenze del trattamento: nessuna inibizione delle libertà o dell'esercizio dei diritti dei cittadini

Da quanto sopra esposto, dall'esperienza quotidiana dei sistemi di videosorveglianza e del loro impatto sulla vita e le abitudini dei cittadini, dalla standardizzazione delle funzionalità e delle capacità operative dei sistemi tecnologici nonché dalle specifiche finalità perseguite con l'utilizzo dei sistemi di videosorveglianza, può sostenersi come l'impatto sulle libertà e l'esercizio dei diritti dei cittadini.

VALUTAZIONE DELLE MINACCE

Minacce	Livello di probabilità
Attacchi informatici	alto
Abusi di privilegi di accesso/utillizzo improprio	alto
Modifica dei dati	medio-basso
Errori nei processi di elaborazione	medio-basso
Perdita dati per guasto/furto/smarrimento hardware	medio-basso
Cancellazione accidentale	medio-basso
Inefficiente gestione del dato	medio-basso

La valutazione delle minacce qui dinanzi rappresentato, si basa su una previsione di massima delle minacce tipo che possono paventarsi nell'ambito dell'utilizzo dei sistemi di videosorveglianza adottati, facendo tuttavia salva la necessità di costante e periodico aggiornamento del presente documento alla luce delle criticità ovvero migliorie tecniche e di utilizzo che possono essere suggerite o rilevate.

La parte relativa all'adozione ed alla gestione delle misure di protezione dei sistemi di videosorveglianza è di competenza dei settori Lavori Pubblici e Comando Polizia Municipale del Comune di Marano di Napoli.

CONCLUSIONI

La considerazione del contesto in cui si sviluppa l'azione dei sistemi di videosorveglianza adottati dal Comune di Marano di Napoli nonché le sue finalità, le modalità con cui avviene il trattamento dei dati e la tipologia dei medesimi e le misure giuridiche di contenimento dei rischi consentono di poter considerare il rischio per le libertà e di diritti dei cittadini di livello complessivo MEDIO-BASSO. Per quanto attiene le misure di sicurezza informatiche, si ritiene che di debba fare un'attività di implementazione dello stato attuale.

Per effetto dell'utilizzo di misure innovative, quali la videosorveglianza partecipata, nonché affinché i sistemi in uso consentano lo svolgimento delle finalità di rilevanza pubblica nel pieno rispetto delle libertà e diritti dei cittadini, la congruità ed adeguatezza della presente Valutazione di Impatto Privacy andrà verificata semestralmente per il primo anno ed ogni volta che dovesse essere rilevata qualche criticità ovvero appalesarsi la necessità di rivalutare l'adeguatezza e la conformità del funzionamento dei sistemi in uso.

Marano di Napoli, li 28/11/2024

Il Titolare

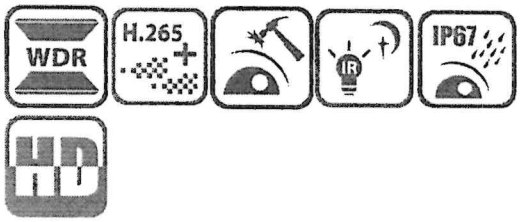
Sindaco Dott. Matteo Morra

Il Responsabile Protezione Dati

Ing. Armando Lucci

HIKVISION

DS-2CD1743G0-I(Z)
4 MP Varifocal Dome Network Camera



- High quality imaging with 4 MP resolution
- Efficient H.265+ compression technology
- Clear imaging even with strong back lighting due to 120 dB WDR
- Up to 256 GB memory card slot for storage
- 2.8 to 12 mm motorized varifocal lens for easy installation and monitoring
- Water and dust resistant (IP67) and vandal proof (IK10)
- EXIR 2.0: advanced infrared technology with long IR range

▪ Specification

Camera	
Image Sensor	1/3" Progressive Scan CMOS
Max. Resolution	2560 × 1440
Min. Illumination	Color: 0.005 Lux @(F1.6, AGC ON), B/W: 0 Lux with IR
Shutter Speed	1/3 s to 1/100,000 s
Wide Dynamic Range	120 dB
Day & Night	IR Cut Filter
Angle Adjustment	Pan: 0° to 355°, tilt: 0° to 70°, rotation: 0° to 355°
Lens	
Lens Type	Varifocal Lens, motoried lens, 2.8 to 12 mm
Focal Length & FOV	2.8 to 12 mm: horizontal FOV 102° to 31°, vertical FOV 54° to 17°, diagonal FOV 123° to 35°
Lens Mount	Ø14
Iris Type	Fixed
Aperture	F1.6
Illuminator	
IR Wavelength	850 nm
IR Range	Up to 30 m
Video	
Main Stream	50 Hz: 20 fps (2560 × 1440) 25 fps (1920 × 1080, 1280 × 720) 60 Hz: 20 fps (2560 × 1440) 30 fps (1920 × 1080, 1280 × 720)
Sub-Stream	50 Hz: 25 fps (1280 × 720, 640 × 480, 640 × 360) 60 Hz: 30 fps (1280 × 720, 640 × 480, 640 × 360)
Video Compression	Main stream: H.265+/H.265/H.264+/H.264 Sub-stream: H.265/H.264/MJPEG
Video Bit Rate	32 Kbps to 8 Mbps
H.264 Type	Baseline Profile/Main Profile/High Profile
H.265 Type	Main Profile
Region of Interest (ROI)	1 fixed region for main stream
Audio	
Audio Compression	-S: G.711ulaw/G.711alaw/G.722.1/G.726/MP2L2/PCM/AAC
Audio Bit Rate	-S: 64 Kbps (G.711)/16 Kbps (G.722.1)/16 Kbps (G.726)/32 to 160 Kbps (MP2L2)/16 to 64 Kbps (AAC)
Audio Sampling Rate	-S: 8 kHz/16 kHz
Environment Noise Filtering	-S: Yes
Network	
Protocols	TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, NTP, UPnP™, SMTP, IGMP, 802.1X, QoS, IPv6, Bonjour, IPv4, UDP, SSL/TLS
Simultaneous Live View	Up to 6 channels
API	Open Network Video Interface, ISAPI
User/Host	Up to 32 users. 3 levels: administrator, operator and user

Network Storage	MicroSD/SDHC/SDXC card (256 GB) local storage
Client	iVMS-4200, Hik-Connect
Web Browser	Plug-in required live view: IE 10+ Plug-in free live view: Chrome 57.0+, Firefox 52.0+ Local service: Chrome 57.0+, Firefox 52.0+
Image	
Image Settings	Saturation, brightness, contrast, sharpness, AGC, white balance adjustable by client software or web browser
Day/Night Switch	Auto, Schedule, Day, Night
Image Enhancement	BLC, 3D DNR
Interface	
Ethernet Interface	1 RJ45 10 M/100 M self-adaptive Ethernet port
On-Board Storage	Built-in memory card slot, support microSD card, up to 256 GB
Audio	-S: 1 input (line in), two-core terminal block, max. input amplitude: 3.3 Vpp, input impedance: 4.7 KΩ, interface type: non-equilibrium 1 output (line out), two-core terminal block, max. output amplitude: 3.3 Vpp, output impedance: 100 Ω, interface type: non-equilibrium
Alarm	-S: 1 input,1 output, max. 12 VDC, 30 mA
Reset Key	Yes
Event	
Basic Event	Motion detection, video tampering alarm, exception
Linkage	Upload to FTP, notify surveillance center, send email, upload to memory card, trigger recording, trigger capture
General	
Power	12 VDC ± 25%, 0.8 A, max. 10 W, Ø5.5 mm coaxial power plug PoE: 802.3af, Class 3, 36 V to 57 V, 0.32 A to 0.2 A, max. 11.5 W
Camera Material	Metal
Camera Dimension	Ø141 mm × 99.9 mm (Ø5.6" × 3.9")
Package Dimension	140 mm × 140 mm × 154 mm (5.5" × 5.5" × 6.1")
Camera Weight	Approx. 820 g (1.8 lb.)
With Package Weight	Approx. 1200 g (2.6 lb.)
Storage Conditions	-30 °C to 60 °C (22 °F to +140 °F). Humidity 95% or less (non-condensing)
Startup and Operating Conditions	-30 °C to 60 °C (22 °F to +140 °F). Humidity 95% or less (non-condensing)
Language	English, Ukrainian
General Function	Anti-flicker, heartbeat, mirror, password protection, privacy mask, watermark, IP address filter
Approval	
EMC	FCC SDoC (47 CFR Part 15, Subpart B); CE-EMC (EN 55032: 2015, EN 61000-3-2: 2014, EN 61000-3-3: 2013, EN 50130-4: 2011 +A1: 2014); RCM (AS/NZS CISPR 32: 2015); IC VoC (ICES-003: Issue 6, 2016); KC (KN 32: 2015, KN 35: 2015)

Safety	UL (UL 60950-1); CB (IEC 60950-1:2005 + Am 1:2009 + Am 2:2013, IEC 62368-1:2014); CE-LVD (EN 60950-1:2005 + Am 1:2009 + Am 2:2013, IEC 62368-1:2014); BIS (IS 13252(Part 1):2010+A1:2013+A2:2015)
Environment	CE-RoHS (2011/65/EU); WEEE (2012/19/EU); Reach (Regulation (EC) No 1907/2006)
Electrical Safety Protection	IP67 (IEC 60529-2013), IK10 (IEC 62262:2002)

▪ Available Model

DS-2CD1743G0-IZS (2.8 to 12 mm)
DS-2CD1743G0-IZ (2.8 to 12 mm)

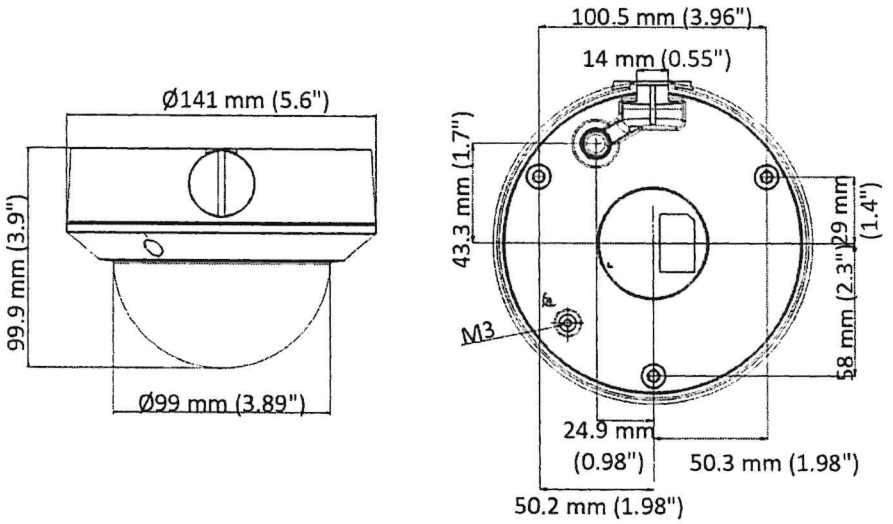
Typical Application

Hikvision products are classified into three levels according to their anti-corrosion performance. Refer to the following description to choose for your using environment.

This model has NO SPECIFIC PROTECTION.

Level	Description
Top-level protection	Hikvision products at this level are equipped for use in areas where professional anti-corrosion protection is a must. Typical application scenarios include coastlines, docks, chemical plants, and more.
Moderate protection	Hikvision products at this level are equipped for use in areas with moderate anti-corrosion demands. Typical application scenarios include coastal areas about 2 kilometers (1.24 miles) away from coastlines, as well as areas affected by acid rain.
No specific protection	Hikvision products at this level are equipped for use in areas where no specific anti-corrosion protection is needed.

▪ Dimension



Unit: mm (inch)

▪ Accessory

▪ Optional

DS-1275ZJ-SUS
Vertical Pole Mount

DS-1276ZJ-SUS
Corner Mount

DS-1258ZJ-L
Wall Mount

DS-1271ZJ-135
Pendant Mount

D20-AP
Adapter Plate

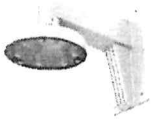
DS-1253ZJ-L
Rain Shade

DS-1250ZJ
Rain Shade

DS-1227ZJ
In-Ceiling Mount

DS-1473ZJ-135B
Wall Mount

DS-1273ZJ-135
Wall Mount



DS-1281ZJ-DM23
Inclined Ceiling Mount

DS-1280ZJ-DM21
Junction Box

HIKVISION

Headquarters
No. 555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
overseasbusiness@hikvision.com

Hikvision USA
T +1-909-895-0400
sales.usa@hikvision.com

Hikvision Europe
T +31-23-5542770
sales.eu@hikvision.com

Hikvision UK & Ireland
T +01628-902140
sales.uk@hikvision.com

Hikvision UAE
T +971-4-4463700
sales.me@hikvision.com

Hikvision Russia
T +7-495-669-67-99
sales.ru@hikvision.com

Hikvision Australia
T +61-2-8599-4033
sales.anz@hikvision.com

Hikvision Italy
T +39-0438-6902
info.it@hikvision.com

Hikvision South Africa
T +27 (10) 035 1777
sales.africa@hikvision.com

Hikvision Singapore
T +65-6684 4718
sales.sg@hikvision.com

Hikvision Korea
T +82 10 3171 7971
sales.kor@hikvision.com

Hikvision India
T +91-22-4041 9900
sales@pramahikvision.com

Hikvision Brazil
T +55 11 3318 0050
vendas.br@hikvision.com

Hikvision France
T +33 (0)1 85 33 89 00
info.fr@hikvision.com

Hikvision Spain
T +34-91-737-16-55
info.es@hikvision.com

Hikvision Poland
T +48 22 460 01 50
info.pl@hikvision.com

Hikvision Canada
T +1-866-200-6690
sales.ca@hikvision.com

Hikvision Turkey
T +90 (216) 521 7070 (Pbx)
sales.tr@hikvision.com

Hikvision Kazakhstan
T +7-727-692-8797
info.kz@hikvision.ru

Hikvision Tashkent
T +998-97-132-6779
uz@hikvision.ru

Hikvision Indonesia
T +62-21-2654-1819
sales.indonesia@hikvision.com

Hikvision Thailand
T +66-2256-4048
sales.th@hikvision.com

Hikvision Malaysia
T +60 3 7652 2413
sales.my@hikvision.com

Hikvision Vietnam
T +84-9742700**
sales.vn@hikvision.com

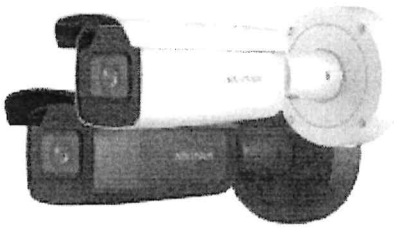
Hikvision Hong Kong
T +852-2151-1761
info.hk@hikvision.com

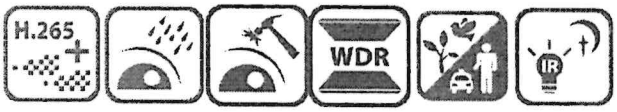
Hikvision Colombia
sales.colombia@hikvision.com

HIKVISION

DS-2CD2646G2-IZS

4 MP AcuSense Powered-by-DarkFighter Motorized Varifocal Bullet Network Camera





Empowered by deep learning algorithms, Hikvision AcuSense technology brings human and vehicle targets classification alarms to front- and back-end devices. The system focuses on human and vehicle targets, vastly improving alarm efficiency and effectiveness.

- High quality imaging with 4 MP resolution
- Excellent low-light performance with powered-by-DarkFighter technology
- Motorized varifocal lens for easy installation
- Clear imaging against strong backlight due to 120 dB true WDR technology
- Efficient H.265+ compression technology
- Audio and alarm interface available
- Focus on human and vehicle targets classification based on deep learning
- Water and dust resistant (IP66) and vandal-resistant (IK10)

▪ Specification

Camera	
Image Sensor	1/3" Progressive Scan CMOS
Max. Resolution	2688 × 1520
Min. Illumination	Color: 0.003 Lux @ (F1.4, AGC ON), B/W: 0 Lux with IR
Shutter Time	1/3 s to 1/100,000 s
Day & Night	IR cut filter
Angle Adjustment	Pan: 0° to 355°, tilt: 0° to 90°, rotate: 0° to 360°
Lens	
Lens Type	Varifocal lens, motor-driven lens, 2.8 to 12 mm
Focal Length & FOV	2.8 to 12 mm, horizontal FOV 108° to 30°, vertical FOV 56° to 17°, diagonal FOV 131° to 35°
Lens Mount	Ø14
Iris Type	Fixed
Aperture	F1.4
DORI	
DORI	2.8 to 12 mm: Wide: D: 64.0 m, O: 25.4 m, R: 12.8 m, I: 6.4 m Tele: D: 190 m, O: 75.4 m, R: 38.0 m, I: 19.0 m
Illuminator	
Supplement Light Type	IR
Supplement Light Range	Up to 60 m
Smart Supplement Light	Yes
IR Wavelength	Yes
Video	
Main Stream	50 Hz: 25 fps (2688 × 1520, 1920 × 1080, 1280 × 720) 60 Hz: 30 fps (2688 × 1520, 1920 × 1080, 1280 × 720)
Sub-Stream	50 Hz: 25 fps (1280 × 720, 640 × 480, 640 × 360) 60 Hz: 30 fps (1280 × 720, 640 × 480, 640 × 360)
Third Stream	50 Hz: 10 fps (1920 × 1080, 1280 × 720, 640 × 480, 640 × 360) 60 Hz: 10 fps (1920 × 1080, 1280 × 720, 640 × 480, 640 × 360) *Third stream is supported under certain settings.
Video Compression	Main stream: H.265/H.264/H.265+/H.264+ Sub-stream: H.265/H.264/MJPEG Third stream: H.265/H.264 *Third stream is supported under certain settings.
Video Bit Rate	32 Kbps to 8 Mbps
H.264 Type	Baseline Profile/Main Profile/High Profile
H.265 Type	Main Profile
Bit Rate Control	CBR/VBR
Scalable Video Coding (SVC)	H.264 and H.265 encoding
Region of Interest (ROI)	1 fixed region for main stream and sub-stream
Audio	
Audio Type	Mono sound
Audio Compression	G.711/G.722.1/G.726/MP2L2/PCM/MP3/AAC-LC

Audio Bit Rate	64 Kbps (G.711ulaw/G.711alaw)/16 Kbps (G.722.1)/16 Kbps (G.726)/32 to 192 Kbps (MP2L2)/8 to 320 Kbps (MP3)/16 to 64 Kbps (AAC-LC)
Audio Sampling Rate	8 kHz/16 kHz/32 kHz/44.1 kHz/48 kHz
Environment Noise Filtering	Yes
Network	
Protocols	TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, NTP, UPnP, SMTP, IGMP, 802.1X, QoS, IPv4, IPv6, UDP, Bonjour, SSL/TLS, PPPoE, SNMP, ARP, WebSocket, WebSockets
Simultaneous Live View	Up to 6 channels
API	Open Network Video Interface (PROFILE S, PROFILE G, PROFILE T), ISAPI, SDK
User/Host	Up to 32 users. 3 user levels: administrator, operator and user
Security	Password protection, complicated password, HTTPS encryption, IP address filter, Security Audit Log, basic and digest authentication for HTTP/HTTPS, TLS 1.1/1.2, WSSE and digest authentication for Open Network Video Interface
Network Storage	NAS (NFS, SMB/CIFS), Auto Network Replenishment (ANR), Together with high-end Hikvision memory card, memory card encryption and health detection are supported.
Client	iVMS-4200, Hik-Connect, Hik-Central
Web Browser	Plug-in required live view: IE 10, IE 11, Plug-in free live view: Chrome 57.0+, Firefox 52.0+, Edge 89+, Local service: Chrome 57.0+, Firefox 52.0+, Edge 89+
Image	
Image Parameters Switch	Yes
Image Settings	Rotate mode, saturation, brightness, contrast, sharpness, gain, white balance adjustable by client software or web browser
Day/Night Switch	Day, Night, Auto, Schedule
Wide Dynamic Range (WDR)	120 dB
SNR	≥ 52 dB
Image Enhancement	BLC, HLC, 3D DNR
Interface	
Ethernet Interface	1 RJ45 10 M/100 M self-adaptive Ethernet port
On-Board Storage	Built-in memory card slot, support microSD card, up to 512 GB
Audio	1 input (line in), 3.5 mm connector, max. input amplitude: 3.3 Vpp, input impedance: 4.7 KΩ, interface type: non-equilibrium; 1 output (line out), 3.5 mm connector, max. output amplitude: 3.3 Vpp, output impedance: 100 Ω, interface type: non-equilibrium
Alarm	1 input, 1 output (max. 24 VDC/24 VAC, 1 A)
Reset Key	Yes
Event	
Basic Event	Motion detection (human and vehicle targets classification), video tampering alarm, exception
Smart Event	Line crossing detection, intrusion detection, region entrance detection, region exiting detection (support alarm triggering by specified target types (human and vehicle)) Scene change detection

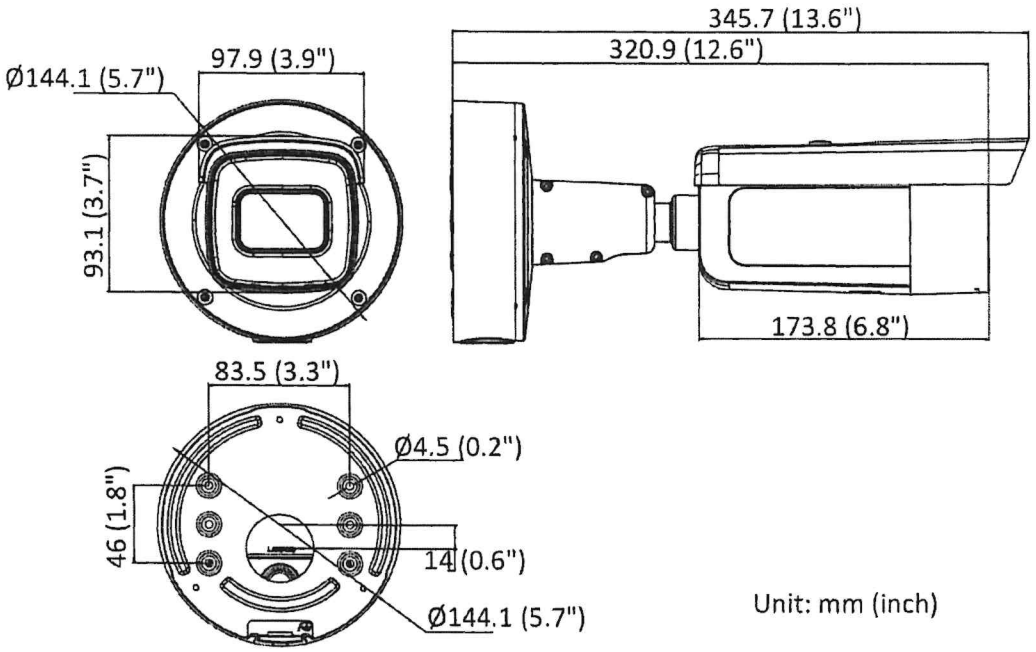
Linkage	Upload to NAS/memory card/FTP, notify surveillance center, trigger recording, trigger capture, send email, audible warning
Deep Learning Function	
Face Capture	Yes
General	
Power	12 VDC ± 25%, 1.08 A, max. 13 W, Ø5.5 mm coaxial power plug, reverse polarity protection PoE: 802.3at, Class 4, 42.5 V to 57 V, 0.36 A to 0.27 A, max. 15 W
Material	ADC12
Dimension	Ø144.1 mm × 345.7 mm (Ø5.7" × 13.6")
Package Dimension	385 mm × 190 mm × 180 mm (15.2" × 7.5" × 7.1")
Weight	Approx. 1445 g (3.2 lb.)
With Package Weight	Approx. 2571 g (5.7 lb.)
Storage Conditions	-30 °C to 60 °C (-22 °F to 140 °F). Humidity 95% or less (non-condensing)
Startup and Operating Conditions	-30 °C to 60 °C (-22 °F to 140 °F). Humidity 95% or less (non-condensing)
Language	33 languages English, Russian, Estonian, Bulgarian, Hungarian, Greek, German, Italian, Czech, Slovak, French, Polish, Dutch, Portuguese, Spanish, Romanian, Danish, Swedish, Norwegian, Finnish, Croatian, Slovenian, Serbian, Turkish, Korean, Traditional Chinese, Thai, Vietnamese, Japanese, Latvian, Lithuanian, Portuguese (Brazil), Ukrainian
General Function	Anti-flicker, heartbeat, mirror, privacy mask, flash log, password reset via email, pixel counter
Approval	
EMC	FCC (47 CFR Part 15, Subpart B); CE-EMC (EN 55032: 2015, EN 61000-3-2: 2014, EN 61000-3-3: 2013, EN 50130-4: 2011 +A1: 2014); RCM (AS/NZS CISPR 32: 2015); KC (KN 32: 2015, KN 35: 2015)
Safety	UL (UL 60950-1); CB (IEC 60950-1: 2005 + Am 1: 2009 + Am 2: 2013); CE-LVD (EN 60950-1: 2005 + Am 1: 2009 + Am 2: 2013); LOA (IEC/EN 60950-1)
Environment	CE-RoHS (2011/65/EU); WEEE (2012/19/EU); Reach (Regulation (EC) No 1907/2006)
Protection	IK10: IEC 62262:2002, IP66: IEC 60529-2013

▪ Available Model

DS-2CD2646G2-IZS(2.8-12mm)(C)

DS-2CD2646G2-IZS(2.8-12mm)(C)(black)

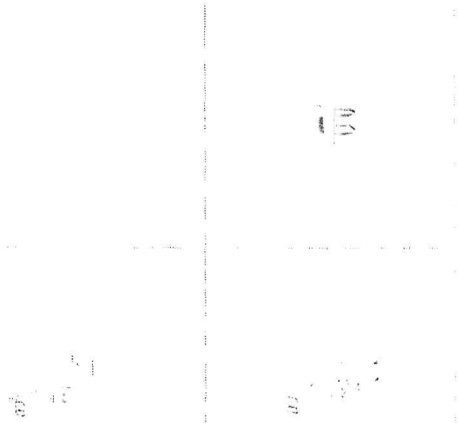
▪ Dimension



Unit: mm (inch)

▪ Accessory

▪ Optional

DS-1475ZJ-SUS Vertical pole mount	DS-1476ZJ-SUS Corner mount	DS-1275ZJ-S-SUS Vertical pole mount
		

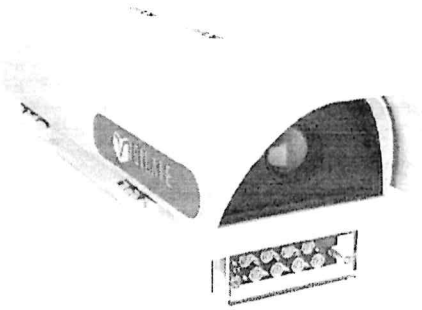
Headquarters
[illegible]
T [illegible]
[illegible].com

VIGILATE

V-LANE A2B

2MP@60fps 250 Km/h (1 Corsia)

- Copertura di 1 corsia
- Telecamera singola testa infrarossi + colori (bispettrale)
- Lettura targhe fino a 250 km/h in free-run
- Illuminatore IR integrato a led stroboscopici
- Risoluzione 2 Mpixel (contesto + OCR)
- Libreria OCR on board con 41 nazioni Europa, 13 Asia, 6 Africa, 5 Sud America e targhe speciali quali Rimorchi, Kemler ADR, Kemler ADR Empty, Tram
- Classificazione diurna dei veicoli per tipologia in 11 + 1 (Macchine, Camion, Camion con rimorchio, Motoveicoli, Motocicli, Ciclomotori, Bus, Mini van, Big van, Cassonati, Caravan, sconosciuto)
- Classificazione notturna dei veicoli per tipologia in 4 classi +1 (camion, bus, macchine, motoveicoli e sconosciuto)
- Classificazione diurna dei veicoli per colore in 11 classi + 1 (nero, bianco, grigio, rosso, blu, giallo, verde, arancio, rosa, viola, ciano, sconosciuto)
- Classificazione brand del veicolo (circa 100 brand supportati)
- Classificazione modello dei veicoli in transito ripresa posteriore (circa 400 modelli supportati)
- Algoritmi di AID di varco per il controllo del traffico (veicolo fermo, veicolo contromano, traffico lento, coda)
- Funzione stima della velocità di transito
- Liste Black & White
- ONVIF Profilo S
- Funzione NVR locale per storage registrazione continua dello streaming video e creazione di micro filmati su transito
- Accessibile via Cloud
- Compatibile con la piattaforma di supervisione generale v-SUITE di Vigilate
- Libreria OCR più volte validata UNI 10772:2016 Classe A



DESCRIZIONI

Analisi e riconoscimento: v-LANE A2B è la camera intelligente 2Mpixels in grado di controllare e gestire tutte le problematiche di un varco stradale sia per aspetti della sicurezza che per gli aspetti relativi al controllo del traffico. V-LANE A2B rileva 60 immagini al secondo entro le quali analizza, individua e convalida le targhe dei veicoli presenti. Questo risultato ottenuto mediante l'impiego di sofisticati software permette di leggere la targa di veicoli in transito con velocità fino a 250 Km/h in modalità free-run (senza dispositivo trigger esterno).

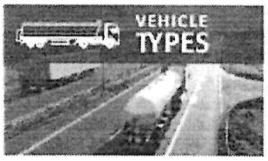
Dati Dati ed immagini possono essere memorizzati direttamente in locale su SSD, inviati al sistema di supervisione del cliente o inviati alla piattaforma di supervisione v-SUITE.Il dispositivo dispone di protocolli di trasmissione FTP, XML-RPC (su HTTPS) e seriale.Software Libreria di Optical Character Recognition (OCR) completa di 41 nazioni Europa, 13 Asia, 6 Africa, 5 Sud America e targhe speciali quali Rimorchi, Kemler ADR, Kemler ADR Empty, Tram (Polizia, Esercito, Ambulanze, Protezione civile...).

Classificazione La camera è dotata di un software di classificazione video in grado di riconoscere le tipologie di veicolo con 11 + 1 classi tra cui (Macchine, Camion, Camion con rimorchio, Motoveicoli, Motocicli, Ciclomotori, Bus, Mini van, Big van, Cassonati, Caravan, sconosciuto); inoltre è in grado d'individuare il colore dominante tra una gamma di 11 colori + 1 (nero, bianco, grigio, rosso, blu, giallo, verde, arancio, rosa, viola, ciano, sconosciuto). v-Lane è dotata di algoritmi di AID di varco per il controllo del traffico (veicolo fermo, veicolo contromano, traffico lento, coda)

Sicurezza dei dati La memorizzazione e la trasmissione dei dati generati dal prodotto, avvengono mediante protocolli altamente affidabili e sicuri, garantendo il massimo livello d'inviolabilità e privacy. Vigilate rispetta le normative più restrittive sulla sicurezza del dato quali la ISO27001:2022 - Privacy by Default e Privacy by Design.

Esempi di applicazioni Controllo accessi parcheggi pubblici e privati Controllo del territorio e della viabilità Controllo accessi zone residenziali Sistemi di pedaggiamento

Vigilate S.r.l.
Via Nobel, 2/e - 25086 Rezzato (BS) Italy - www.vigilate.com
Partita IVA IT03596630056 - Tel. +39.030.9981000 - Fax vigilate@pec.it



v-SUITE

Vigilate - PSIM
(Physical Security Information Management)

ONVIF

VIGILATE

CARATTERISTICHE TECNICHE

Gruppo ottico

Sensore (OCR + COLOR)	2 MP (1920 x 1080) CMOS COLOR + IR (bispectral) global shutter sensor
Frame rate	Up to 60 fps
Ottiche	Standard varifocal lens, 8-50 mm

Illuminatore

Illuminatore IR integrato	n.8 LED IR (CLASS 1M CEI EN 69825-1 ED. 4, 850 nm IR LED)

Caratteristiche HW

Processore	Quad-core + HW video encoder unit + Neural coprocessor
Memoria	16 GB e-MMC Flash
RAM	4 GB
S.O.	Linux
Disco di archiviazione	HD SSD 128 GB (up to 2 TB)
I/O	N. 2 input opto-isolated N. 1 output relè N. 1 fast output strobo 12-24 VDC N. 1 output open-collector 12-24 VDC
Porte	N.1 USB port N.1 RS-485 port N.1 10/100/1000 Mbps Ethernet port

Caratteristiche SW

Modalità di funzionamento	Acquisizione continua (free-run) Su richiesta (tramite trigger SW o trigger HW) Entrambe le modalità possono attingere alle due liste locali configurabili localmente o tramite sincronizzazione remota con il server FTP
Diagnostica in real-time	Temperatura CPU Temperatura main board Funzionamento modulo illuminazione IR Picchi di corrente del modulo di illuminazione Stato cattura dei sensori fisicamente connessi Livello delle correnti in ingresso (power port) Livello delle tensioni in ingresso (power port) Angolo di inclinazione della camera Livello di umidità interna Consumo CPU Consumo RAM Stato dei dischi di storage Utilizzo dei 4 core fisici (monitoraggio CPU) Verifica stato dei threads operativi Monitoraggio tempi di analisi e stato di funzionamento algoritmi attivi Generazione di eventuali allarmi (locali ed eventualmente remoti) a fronte di anomalie rilevate
Protocolli di invio supportati	TCP (nei formati binario, XML, string) TCP Milestone FTP (imgs + dati testuali in *.txt/*.csv) RPC-XML over HTTP / HTTPS (messaggio BASE oppure ESTESO) Custom Protocol (messaggio configurabile mediante template ed inviabile tramite protocolli HTTP POST / HTTPS POST /TCP) Seriale (su porta RS 485) Wiegand (è necessario installare SC20 converter) Xentinel message (over HTTP) v-SUITE message (over HTTP / HTTPS)
Protocolli di comunicazione supportati	TCP/IP UDP HTTP HTTPS FTP FTPS RTP/RTSP openVPN ONVIF (S- profile) NTP SNMP
Protezione dei dati	Possibilità di attivare la gestione del configuratore web tramite connessione HTTPS Cifratura FTPS su protocollo TLS/SSL Cifratura AES-256-ECB per dati e immagini salvati localmente e/o inviate tramite i protocolli supportati Hash delle immagini tramite algoritmo SHA-512 ed eventuale cifratura della firma stessa tramite AES-256-ECB Gestione dello storage totalmente GDPR compliant con cancellazione periodica

dello storico
Funzionalità di mascheramento abitacolo (in caso di rilevazione frontale dei veicoli) al fine di garantire il rispetto della privacy
Possibilità di connettere la camera all'interno di una openVPN con certificato installato direttamente on board
Gestione avanzata del firewall a bordo macchina con possibilità di disattivare gli accessi ai server locali presenti a bordo macchina (server FTP, server ONVIF, server SNMP, porte di servizio)

Alimentazione

Alimentazione supportata	24VDC (2,5 A) or +12VDC (5 A) or UPoE 60W class 6
Consumi	12W typically

Caratteristiche generali

Dimensioni	450 x 140 x 150 mm
Peso	2,6 Kg
Temperatura di funzionamento	- 30°; +60°
Umidità	fino al 90%
Protezione	IP67 - classe IK10 (su richiesta)

Certificazioni

Libreria OCR	Alta affidabilità certificata dal fatto che la libreria è stata più volte validata UNI 10772:2016 classe A per tutte le classi veicolo
Algoritmi di classificazione	Le percentuali di corretta classificazione dipendono dal rispetto della geometria istallativa ma sono al di sopra del 90% indipendentemente dalle condizioni ambientali esterne
Algoritmo AID	La stima istantanea della velocità mediante analisi video e di conseguenza l'algoritmo di AID con le varie funzionalità supportate risultano altamente affidabili come dimostrato da numerosi test di campo in presenza di sistemi omologati per la stima della velocità a scopo sanzionatorio.

UNI 10772:2016
library validated several times

Normativa

Normative rispettate	EN 55032:2015, EN 55035:2017, EN 50561-1:2013 EN 62368-1 (EN 62368-1:2014+A11:2017) EN 60068-2-14:Nb 2011-11 EN 60068-2-78:2013-11 EN 62471:2010 EN60529:1991+A1:2000+A2:2013 UE Regulation 2016/679 (GDPR)

OPZIONALI

- Estensione capacità del disco di storage: fino a 4TB
- Ottica fissa
- Modulo GPS
- Modulo Wi-fi
- Licenza classificazione modello

MADE IN ITALY

Vigilate S.r.l.
Via Napoli snc 6 - 25086 Rezzato BS Italy - www.vigilatevision.com
Partita IVA IT03966630364 - Tel. +39 030 8681000 - Pec info@vigilatepec.it