E.1.

Città di Modica

DELIBERAZIONE
della
GIUNTA COMUNALE
N. 169 del - 7 GIU. 2022

OGGETTO: Aggiornamento approvazione valutazione d'impatto sulla Protezione dei Dati Personali – (Data Protection Impact Assessment – D.P.I.A.) (Art. 35 GDPR 2016/679) del Sistema di videosorveglianza Settore "Ecologia, Ambiente e Igiene Urbana" installato sul territorio del Comune di Modica.

L'anno duemilaventidue il giorno SETTE del mese di GIUGNO alle ore 15,30 nel Palazzo di Città e nella stanza del Sindaco, in seguito ad invito di convocazione, si è riunita la Giunta Comunale, alla quale risultano presenti:

		Presente	Assente
Viola Rosario	Vice Sindaco	X	
Aiello Anna Maria	Assessore	X	
Linguanti Giorgio	Assessore	X	
Lorefice Salvatore Pietro	Assessore	X	
Monisteri Caschetto Maria	Assessore	X	
Belluardo Giorgio	Assessore	X	

Partecipa il Segretario Generale, Dott. Giampiero Bella, con funzioni consultive, referenti, di assistenza e verbalizzazione, ai sensi dell'art.97, comma 4, lett. a) del d. Lgs. n.267/2000.

Assunta la presidenza, il Vice Sindaco, Rosario Viola, constatata la legalità dell'adunanza, dichiara aperta la seduta ed invita la Giunta Comunale all'esame della proposta di deliberazione in oggetto, in merito alla quale sono stati espressi i pareri di legge.

LA GIUNTA COMUNALE

Esaminata l'allegata proposta di deliberazione di pari oggetto, prot. n. 28250 del 07.06.2022, parte integrante e sostanziale del presente atto;

Considerato che della stessa se ne condividono tutti i presupposti di fatto e di diritto;

Preso atto che su tale proposta di deliberazione è stato espresso il parere favorevole in ordine alla regolarità tecnica dello stesso proponente, ai sensi dell'art. 1, comma 1, lett.i, della L.R. n. 48/91, come modificato ed integrato dall'art.12 L.R. n.30/2000. e che la stessa non necessita di ulteriori pareri;

Ritenuto di provvedere in merito;

Visto lo Statuto Comunale;

Visto il vigente O.R.E.L.;

Vista la L.R. n. 48/1991 e successive modifiche ed integrazioni;

Visto l'art. 12 della L.R. n. 44/1991;

Ad unanimità di voti, resi nelle forme di legge

DELIBERA

1. Di approvare e far propria la proposta di deliberazione di pari oggetto richiamata in premessa, che si allega alla presente deliberazione per farne parte integrante e sostanziale;

2. Di dichiarare la presente deliberazione immediatamente esecutiva, con successiva e separata votazione unanime, resa ai sensi dell'art. 12, comma 2, della L.R. n. 44/91, attesa l'urgenza di provvedere in merito, nell'interesse dell'Ente, per i motivi citati nella stessa proposta deliberativa.

E.1.

PROPOSTA di DELIBERAZIONE
della GIUNTA COMUNALE

SETTORE IX
ECOLOGIA-AMBIENTE-IGIENE URBANA

Città di Modica

Prot. n. 28250 del 07 GIU 2022

Oggetto: Aggiornamento Approvazione Valutazione d'Impatto sulla Protezione dei Dati Personali – (Data Protection Impact Assessment – D.P.I.A.) (Art. 35 GDPR 2016/679) del Sistema di videosorveglianza Settore "Ecologia, Ambiente e Igiene Urbana" installato sul territorio del Comune di Modica

****

IL RESONSABILE P.O. DEL IX SETTORE

DOTT. SSA VINCENZA DI ROSA

Premesso che:

- 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", in vigore dal 24 maggio 2016 e applicabile a partire dal 25 maggio 2018, ha introdotto precise regole in materia di informativa e consenso, definendo i limiti al trattamento automatizzato dei dati personali e ponendo, nello stesso tempo, le basi per l'esercizio di nuovi diritti in caso di violazione dei dati personali (data breach);
- il Regolamento (UE) 2016/679 (GDPR – General Data Protection Regulation) è basato sul principio di accountability ("responsabilizzazione") in virtù del quale il Titolare del trattamento adotta politiche e attua misure adeguate per garantire – ed essere in grado di dimostrare – che il trattamento dei dati personali effettuato è conforme al GDPR;
- 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 un clima di fiducia funzionale allo sviluppo dell'economia digitale in tutto il mercato interno;
- il GDPR (art. 37) ha previsto l'obbligo per le autorità pubbliche e gli organismi di diritto pubblico di nominare un DPO – Data Protection Officer (in italiano, RPD o responsabile della protezione dei dati personali), una figura dotata di specifiche competenze in diritto amministrativo, ordinamento degli Enti locali, diritto delle nuove tecnologie nonché in materia di normativa Privacy e deve occuparsi, prevalentemente, di informare e fornire consulenza sulla corretta applicazione della normativa, curando con particolare attenzione la formazione del personale
- con Delibera di Consiglio Comunale n° 51 del 24.05.2018 è stato approvato il Regolamento attuativo del predetto Regolamento n° 679/UE/2016 in materia di protezione dei dati personali;
- il Titolare del Trattamento, così come definito dall'art. 4 comma 7 del GDPR, rappresentato dal Sindaco pro-tempore, con atto del 18.11.2020, ha designato e nominato, ai sensi dell'art. 37 quale Responsabile della Protezione dei dati personali (RPD) (DPO) del Comune di Modica il GRUPPO CONSULTING SOC. COOP. STP. (P.IVA 01667050882), legale rappresentante, il dott. Ing. Carmelo Mezzasalma, incaricato di supportare

il Sindaco nella fase di implementazione di un sistema di gestione della privacy del Comune di Modica conformemente al nuovo Regolamento Europeo in materia di privacy – GDPR 2016/679/UE;

- il Sindaco, titolare del trattamento, con determinazione n° 2929 del 27.11.2020 ha nominato, ai sensi dell'art. 28 comma 4 del detto Regolamento UE 679/2016, i Responsabili P.O. quali responsabili interni del trattamento dati ciascuno con riferimento al Settore diretto, dando loro mandato di effettuare la ricognizione dei responsabili esterni;

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, qualora ne ricorrano i presupposti, obbliga il titolare del trattamento, che può essere coadiuvato dal DPO e dal Responsabile di trattamento, di effettuare la D.P.I.A. (Data Protection Impact Assessment);

Rilevato che:

- l'art. 35 del GDPR individua i casi in cui la D.P.I.A. è necessaria quando un trattamento dei dati personali "può comportare un rischio elevato per i diritti e le libertà delle persone fisiche", che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli;
- in particolare la "procedura di valutazione" è prevista nei casi di sorveglianza sistematica, su larga scala, di una zona accessibile al pubblico (art. 35 comma 3), come nel caso di trattamento di dati personali effettuato tramite sistemi di videosorveglianza;

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

Rilevato che la D.P.I.A.:

- assicura trasparenza e protezione nelle operazioni di trattamento dei dati personali e rappresenta lo strumento cardine tramite il quale il titolare effettua l'anali dei rischi derivanti dai trattamenti posti in essere;
- deve essere condotta prima di procedere al trattamento e, pertanto, deve prevedere le misure da adottare a garanzia di un corretto trattamento dei dati;

Dato atto che:

- trattandosi di una valutazione preventiva, deve, comunque, essere previsto un riesame continuo della D.P.I.A., ripetendo la valutazione a intervalli regolari;
- la responsabilità della D.P.I.A. spetta al titolare, anche se la conduzione materiale della valutazione di impatto può essere affidata ad un altro soggetto interno o esterno all'organizzazione;

Visti:

- le «Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679» del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 e fatte proprie dal Comitato europeo per la protezione dei dati (European Data Protection Board - EDPB) il 25 maggio 2018 ("WP 248, rev. 01");
- il provvedimento del Garante per la protezione dei dati personali avente ad oggetto "*Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 – n. 467 del 11 ottobre 2018*", con il quale Garante ha predisposto un elenco non esaustivo delle tipologie di trattamento ai sensi dell'art. 35, par. 4 da sottoporre a valutazione d'impatto, per cui è necessario sottoporre a valutazione di rischio tali trattamenti legati all'attività di videosorveglianza quali " utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati", "dati aventi carattere estremamente personale", "uso di tecnologie evolute";

Riscontrato, in base alla predetta disciplina, che i trattamenti di dati personali effettuati tramite sistemi di videosorveglianza necessitano della valutazione d'impatto, poiché rientrano nel caso previsto all'art. 35 GDPR c. 3 lett. c) "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico." (Il Garante ha chiarito come le espressioni trattamenti "sistematici" e "non occasionali", indicate nell'elenco delle tipologie di trattamenti, siano riconducibili al criterio della "larga scala" illustrato nelle Linee Guida WP n. 248, rev. 01);

Rilevato che, per quanto sopra, è necessario attivare :

- una "determinazione preliminare" della possibilità che il trattamento possa presentare un rischio elevato" per i diritti e le libertà delle persone fisiche, quale il diritto alla privacy e ad altri diritti fondamentali, come la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione;
- una "valutazione di impatto" nel caso in cui la determinazione preliminare accerti la possibilità che il trattamento possa presentare un rischio elevato;

Vista la Valutazione d'impatto (P.I.A. - Privacy Impact Assessment) sul sistema di videosorveglianza del Settore Ecologia e Ambiente relativa al trattamento operato dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza sia fissi che mobili attivati nel territorio del Comune di Modica, ai sensi del Reg. UE 2016/679, della Direttiva UE 2016/680 in osservanza alle disposizioni contenute nel "decalogo" del 8 aprile 2010 dal Garante della Privacy e del Codice Nazionale sulla Privacy del Dlgs 196/2003 come modificato dal D.Lgs. 10 agosto 2018 n. 101;

Dato atto che:

- la valutazione di impatto di tale sistema di videosorveglianza pone particolare attenzione ai diritti e alle libertà fondamentali e alla dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale, al fine di garantire la protezione dei dati personali di tutti coloro che entrano in contatto con l'attività di videosorveglianza;
- l'utilizzo dei sistemi di videosorveglianza è finalizzato a contrastare il grave fenomeno dell'abbandono illecito di rifiuti a salvaguardia e a tutela dell'igiene e della salute pubblica, ad accertare e sanzionare le violazioni delle norme in materia ambientale, quale strumento di prevenzione per preservare l'integrità del patrimonio pubblico e privato e tutelare il decoro e la quiete pubblica, volto a garantire l'interesse pubblico e a salvaguardare la sicurezza pubblica ai sensi dell'art. 5 del D. lgs. n° 51/2018;

Dato atto, altresì, che le responsabilità del trattamento sono connesse ai ruoli ricoperti e così individuati:

- **Titolare del trattamento** è il Sindaco pro-tempore - l'art. 4 comma 7 del GDPR definisce «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;
- **Responsabile interno del trattamento dati** è il dirigente/responsabile di P.O. del Settore Ecologia e Ambiente, come definito dall'art. 4 comma 8 e come formalmente nominato dal Sindaco con determinazione n° 2929 del 27.11.2020;
- **Responsabile della Protezione dei dati personali (RPD) (DPO)** per il Comune di Modica è il GRUPPO CONSULTING SOC. COOP. STP. (P.IVA 01667050882), con sede a Ragusa in Via Mons. G. Iacono n. 20, legale rappresentante, il dott. Ing. Carmelo Mezzasalma, nominato con Determinazione n° 2693 del 04.11.2020, con proroga fino al novembre 2022;
- **Responsabili esterni del trattamento** sono rappresentati da tutti i soggetti fisici o giuridici che gestiscono per conto dell'Ente dati personali nell'ambito di un appalto di servizi relativi al supporto per la gestione degli impianti, individuati:
    - nella ditta "Ermeslink" di Di Stefano Giovanni, quale responsabile esterno per la gestione, la manutenzione e il prelievo delle immagini delle telecamere fisse;
    - nella ditta "Steam Service" di Amato Giuseppe, quale responsabile esterno per la gestione e la manutenzione delle telecamere mobili;

Vista l'allegata Valutazione di Impatto – D.P.I.A. aggiornata avente ad oggetto *"Valutazione d'impatto sulla protezione dei dati (Art. 35 GDPR 2016/679) Settore Ecologia e Ambiente del Comune di Modica - Sistema di videosorveglianza"* formulata con la consulenza del predetto Responsabile Protezione Dati e *"validata"* dallo stesso;

Considerato che, con la D.P.I.A. formulata, ai sensi dell'art. 35 del Regolamento n° 679/2016, in relazione alle metodologie di lavoro da applicare nella valutazione preventiva dell'impatto di violazione, con analisi e valutazione dei rischi e delle misure adottate per affrontarli in materia di sicurezza di conservazione dei dati, di vulnerabilità del sistema adottato per evitare rischi di perdita di dati e preservarne la riservatezza, è stato rilevato in tutti i casi una probabilità di rischio *"limitata"*;

Tenuto conto che la superiore Valutazione d'Impatto – D.P.I.A. costituisce un documento soggetto a periodico aggiornamento, in particolare quando insorgono variazioni del rischio per l'utilizzo di nuovi strumenti tecnologici e/o per il verificarsi di nuove problematiche;

Ritenuto, per quanto sopra, necessario provvedere all'approvazione del documento di Valutazione - D.P.I.A. e relativi allegati, parte integrante e sostanziale del presente atto, relativa ai rischi di violazione del predetto sistema di videosorveglianza del Settore Ecologia e Ambiente;

Visti:

- la Legge n° 241 del 07.08.1990 e ss.mm.ii.;
- la L.R. n° 48/91;
- il D.Lgs. n. 267/2000 e successive modifiche e integrazioni;
- il Dlgs 196/2003 come modificato dal D.Lgs. 10 agosto 2018 n. 101;
- il "Provvedimento in materia di videosorveglianza" dell'8 aprile 2010 del Garante per la protezione dei dati personali
- il Regolamento UE 679/2016 GDPR per la Protezione dei Dati Personali;
- la determina sindacale n. 4247/31.12.2021 e n° 1039/17.03.2022 di modifica ed integrazione della nomina a Responsabile P.O. del IX Settore "Ecologia, Ambiente, Igiene Urbana", e l'art. 107 del D.Lgs 267/2000 (T.U.E.L.) e ss. mm. ii. relativo alle funzioni dirigenziali a rilevanza esterna esercitate con l'adozione dell'atto;
- l'O.R.E.L. vigente in Sicilia

Ritenute le proprie competenze;

Acquisiti:

- il parere favorevole ex art. 49 DLgs. n. 267/2000 e ss.mm.ii. espresso dal Responsabile del Servizio competente;
- il parere favorevole ex art. 49 DLgs. n. 267/2000 e ss.mm.ii. espresso dal Responsabile del Servizio finanziario in ordine alla regolarità contabile ;

PROPONE ALLA GIUNTA COMUNALE

Per le motivazioni citate in premessa che si intendono integralmente trascritte, di:

1. Di approvare il documento aggiornato di Valutazione - D.P.I.A. avente ad oggetto *"Valutazione d'impatto sulla protezione dei dati (Art. 35 GDPR 2016/679) Settore Ecologia e Ambiente del Comune di Modica - Sistema di videosorveglianza"* e relativi allegati, parte integrante e sostanziale del presente atto, relativa ai rischi di violazione del predetto sistema di videosorveglianza del Settore Ecologia e Ambiente;

2. Di notificare il presente atto al Responsabile P.O. del IX Settore – "Ecologia, Ambiente e Igiene Urbana";

3. Di dare mandato al Responsabile P.O. del IX Settore di trasmetterne copia alla DPO del Comune di Modica - il

GRUPPO CONSULTING SOC. COOP. STP. (P.IVA 01667050882), con sede a Ragusa in Via Mons. G. Iacono n. 20, legale rappresentante, il dott. Ing. Carmelo Mezzasalma;

4. Di dichiarare ai sensi dell'art. 6 par. "Conflitto d'interessi, del vigente P.T.C.P. che la scrivente è in assenza di conflitto di interessi di cui all'art. 6 bis della L. n. 241/1990 come introdotto dall'art.1, comma 41, della Legge 190/2012;

5. Di disporre la pubblicazione del presente provvedimento sul siyo web dell'Ente, Sezione Atti – "Protezione Dati Regolamento UE 679/2016" – sottosezione Settore IX – Atti Videosorveglianza Settore Ambiente;

6. Di dichiarare, con separata e unanime votazione, la presente deliberazione immediatamente esecutiva ai sensi dell'art. 134, comma 4, del DLgs. n. 267/2000 e ss.mm.ii.

Il Responsabile P.O. del IX Settore
Dott.ssa Vincenza Di Rosa

Sulla proposta di deliberazione di cui sopra sono stati espressi i seguenti pareri, ai sensi dell'art. 1, comma 1, lett. i, L.R. n. 48/91, come modificato ed integrato dall'art. 12 L.R. n.30/2000.

Parere del Responsabile del Settore proponente per la regolarità tecnica: **favorevole** Modica, lì 06.06.2022 **Il Responsabile del Settore** Vincenzo Di Rosa
Parere del Responsabile del settore finanziario per la regolarità contabile: **favorevole** Modica, lì **Il Responsabile del Settore Finanziario**
Per l'assunzione dell'impegno di spesa, si attesta la regolare copertura finanziaria, ai sensi degli artt. 153, 183, 191 del D.L.vo n.267/2000, con spesa da impegnare al cap. _____ del Bilancio 2021. Modica, lì **Il Responsabile del Settore Finanziario**

La proposta infra riportata si compone di n. _____ pagine. incluso il presente prospetto,.

Visto
L'Assessore al ramo

Il Responsabile proponente
Vincenzo Di Rosa

La presente proposta è approvata con deliberazione della Giunta Municipale n. 169 del - 7 GIU. 2022

Il Segretario Comunale

Valutazione d'impatto sulla protezione dei dati (Art. 35 GDPR 2016/679)
Settore Ecologia e ambiente del Comune di Modica
Sistema di videosorveglianza

Valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment - DPIA) alla luce delle linee guida del WP Art. 29 del 4.10.2017 e del Decreto Legislativo N.101 del 10 Agosto 2018 (Modifica del Codice Privacy D. Lgs. n. 101/2018)

Premessa La disciplina sulla DPIA contenuta nel GDPR deve essere integrata da quanto specificato dal WP art. 29 nelle linee guida pubblicate in data 4.10.2017 (versione definitiva). In particolare, il WP art. 29 ha definito i criteri in base ai quali decidere se fare ricorso o meno a una DPIA, quali sono le metodologie utilizzabili dai titolari per condurre una DPIA e quali sono gli elementi sufficienti per una DPIA accettabile.

1. Soggetto obbligato

Il GDPR impone al solo **titolare** del trattamento di effettuare la DPIA, qualora ne ricorrano i presupposti (cfr. art. 35). Nello svolgimento di una DPIA il titolare potrà essere coadiuvato dal DPO e dal responsabile. Quando un trattamento è svolto in **contitolarità,** nella DPIA devono essere specificati con precisione gli obblighi che incombono su ciascun titolare, ad esempio con riferimento alla responsabilità delle singole misure finalizzate alla gestione dei rischi.

2. In quali casi è necessario effettuare una DPIA

La DPIA è obbligatoria solo qualora un trattamento "possa presentare un **rischio elevato"** per i diritti e le libertà delle persone fisiche. Nei **casi dubbi,** si raccomanda di svolgere comunque una DPIA, in quanto questa è una procedura che permette di realizzare e dimostrare la conformità con le norme del GDPR. Il riferimento ai **"diritti e alle libertà"** va inteso come relativo al diritto alla privacy e anche ad altri diritti fondamentali, quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione.

2.a) Casi previsti dal **GDPR**

L'art. 35, paragrafo 3, GDPR cita espressamente tre casi in cui sussiste un rischio elevato ed è quindi necessaria l'effettuazione di una DPIA, ossia: **a)** valutazione sistematica e globale, basata su un trattamento automatizzato, degli aspetti personali relativi a persone fisiche (compresa la **profilazione),** e sulla quale si fondano decisioni che hanno effetti giuridici o incidono significativamente su tali soggetti;

b) trattamento su **larga scala** di **dati sensibili o giudiziari;**

c) sorveglianza sistematica su **larga scala** di una **zona accessibile al pubblico.** Tale elenco non è esaustivo. Secondo il WP art. 29 la DPIA deve essere anche condotta per valutare l'**impatto di un nuovo dispositivo tecnologico** in termini di protezione dei dati. Il GDPR assegna alle autorità di controllo (per l'Italia, al Garante) il compito di redigere e rendere pubblico **un elenco delle tipologie di trattamento** da assoggettare e da non assoggettare a DPIA (cfr. art. 35, paragrafi 4 e 5).

2.b) I 9 criteri enunciati dal WP art. 29

Secondo il WP art. 29 i seguenti **9 criteri** devono essere presi in esame sia dalle autorità di controllo per redigere l'elenco delle tipologie di trattamento da assoggettare a DPIA *ex* art. 35, par. 4, GDPR, sia dai titolari per comprendere quando siano tenuti a svolgere una DPIA:

1. trattamenti valutativi o di *scoring,* compresa la **profilazione** e attività predittive, in particolare a partire da "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" (considerando 71 e 91). Ad es.: società che crea profili comportamentali o di *marketing* a partire dalla operazioni o dalla navigazione compiute sul proprio sito internet;
2. decisioni automatizzate che producono significativi effetti giuridici o di analoga natura. Ad es.: trattamento che possa comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione;
3. monitoraggio sistematico: trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o "la sorveglianza sistematica di un'area accessibile al pubblico"; **4. dati sensibili o dati di natura estremamente personale:** si tratta dei dati sensibili di cui all'art. 9 e dei dati giudiziari di cui all'art. 10;

5. trattamenti di dati su larga scala: il **GDPR** si occupa del termine "larga scala" nel considerando 91. Il Gruppo art. 29 raccomanda di tenere conto dei seguenti fattori al fine di stabile se un trattamento sia svolto su larga scala:

a) numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento;

b) volume dei dati e/ o ambito delle diverse tipologie di dati oggetto di trattamento;

c) durata, o persistenza, dell'attività di trattamento;

d) ambito geografico dell'attività di trattamento;

6. combinazione o raffronto di insieme di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/ o da titolari distinti;

7. dati relativi a interessati vulnerabili (cons. 75), compresi i minori, i dipendenti, i soggetti con patologie psichiatriche, i richiedenti asilo, gli anziani, i pazienti e ogni interessato rispetto al quale possa identificarsi una situazione di disequilibrio con il rispettivo titolare del trattamento;

8. utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

9. trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (art. 22 e cons. 91). Ad es.: *screening* dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno ad un finanziamento.

Quando ricorrono almeno **due dei criteri** sopra indicati, il titolare dovrà condurre una DPIA. Tuttavia, in alcuni casi si dovrà procedere a una DPIA anche di fronte ad un trattamento che soddisfi **solo uno dei criteri** di cui sopra. È, inoltre, possibile che vi sia perfetta coincidenza tra le ipotesi legislative e i criteri enucleati dal WP art. 29 (ad es. la profilazione sistematica che impatta significativamente sull'interessato non è solo un caso legislativamente previsto di DPIA obbligatoria *ex* art. 35, par. 3, lett. a) GDPR, ma anche la combinazione dei criteri n° 1, 2 e 3 stabiliti dal WP art. 29). Si potrebbe verificare anche il caso, ma il WP art. 29 non chiarisce quando tale ipotesi potrebbe verificarsi in concreto, in cui il titolare esclude che debba svolgersi una DPIA perché, pur in presenza dei criteri summenzionati, il trattamento **non** presenta un rischio elevato. In questo caso, il titolare dovrà motivare e documentare la scelta della mancata conduzione della DPIA, allegando o annotando **il** parere del **DPO.** Possiamo immaginare che si tratti della situazione in cui vengano adottate dal titolare misure di sicurezza tali da scongiurare la possibilità di rischio (elevato) per i diritti e le libertà degli interessati (ad es. mediante la pseudonimizzazione e la cifratura dei dati che vengono profilati).
Di seguito si riportano alcuni esempi di trattamento e di funzionamento operativo dei criteri fissati dal WP art. 29: **Esempi di trattamento:** azienda che controlla sistematicamente le attività dei dipendenti, compreso l'utilizzo dei terminali informatici, la navigazione su internet, ecc. **~criteri pertinenti:** monitoraggio sistematico; dati relativi a interessati vulnerabili; **obbligo di DPIA probabile.**

Esempi di trattamento: raccolta di dati pubblici tratti dai *social media* per la creazione di profili **~criteri pertinenti:** valutazione o *scoring;* dati trattati su larga scala; raffronto o combinazione di insiemi di dati; dati sensibili o dati di natura estremamente personale; **obbligo di DPIA probabile.**

Esempi di trattamento: rivista *online* che utilizza una *mailing list* per inviare agli abbonati un bollettino giornaliero di carattere generale ~**criteri pertinenti:** dati trattati su larga scala; **obbligo di DPIA non probabile.**

Esempi di trattamento: sito di *e-commerce* che pubblicizza parti di ricambio per auto d'epoca con limitata profilazione riferita ad alcune sezioni del sito e basata su pregressi acquisti effettuati ~**criteri pertinenti:** valutazione o *scoring,* **obbligo di DPIA non probabile.**

Per quanto riguarda l'aspetto legislativo, le modifiche introdotte dal D. Lgs. n. 101/2018 indicate di seguito delimitano lo spazio di svolgimento dell'attività di trattamento.

Titolo VI - Istruzione

Capo I - Profili generali

Art. 96 ***(Trattamento di dati relativi a studenti)*** 1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le istituzioni del sistema nazionale di istruzione, i centri di formazione professionale regionale, le scuole private non paritarie nonché le istituzioni di alta formazione artistica e coreutica e le università statali o non statali legalmente riconosciute su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali, degli studenti e altri dati personali diversi da quelli di cui agli articoli 9 e 1 O del Regolamento, pertinenti in relazione alle predette finalità e indicati nelle informazioni rese agli interessati ai sensi dell'articolo 13 del Regolamento. I dati possono essere successivamente trattati esclusivamente per le predette finalità. 2. Resta ferma la disposizione di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249, sulla tutela del diritto dello studente alla riservatezza. Restano altresì ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati.

Titolo VII - *Trattamenti* a *fini di archiviazione nel pubblico interesse, di ricerca scientifica* o *storica* o a *fini statistici*

Capo I - Profili generali

Art. 97 ***(Ambito applicativo)***

1. Il presente titolo disciplina il trattamento dei dati personali effettuato a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ai sensi dell'articolo 89 del regolamento.

Art. 98 - Finalità di rilevante interesse pubblico (abrogato)

Art. 99 ***(Durata del trattamento)***

1. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici può essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.

2. A fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici possono comunque essere conservati o ceduti ad altro titolare i dati personali dei quali, per qualsiasi causa, è cessato il trattamento nel rispetto di quanto previsto dall'articolo 89, paragrafo 1, del Regolamento.

Art. 100 - Dati relativi ad attività di studio e ricerca

1. Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico i soggetti pubblici, ivi comprese le università e gli enti di ricerca, possono con autonome determinazioni comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione di quelli di cui agli articoli 9 e 1 O del Regolamento.

2. Resta fermo il diritto dell'interessato di rettifica, cancellazione, limitazione e opposizione ai sensi degli articoli 16, 17, 18 e 21 del Regolamento.

3. I dati di cui al presente articolo non costituiscono documenti amministrativi ai sensi della Legge 7 agosto 1990, n. 241.
4. I dati di cui al presente articolo possono essere successivamente trattati per i soli scopi in base ai quali sono comunicati o diffusi.
4-bis. I diritti di cui al comma 2 si esercitano con le modalità previste dalle regole deontologiche.

Capo II - ***Trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica***

Art. 101 - Modalità di trattamento
1. I dati personali raccolti a fini di archiviazione nel pubblico interesse o di ricerca storica non possono essere utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati anche per altre finalità nel rispetto dell'articolo 5 del regolamento.
2. I documenti contenenti dati personali, trattati a fini di archiviazione nel pubblico interesse o di ricerca storica, possono essere utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il perseguimento di tali scopi. I dati personali diffusi possono essere utilizzati solo per il perseguimento dei medesimi scopi.
3. I dati personali possono essere comunque diffusi quando sono relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso suoi comportamenti in pubblico.
Art. 102 - *Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica*
1. Il Garante promuove, ai sensi dell'articolo *2-quater,* la sottoscrizione di regole deontologiche per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati a fini di archiviazione nel pubblico interesse o di ricerca storica.
2. Le regole deontologiche di cui al comma 1 individuano garanzie adeguate per i diritti e le libertà dell'interessato in particolare: a. le regole di correttezza e di non discriminazione nei confronti degli utenti da osservare anche nella comunicazione e diffusione dei dati, in armonia con le disposizioni del presente codice e del Regolamento applicabili ai trattamenti di dati per finalità giornalistiche o di pubblicazione di articoli, saggi e altre manifestazioni del pensiero anche nell'espressione artistica; b. le particolari cautele per la raccolta, la consultazione e la diffusione di documenti concernenti dati idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare, identificando casi in cui l'interessato o chi vi abbia interesse è informato dall'utente della prevista diffusione di dati; c. le modalità di applicazione agli archivi privati della disciplina dettata in materia di trattamento dei dati a fini di archiviazione nel pubblico interesse o di ricerca storica, anche in riferimento all'uniformità dei criteri da seguire per la consultazione e alle cautele da osservare nella comunicazione e nella diffusione.
Art. 103 - *Consultazione di documenti conservati in archivi*
1. La consultazione dei documenti conservati negli archivi di Stato, in quelli storici degli enti pubblici e in archivi privati dichiarati di interesse storico particolarmente importante è disciplinata dal decreto legislativo 22 gennaio 2004, n. 42 e dalle relative regole deontologiche.

TITOLO VIII - *Trattamenti nell'ambito del rapporto di lavoro*

Capo I - **Profili generali**

Art. 111 *(Regole deontologiche per trattamenti nell'ambito del rapporto di lavoro)*
1. Il Garante promuove, ai sensi dell'articolo *2-quater,* l'adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalità di cui all'articolo 88 del Regolamento, prevedendo anche specifiche modalità per le informazioni da rendere all'interessato.
2. **Art. 111-bis *(Informazioni in caso di ricezione di curriculum)***
3. 1. Le informazioni di cui all'articolo 13 del Regolamento, nei casi di ricezione dei *curricula* spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, vengono fornite al momento del primo contatto utile, successivo all'invio del *curriculum* medesimo. Nei limiti delle finalità di cui all'articolo 6, paragrafo 1, lettera b), del Regolamento, il consenso al trattamento dei dati personali presenti nei *curricu/a* non è dovuto.
4. **Art. 112 - Finalità di rilevante interesse pubblico (abrogato)**

Capo II - ***Trattamento di dati riguardanti i prestatori di lavoro***

5. **Art. 113 Raccolta di dati e pertinenza**

1. Resta fermo quanto disposto dall'articolo 8 della legge 20 maggio 1970, n.300 nonché dall'articolo 1 O del decreto legislativo 1 O settembre 2003, n. 276. **Capo lii - *Controllo a distanza, lavoro agile e telelavoro***

6. **Art. 114 *(Garanzie in materia di controllo a distanza)***

1. Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n.300.

7. **Art. 115 *(Telelavoro, lavoro agile e lavoro domestico)***

1. Nell'ambito del rapporto di lavoro domestico del telelavoro e del lavoro agile il datore di lavoro è tenuto a garantire al lavoratore il rispetto della sua personalità e della sua libertà morale.

2. il lavoratore domestico è tenuto a mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare.

Capo IV - Istituti di patronato e di assistenza sociale

8. **Art. 116 Conoscibilità di dati su mandato dell'interessato**

1. Per lo svolgimento delle proprie attività gli istituti di patronato e di assistenza sociale, nell'ambito del mandato conferito dall'interessato, possono accedere alle banche di dati degli enti eroganti le prestazioni, in relazione a tipi di dati individuati specificamente con il consenso manifestato dall'interessato medesimo.

2. il Ministro del lavoro e delle politiche sociali stabilisce con proprio decreto le linee- guida di apposite convenzioni da stipulare tra gli istituti di patronato e di assistenza sociale e gli enti eroganti le prestazioni.

Titolo IX - *Altri trattamenti in ambito pubblico o di interesse pubblico* Capo ! - *(Assicurazioni)*

Art. 117 - Affidabilità e puntualità nei pagamenti(abrogato) Art. 118 - Informazioni commerciali (abrogato)

Art. 119 - Dati relativi al comportamento debitorio (abrogato)

Art. 120 - Sinistri

1. L'Istituto per la vigilanza sulle assicurazioni definisce con proprio provvedimento le procedure e le modalità di funzionamento della banca di dati dei sinistri istituita per la prevenzione e il contrasto di comportamenti fraudolenti nel settore delle assicurazioni obbligatorie per i veicoli a motore immatricolati in Italia, stabilisce le modalità di accesso alle informazioni raccolte dalla banca dati per gli organi giudiziari e per le pubbliche amministrazioni competenti in materia di prevenzione e contrasto di comportamenti fraudolenti nel settore delle assicurazioni obbligatorie, nonché le modalità e i limiti per l'accesso alle informazioni da parte delle imprese di assicurazione.

2. Il trattamento e la comunicazione ai soggetti di cui al comma 1 dei dati personali sono consentiti per lo svolgimento delle funzioni indicate nel medesimo comma.

3. Per quanto non previsto dal presente articolo si applicano le disposizioni dall'articolo 135 del codice delle assicurazioni private di cui al decreto legislativo 7 settembre 2005, n. 209.

Titolo X - Comunicazioni elettroniche

Capo I - Servizi di comunicazione elettronica

Art. 121 (Servizi interessati e definizioni)

1. Le disposizioni del presente titolo si applicano al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni, comprese quelle che supportano i dispositivi di raccolta dei dati e di identificazione.

1-bis. Ai fini dell'applicazione delle disposizioni del presente titolo si intende per:

a) «comunicazione elettronica», ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un contraente o utente ricevente, identificato o identificabile;

b) «chiamata», la connessione istituita da un servizio di comunicazione elettronica accessibile al pubblico che consente la comunicazione bidirezionale;

c) «reti di comunicazione elettronica», i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il

trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

d) «rete pubblica di comunicazioni», una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di reti;

e) «servizio di comunicazione elettronica», i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera e), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

f) «contraente», qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

g) «utente», qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

h) «dati relativi al traffico», qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

i) «dati relativi all'ubicazione», ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica
dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

j) «servizio a valore aggiunto», il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto e' necessario per la trasmissione di una comunicazione o della relativa fatturazione;

k) «posta elettronica», messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

Informazioni sulla PIA

Nome della PIA
Valutazione d'impatto sul sistema di videosorveglianza Settore Ecologia

Nome autore
Sindaco

Nome valutatore
Responsabile Settore Ecologia

Nome validatore
Responsabile protezione dati Dott. Ing. Carmelo Mezzasalma

Data di creazione
20/05/2022

Allegati

ALLEGATO 1.pdf

ALLEGATO 2.pdf

ALLEGATO 3.pdf

ALLEGATO 4.pdf

ALLEGATO 5.pdf

ALLEGATO 6.pdf

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?
Il trattamento operato dal responsabile di servizio P.O. settore ecologia e ambiente, interamente o parzialmente automatizzato, dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza sia fissi che mobili, attivati nel territorio dell'Ente, ai sensi del Reg. UE 2016/679, della Direttiva UE 2016/680, in osservanza delle disposizioni contenuti nel "decalogo" del 8 aprile 2010 dal Garante della Privacy e del Codice Nazionale sulla Privacy dlgs 196/2003.

L'impatto è valutato con particolare attenzione ai diritti e alle libertà degli interessati e ha come obbiettivo di verificare e garantire la protezione dei dati personali di tutti coloro che entrano in contatto o in relazione con l'attività di videosorveglianza. In attuazione del principio di necessità, i sistemi di videosorveglianza ed i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere raggiunte mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

L'utilizzo dei sistemi di videosorveglianza è finalizzato altresì a:

a) prevenire e reprimere fenomeni di degrado urbano e svolgere controlli volti ad accertare e sanzionare violazioni delle norme in materia ambientale e delle disposizioni del regolamento per la gestione integrata dei rifiuti urbani, qualora risultino difficili o inefficaci l'attuazione di altre misure;

b) vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato, dell'ordine, del decoro e della quiete pubblica;

L'utilizzo dei sistemi di videosorveglianza da parte del responsabile di P.O. Settore Ecologia del comune di Modica, costituisce inoltre strumento di prevenzione e di razionalizzazione dell'azione di Polizia giudiziaria sul territorio comunale, in stretto raccordo con la Polizia Locale.

Quali sono le responsabilità connesse al trattamento?

Le responsabilità del trattamento sono connesse ai ruoli ricoperti, il titolare del trattamento è il Sindaco pro tempore, il designato al trattamento (responsabili interni) è il dirigente/responsabile di posizione organizzativa del servizio del settore ecologia e ambiente, se formalmente nominato, possono essere nominati come responsabili esterni del trattamento tutti i soggetti fisici o giuridici che gestiscono per conto dell'ente dati personali nell'ambito di un appalto di servizi relativo al supporto per la gestione degli impianti.
Responsabili esterni per gestione e manutenzione e analisi delle immagini telecamere fisse:
Ermes Link di Di Stefano Giovanni (vedi allegati)
Responsabili esterni per manutenzione e gestione telecamere mobili:
Steam service (vedi allegati)

Ci sono standard applicabili al trattamento?

Al momento non sono contemplati standard da applicare direttamente al trattamento, tuttavia l'attività di videosorveglianza è disciplinata da specifico regolamento dell'ente.

Valutazione : Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Gli impianti riprendono e registrano immagini che permettono di identificare in modo diretto o indiretto le persone riprese, consentono riprese unicamente di video o foto e sono installati nel territorio dell'Ente e possono essere sia fissi che mobili. Vengono trattati i dati degli autoveicoli, targhe e persone fisiche che circolano in prossimità delle telecamere.

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

Le immagini riprese da telecamere fisse prelevate e consegnate dalla Ditta Ermeslink al personale interno incaricato del Settore Ecologia per la successiva consegna alla Polizia Locale delle solo immagini dove si evidenzia un reato per la redazione del verbale e l'elevazione della relativa sanzione

Le immagini riprese dalle telecamere mobili vengono visualizzate in modalità remota all'interno degli uffici del settore ecologia da personale debitamente autorizzato.

Ogni telecamera P2P o videoregistratore di rete (NVR) vengono identificati con un numero ID univoco (UID) registrato e integrato a livello di sviluppo, che viene utilizzato per eseguire il ping del server P2P;
- una volta connessa la IP cam con l'app / software, gli utenti possono visualizzare in streaming in tempo reale i video dalla telecamera di sicurezza, anche al di fuori della rete locale (LAN), mediante l' RTSP (Real Time Streaming Protocol) e del protocollo HTTPS (HyperText Transfer Protocol Secure), garantendo così un canale di comunicazione criptato e certificato dal Transport Layer Security (TLS) tra il client e il server localizzato in Francoforte (Germania);
- tutti i dati (video) e altri concernenti la configurabilità, l'account e altre informazioni necessaria al funzionamento del sistema, sono conservati in modalità criptata;

- l'utente che desidera aprire il video dalla scheda SD, deve prima inserire la password in formato crittografato AES, a cura di Dahua;
- le immagini e video vengono sovrascritti in maniera automatica dopo sette giorni dalla loro rilevazione.

Quali sono le risorse di supporto ai dati?

Gli impianti consentono riprese video e foto a colori, diurne e notturne, in condizioni di sufficiente illuminazione naturale o artificiale, gli impianti di videosorveglianza sono sempre in funzione e registrano in maniera continuativa, mentre gli impianti di si innescano in modo autonomo a seguito di qualsiasi movimento di veicoli o esseri umani catturando immagini.

I segnali video e foto delle unità di ripresa sono inviati presso la sede settore ecologia su data center individuato appositamente dove sono registrati su appositi server. In queste sedi le immagini sono visualizzate su monitor e hardware client appositamente configurato il cui accesso è protetto, riservato e consentito unicamente al personale formalmente e appositamente incaricato

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento dei dati personali, acquisiti mediante l'utilizzo degli impianti di videosorveglianza gestiti dall'Ente e collegati alle centrali di controllo ubicate presso gli Uffici dell'Ente, si svolge nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. Garantisce al contempo il rispetto dei diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento.

In particolare, il sistema di videosorveglianza comunale è volto a perseguire le seguenti finalità istituzionali, nel rispetto delle vigenti disposizioni di legge e di regolamento, nonché dallo Statuto, dalle ordinanze e dai Regolamenti Comunali:

attivazione di misure di prevenzione contro l'abbandono di rifiuti o l'uso non conforme dei contenitori delle isole ecologiche.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica del trattamento è data dunque dalla necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri ai sensi dell'art. 6, paragrafo 1, lettera e) GDPR, nonché dalla necessità di eseguire un compito di un'autorità competente per le finalità di prevenzione, accertamento e perseguimento di reati, salvaguardia contro e la prevenzione di minacce alla sicurezza urbana ai sensi dell'art. 5 del D.lgs n. 51/2018.

Valutazione : Accettabile

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

L'attività di videosorveglianza raccoglie esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, 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. La localizzazione delle telecamere e le modalità di ripresa saranno quindi stabilite in modo conseguente.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

I dati sono esatti ed aggiornati. Il DVR è configurato in modo tale da conservare le immagini entro sette giorni dalla rilevazione delle stesse.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

I dati personali registrati mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento sono conservati per un periodo di tempo non superiore a sette giorni dalla data della rilevazione. Decorso tale periodo, i dati registrati sono cancellati con modalità automatica. Gli strumenti e i supporti elettronici utilizzati sono dotati dei sistemi di protezioni che garantiscono la tutela dei dati trattati.

Valutazione : Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati sono informati nei seguenti modi:
a) pubblicazione sul sito internet istituzionale di documentazione relative alle zone videosorvegliate e foto-sorvegliate;

b) installazione di apposita segnaletica permanente contenente l'informativa minima nelle aree in cui sono concretamente posizionate le telecamere, di cui al già richiamato Provvedimento in materia di videosorveglianza del Garante per la Protezione dei dati Personali del 08/04/2010. Sono fatti salvi i casi di prevenzione, accertamento o repressione dei reati.

c) informativa contenente gli elementi di cui all'art. 13 e 14 del Regolamento UE 2016/679 disponibile agevolmente senza oneri per gli interessati con modalità facilmente accessibili anche con strumenti informatici o telematici.

d) La segnaletica deve essere collocata prima del raggio di azione della telecamera, o nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; la stessa deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno.

e) In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, andranno installati più cartelli informativi.

f) L'Ente, nella persona del Titolare del trattamento dei dati, si obbliga ad informare la comunità cittadina dell'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di videosorveglianza, dell'eventuale incremento dimensionale dell'impianto stesso e dell'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Essendo l'ente una pubblica amministrazione che eroga servizi pubblici legalmente attribuiti non è tenuto all'acquisizione del consenso al trattamento dei dati, nei casi in cui questo sia dovuto viene acquisito per iscritto.

Valutazione : Accettabile

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

1. In relazione al trattamento di dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss., RGPD, su presentazione di apposita istanza, 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 qualora sussista uno dei motivi di cui all'art. 17 RGPD, 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, ai sensi dell'art. 21, RGPD.

2. L'istanza per l'esercizio dei diritti dell'interessato è presentata al Responsabile della Protezione dei dati dell'Ente, ai sensi dell'art. 38, paragrafo 4, RGDP ovvero al Responsabile del trattamento dei

dati individuato.

3. Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare:

a) il luogo, la data e la fascia oraria della possibile ripresa;

b) l'abbigliamento indossato al momento della possibile ripresa;

c) gli eventuali accessori in uso al momento della possibile ripresa;

d) l'eventuale presenza di accompagnatori al momento della possibile ripresa;

e) l'eventuale attività svolta al momento della possibile ripresa;

f) eventuali ulteriori elementi utili all'identificazione dell'interessato.

4. Il responsabile della protezione dei dati dell'Ente ovvero il responsabile del trattamento 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.

5. Qualora, ai sensi dell'art. 15, paragrafo 3, RGPD, l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei files contenenti le immagini in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della ripresa, in ossequio alla previsione di cui all'art. 15, paragrafo 4, RGPD.

6. I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

7. Nell'esercizio dei diritti di cui al comma 1 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.

Le istanze di cui al presente articolo possono essere trasmesse al titolare o al responsabile anche mediante lettera raccomandata o posta elettronica certificata, nel caso di esito negativo alla istanza 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.

Possono essere adottate misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato e per il tempo in cui ciò costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di:

1 . Non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;

2. Non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali;

3. Proteggere la sicurezza pubblica;

4. Proteggere la sicurezza nazionale;

Valutazione : Accettabile

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

Per esercitare il diritto alla cancellazione, se possibile in ragione dell'obbligo dell'ente di conservazione delle informazioni, gli interessati possono contattare direttamente il titolare o il designato del trattamento dei dati recandosi direttamente presso l'ente, a mezzo raccomandata o posta elettronica certificata.

Valutazione : Accettabile

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

Per esercitare il diritto di limitazione o opposizione, se possibile, gli interessati possono contattare direttamente il titolare o il designato del trattamento dei dati recandosi direttamente presso l'ente, a mezzo raccomandata o posta elettronica certificata.

Valutazione : Accettabile

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 nei contratti di appalto dei relativi servizi o con specifica comunicazione.

Valutazione : Accettabile

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.

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Sicurezza telecamere mobili

una volta connessa la IP cam con l'app / software, gli utenti possono visualizzare in streaming in tempo reale i video dalla telecamera di sicurezza, anche al di fuori della rete locale (LAN), mediante l' RTSP (Real Time Streaming Protocol) e del protocollo HTTPS (HyperText Transfer Protocol Secure), garantendo così un canale di comunicazione criptato e certificato dal Transport Layer Security (TLS) tra il client e il server localizzato in Francoforte (Germania);

Valutazione : Accettabile

Crittografia

tutti i dati (video) e altri concernenti la configurabilità, l'account e altre informazioni necessaria al funzionamento del sistema, sono conservati in modalità criptata;

Valutazione : Accettabile

Controllo degli accessi logici

l'utente che desidera aprire il video dalla scheda SD, deve prima inserire la password in formato crittografato AES, a cura di Dahua;

Valutazione : Accettabile

Tracciabilità

Il software prevede la registrazione e conseguente tracciabilità degli accessi logici e delle operazioni effettuate dagli autorizzati al trattamento dati.

Valutazione : Accettabile

Archiviazione

Non viene effettuata una vera e propria archiviazione, solo dopo aver filtrato le immagini e selezionato quelle rilevanti reati ambientali o all'ecologia i dati vengono copiati in chiavette protette da impronte digitali e consegnate al comando di polizia locale.

Valutazione : Accettabile

Minimizzazione dei dati

Vengono raccolti e conservati unicamente i dati necessari all'erogazione del servizio.

Valutazione : Accettabile

Vulnerabilità

ogni telecamera P2P o videoregistratore di rete (NVR) vengono identificati con un numero ID univoco (UID) registrato e integrato a livello di sviluppo, che viene utilizzato per eseguire il ping dei server P2P;
- una volta connessa la IP cam con l'app / software, gli utenti possono visualizzare in streaming in tempo reale i video dalla telecamera di sicurezza, anche al di fuori della rete locale (LAN), mediante l' RTSP (Real Time Streaming Protocol) e del protocollo HTTPS (HyperText Transfer Protocol Secure), garantendo così un canale di comunicazione criptato e certificato dal Transport Layer Security (TLS) tra il client e il server localizzato in Francoforte (Germania);
- tutti i dati (video) e altri concernenti la configurabilità, l'account e altre informazioni necessaria al funzionamento del sistema, sono conservati in modalità criptata;

Valutazione : Accettabile

Lotta contro il malware

L'antimalware è regolarmente istallato e costantemente aggiornato.

Valutazione : Accettabile

Sicurezza dei canali informatici

Il Firewall è correttamente installato e protetto

Valutazione : Accettabile

Contratto con il responsabile del trattamento

E' stipulato un contratto di fornitura con il responsabile del trattamento, il quale è nominato con atto specifico ai sensi dell'art. 28 del Regolamento UE 679/2016

Valutazione : Accettabile

Sicurezza telecamere fisse

Sicurezza telecamere fisse: Password protection, complicated password, HTTPS encryption, 802.1X authentication (EAP-TLS 1.2, EAP-LEAP, EAP-MD5), watermark, IP address filter, basic and digest authentication for HTTP/HTTPS, WSSE and digest authentication for ONVIF, TLS1.2

Valutazione : Accettabile

Controllo degli accessi fisici

Gli accessi fisici agli uffici sono limitati e controllati.

Valutazione : Accettabile

Backup

Backup giornaliero su server dati

Valutazione : Accettabile

Manutenzione

La manutenzione fisica dei dispositivi viene effettuata costantemente ed anche all'occorrenza.

Valutazione : Accettabile

Network storage telecamere fisse

Support micro SD/SDHC/SDXC card (128G) local storage, NAS (NFS,SMB/CIFS), ANR

Valutazione : Accettabile

Politica di tutela della privacy

Le politiche di tutela alla privacy comprendono il regolamento sulla videosorveglianza adottato dall'ente, nonchè l'osservanza del Regolamento UE 679/2016 con relativa nomina DPO

Valutazione : Accettabile

Gestione del personale

I dipendenti sono regolarmente invitati a partecipare ad incontri di formazione al fine di essere istruiti sul corretto trattamento dei dati personali.

Valutazione : Accettabile

Specifiche misure di sicurezza

Ai sensi di quanto previsto dall'articolo 24 del Reg. UE 201 6/679, i dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza sono protetti da misure di sicurezza tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato e trattamento non consentito o non conforme alle finalità di cui all'articolo 3 del presente Regolamento.

Ai sensi dell'art. 29 c. 2 della Direttiva UE 2016/680 il Titolare del trattamento, previa valutazione dei rischi, mette in atto misure volte a:

a. Vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»);

b. Impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»);

c. Impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»);

d. Impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente)
e. Garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»);

f. Garantire la possibilità di verificare e accertare gli organismi ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»);

g. Garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);

h. Impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»);

i. Garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»);

j. Garantire che le funzioni del sistema siano operative, 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»).

Valutazione : Accettabile

Sicurezza dei dati

Pen drive USB 3.0 128 GB
Accesso tramite autenticazione delle impronte digitali
Fino a 10 ID di impronte digitali consentiti
Riconoscimento ultraveloce – meno di 1 secondo
Protegge i file in modo sicuro utilizzando la crittografia AES a 256 bit

Valutazione : Accettabile

Anonimizzazione

I particolari tipi di dati, ovvero i C.d. dati sensibili, vengono trattati in maniera riservata unicamente dal personale strettamente necessario e a questo autorizzato, vengono resi sempre completamente anonimi quando pubblicati.

Valutazione : Accettabile

Sicurezza dell'hardware

Il server e le postazioni pc sono soggetti a continua manutenzione e protezione tramite firewall, antivirus e antimalware

Valutazione : Accettabile

Prevenzione delle fonti di rischio

Gli uffici dell'ente risultano rispettare le previsioni normative in materia di salute e protezione sui luoghi di lavoro.

Valutazione : Accettabile

Accesso illegittimo ai dati

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

Impatto limitato

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Perdita di dati, uso improprio di dati, diffusione di dati riservati o sensibili.

Quali sono le fonti di rischio?

Fonti di rischio interne ed esterne anche non umane.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Minimizzazione dei dati, Sicurezza telecamere mobili, Sicurezza telecamere fisse, Sicurezza dei canali informatici, Network storage telecamere fisse, Crittografia, Specifiche misure di sicurezza, Sicurezza dei dati, Controllo degli accessi logici

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

Limitata, Secondo le misure pianificate il rischio è limitato.

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

Limitata, Secondo le misure pianificate il rischio è limitato.

Valutazione : Accettabile

Modifiche indesiderate dei dati

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

Impatto limitato

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

Errore materiale, evento doloso o abuso di ufficio da parte degli addetti ai lavori, accesso ai dati da parte di soggetti esterni non competenti e non autorizzati.

Quali sono le fonti di rischio?

Fonti umane interne, fonti umane esterne, fonti non umane.

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

Crittografia, Vulnerabilità, Sicurezza dei canali informatici, Controllo degli accessi fisici, Controllo degli accessi logici, Sicurezza telecamere mobili, Tracciabilità, Lotta contro il malware, Minimizzazione dei dati, Politica di tutela della privacy, Prevenzione delle fonti di rischio, Contratto con il responsabile del trattamento, Sicurezza dei dati

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

Limitata, Il sistema di sicurezza adottato rende il rischio limitato

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

Limitata, Il sistema di sicurezza adottato rende il rischio limitato

Valutazione : Accettabile

Perdita di dati

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

Impatto limitato

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

Errore materiale, evento doloso o abuso di ufficio da parte di addetti ai lavori, accesso ai dati da parte di soggetti esterni non competenti e non autorizzate., Attacco hacker

Quali sono le fonti di rischio?

Fonti umane interne, fonti umane esterne, fonti non umane.

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

Archiviazione, Politica di tutela della privacy, Crittografia, Backup, Sicurezza dei canali informatici, Sicurezza telecamere fisse, Anonimizzazione, Sicurezza dell'hardware, Manutenzione, Lotta contro il malware, Minimizzazione dei dati, Gestione del personale, Controllo degli accessi fisici, Tracciabilità, Controllo degli accessi logici

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

Limitata, Le misure adottate dal titolare permettono di avere un rischio limitato

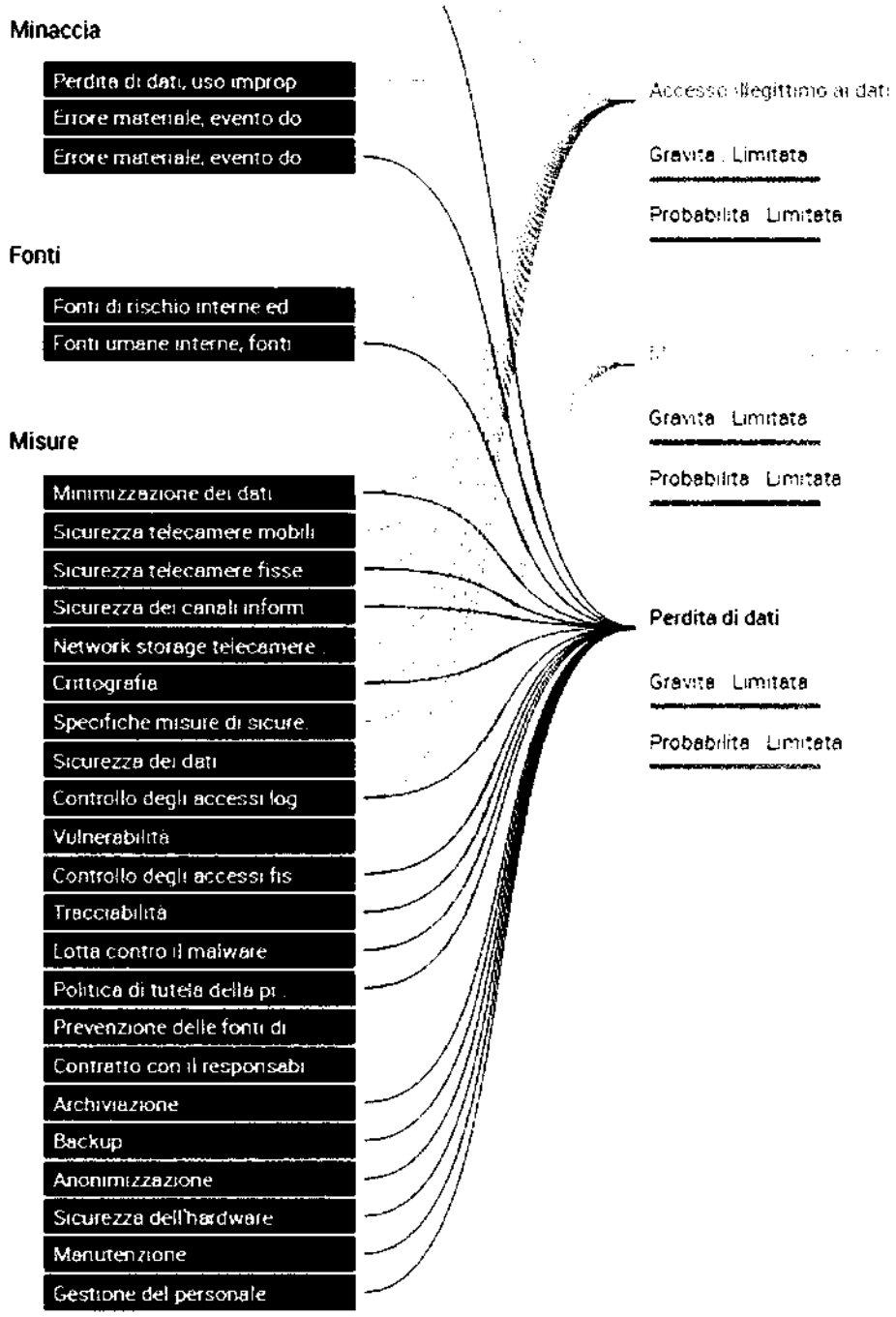
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, Le misure adottate dal titolare permettono di avere un rischio limitato

Valutazione : Accettabile

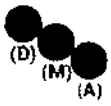
Panoramica dei rischi

Questa visualizzazione permette una panoramica globale e sintetica degli effetti prodotti dalle misure sulle componenti di rischio che esse contribuiscono a mitigare.



Mappatura del rischio

Gravita del rischio



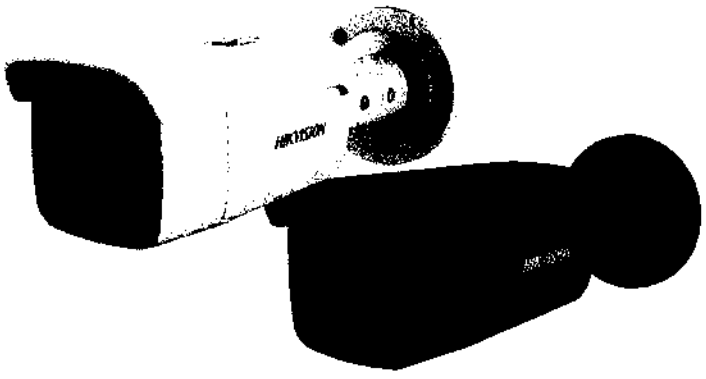
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

Probabilità del rischio

ALL 1

HIKVISION

DS-2CD2T65G1-I5/I8
6 MP IR Fixed Bullet Network Camera



Key Features

- Up to 6 megapixel high resolution
- Max. 3072 × 2048 @20fps
- 2.8 mm/4 mm/6 mm fixed lens, optional
- H.265, H.265+, H.264+, H.264
- 120dB WDR
- Powered by Darkfighter
- 12 VDC & PoE (802.3af, class 3)
- Support on-board storage, up to 128 GB
- IP67
- BLC/3D DNR/ROI/HLC
- Color: 0.008 Lux @ (F1.2, AGC ON), 0.014 Lux @ (F1.6, AGC ON)

Specification

Camera	
Image Sensor	1/2.4" Progressive Scan CMOS
Min. Illumination	Color: 0.008 Lux @ (F1.2, AGC ON), 0.014 Lux @ (F1.6, AGC ON)
Shutter Speed	1/3 s to 1/100,000 s
Slow Shutter	Yes
Focal length	2.8/4/6 mm
Focus	Fixed
Lens	2.8 mm, horizontal FOV: 99°, vertical FOV: 61°, diagonal FOV: 128° 4 mm, horizontal FOV: 80°, vertical FOV: 51°, diagonal FOV: 101° 6 mm, horizontal FOV: 60°, vertical FOV: 38°
Lens Mount	M12
Aperture	F1.6
Day &Night	IR cut filter
DNR	3D DNR
Wide Dynamic Range	120dB
3-Axis Adjustment	Pan: 0° to 360°, tilt: 0° to 90°, rotate: 0° to 360°
Compression Standard	
Video Compression	Main stream: H.265/H.264 Sub-stream: H.265/H.264/MJPEG Third stream: H.265/H.264
H.264 Type	Main Profile/High Profile
H.264+	Main stream supports
H.265 Type	Main Profile
H.265+	Main stream supports
Video Bit Rate	32 Kbps to 16 Mbps
Image	
Max. Resolution	3072 × 2048
Main Stream	50Hz: 20 fps (3072 × 2048, 3072 × 1728, 2944 × 1656), 25 fps (2560 × 1440, 1920 × 1080, 1280 × 720) 60Hz: 20 fps (3072 × 2048, 3072 × 1728, 2944 × 1656), 30 fps (2560 × 1440, 1920 × 1080, 1280 × 720)
Sub-Stream	50Hz: 25fps (640 × 480, 640 × 360, 320 × 240) 60Hz: 30fps (640 × 480, 640 × 360, 320 × 240)
Third Stream	50Hz: 25fps (1280 × 720, 640 × 360, 352 × 288) 60Hz: 30fps (1280 × 720, 640 × 360, 352 × 240)
Image Enhancement	BLC/3D DNR/HLC
Image Setting	Rotate mode, saturation, brightness, contrast, sharpness, AGC, and white balance adjustable by client software or web browser
ROI (Region of Interest)	Support 1 fixed region for main stream and sub-stream separately
Day/Night Switch	Day/Night/Auto/Schedule

* Note: When the main stream resolution is 2944 × 1656 and above, max frame rate is 20 fps for all streams.

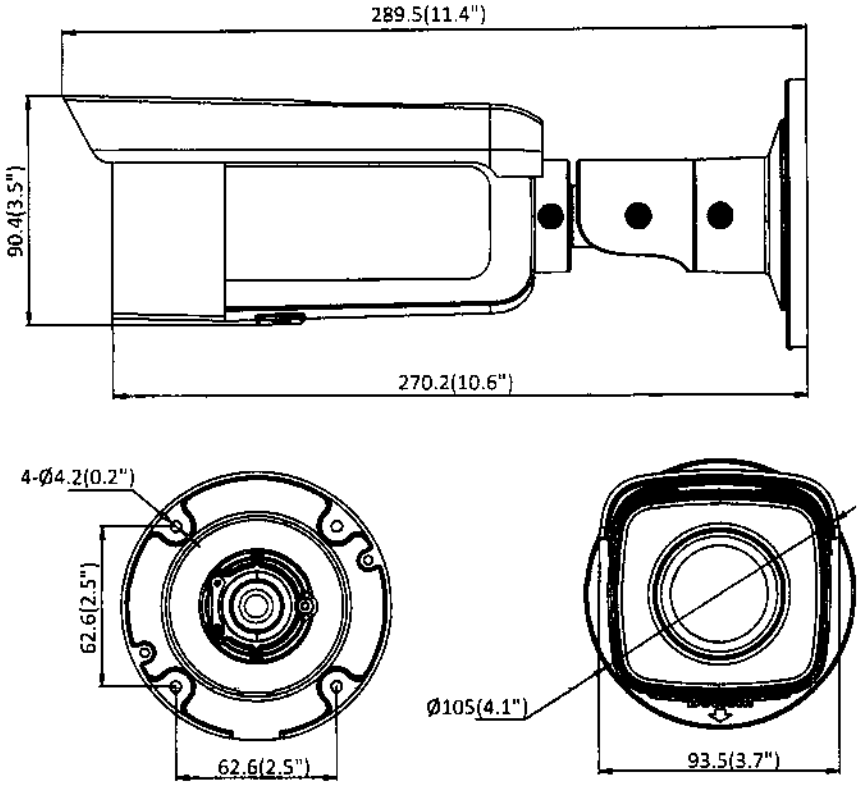
Network	
Network Storage	Support micro SD/SDHC/SDXC card (128G) local storage, NAS (NFS,SMB/CIFS), ANR
Protocols	TCP/IP, UDP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, PPPoE, NTP, UPnP, SMTP, SNMP, IGMP, 802.1X, QoS, IPv6, UDP, Bonjour, SSL/TLS
General Function	Anti-flicker, three streams, heartbeat, mirror, privacy masks, password reset via e-mail, pixel counter, HTTP listening

API	ONVIF (PROFILE S, PROFILE G, PROFILE T), ISAPI, SDK
Security	Password protection, complicated password, HTTPS encryption, 802.1X authentication (EAP-TLS 1.2, EAP-LEAP, EAP-MD5), watermark, IP address filter, basic and digest authentication for HTTP/HTTPS, WSSE and digest authentication for ONVIF, TLS1.2
Simultaneous Live View	Up to 6 channels
User/Host	Up to 32 users 3 levels: Administrator, Operator and User
Client	iVMS-4200, Hik-Connect, Hik-Central
Web Browser	Plug-in required live view: IE8+ Plug-in free live view: Chrome 57.0+, Firefox 52.0+, Safari 11+ Local Service: Chrome 41.0+, Firefox 30.0+
Interface	
Communication Interface	1 RJ45 10M/100M self-adaptive Ethernet port
On-board Storage	Built-in micro SD/SDHC/SDXC slot, up to 128 GB
Reset Button	Yes
Smart Feature-set	
Smart Event	Line crossing detection, intrusion detection, unattended baggage detection, object removal detection, face detection, scene change detection
Basic Event	Motion detection, video tampering alarm, exception (network disconnected, IP address conflict, illegal login, HDD full, HDD error)
Linkage Method	Trigger recording: memory card, network storage, pre-record and post-record Trigger captured pictures uploading: FTP, HTTP, NAS, Email Trigger notification: HTTP, ISAPI, Email
General	
Operating Conditions	-30 °C to +60 °C (-22 °F to +140 °F), humidity 95% or less (non-condensing)
Web Client Language	32 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)
Power Supply	12 VDC ± 25%, 5.5 mm coaxial power plug PoE (802.3af, class 3)
Power Consumption	-I5: 12 VDC, 0.5 A, max: 8 W PoE: (802.3af, 36 VDC to 57 VDC), 0.4 A to 0.2 A, max: 9.5 W -I8: 12 VDC, 1.0 A, max: 11 W PoE: (802.3af, 36 VDC to 57 VDC), 0.4 A to 0.2 A, max: 12.9 W
IR Range	-I5: Up to 50 m -I8: Up to 80 m
Wavelength	850 nm
Protection Level	IP67
Material	Front cover: metal, back cover: metal
Dimensions	Camera: Φ105 × 289.5 mm (4.1" × 11.4")
Weight	Camera: 1000 g (2.2 lb.) With package: 1500 g (3.3 lb.)

Available Model

DS-2CD2T65G1-I5 (2.8/4/6 mm), DS-2CD2T65G1-I8 (2.8/4/6 mm)

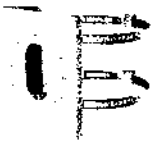
Dimension



Unit: mm(inch)

Accessory

DS-1260ZJ
Junction Box



DS-1275ZJ-S-SUS
Vertical Pole Mount

DS-1276ZJ-SUS
Corner Mount

DS-1260ZJ(Black)
Junction Box

DS-1275ZJ-SUS(Black)
Vertical Pole Mount

DS-1276ZJ-SUS(Black)
Corner Mount

HIKVISION

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

Hikvision USA
Hikvision Europe
Hikvision Middle East
Hikvision Russia
Hikvision India
Hikvision Italy
Hikvision France
Hikvision Spain
Hikvision Poland
Hikvision UK
Hikvision Singapore
Hikvision Oceania
Hikvision Canada
Hikvision Korea
Hikvision Brazil
Hikvision Africa
Hikvision Hong Kong

05060020200413

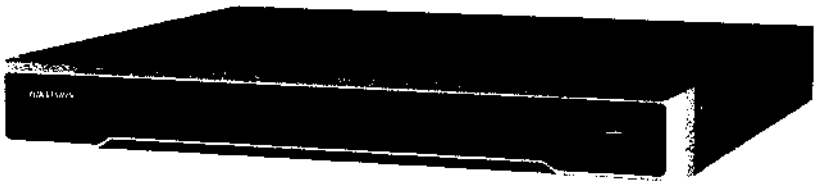
ALL 2

Postazione	Coordinate	Codice palo
C.da Caitina	36.843152, 14.757669	029019
C.da Fasana	36.878997, 14.775278	107032
Maganuco	36.717096, 14.808698	073045
Via Taormina / Via Agrigento	36.709330, 14.791465	071018
C.da Musebbi	36.838169, 14.785264	163030
C.da Cava Gucciardo Quartarella	36.825217, 14.778579	057010
C.da S.Elena	36.852743, 14.797993	075001
Via Sorda Sampieri	36.814530, 14.788062	058007
Giorgio Noto	36.86739, 14.74678	042006
C.da Busita	36.80863, 14.81862	ND
Via Sorda Scicli	36.83278, 14.75815	0060025
Lit. Pozzallo-Sampieri	36.71524, 14.78553	179049

ALL 3

HIKVISION

DS-7600NI-K2/P SERIES NVR



Features and Functions

Professional and Reliable

- Dual-OS design to ensure high reliability of system running
- ANR technology to enhance the storage reliability when the network is disconnected

HD Input

- H.265/H.265+/H.264/H.264+/MPEG4 video formats
- Connectable to the third-party network cameras
- Up to 32 IP cameras can be connected
- Recording at up to 8 MP resolution
- Supports live view, storage, and playback of the connected camera at up to 8 MP resolution

HD Output

- HDMI and VGA independent outputs provided
- HDMI Video output at up to 4K (3840 × 2160) resolution

HD Storage

- Up to 2 SATA interfaces connectable for recording and backup
- Storage space effectively saved by 50% to 70% with the use of H.264+ decoding format

HD Transmission

- 1 self-adaptive 10M/100M/1000 Mbps network interface
- 8/16 independent PoE network interfaces are provided

Various Applications

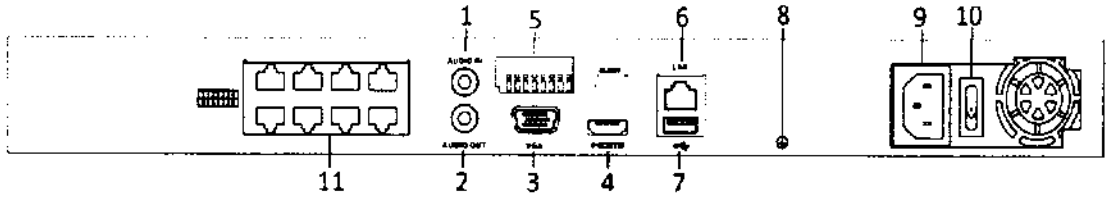
- Adopt stream over TLS encryption technology (enhanced SDK service and RTP over HTTPS protocol) which provides more secure stream transmission service (max. 128 Mbps TLS stream outgoing bandwidth)
- Centralized management of IP cameras, including configuration, information import/export, real-time information display, two-way audio, upgrade, etc.
- Connectable to smart IP cameras from Hikvision and the recording, playing back, and backing up of VCA alarms can be realized
- VCA detection alarm is supported
- Instant playback for assigned channel during multi-channel display mode
- Smart search for the selected area in the video; and smart playback to improve the playback efficiency
- Supports HDD quota and group modes; different capacity can be assigned to different channels
- Hik-Connect for easy network management

HIKVISION

Specifications

Model		DS-7608NI-K2/8P	DS-7616NI-K2/16P	DS-7632NI-K2/16P
Video/ Audio input	IP video input	8-ch	16-ch	32-ch
	Incoming bandwidth	80 Mbps	160 Mbps	256 Mbps
	Outgoing bandwidth	160 Mbps		
Video/ Audio output	HDMI output resolution	4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz		
	VGA output resolution	1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz		
	Audio output	1-ch, RCA (Linear, 1 KΩ)		
Decoding	Decoding format	H.265/H.265+/H.264/H.264+/MPEG4		
	Recording resolution	8MP/6MP/5MP/4MP/3MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF /CIF/QCIF		
	Synchronous playback	8-ch	16-ch	16-ch
	Capability	2-ch @ 8 MP (25fps) / 4-ch @ 4MP (30fps) / 8-ch @ 1080p (30fps)		
Network management	Network protocols	TCP/IP, DHCP, Hik-Connect, DNS, DDNS, NTP, SADP, SMTP, NFS, iSCSI, UPnP™, HTTPS		
Hard disk	SATA	2 SATA interfaces		
	Capacity	Up to 6 TB capacity for each HDD		
External interface	Two-way audio	1-ch, RCA (2.0 Vp-p, 1kΩ)		
	Network interface	1 RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface		
	USB interface	Front panel: 1 × USB 2.0; Rear panel: 1 × USB 3.0		
	Alarm in/out	4/1		
POE interface	Interface	8, RJ-45 10/100 Mbps self-adaptive Ethernet interface	16, RJ-45 10/100 Mbps self-adaptive Ethernet interface	
	Power	≤ 120 W	≤ 200 W	
	Supported standard	IEEE 802.3 af/at		
	Power supply	100 to 240 VAC		
General	Power Consumption (without hard disk)	≤ 180 W	≤ 280 W	
		≤ 15 W (without enabling PoE)		
	Working temperature	-10 °C to 55 °C (14 °F to 131 °F)		
	Working humidity	10 to 90 %		
	Dimensions (W × D × H)	385 × 315× 52 mm (15.2" × 12.4" × 2.0")		
	Weight (without hard disk)	≤ 3 kg (6.6 lb)		

Physical Interfaces



NOTE

The DS-7616NI-K2/16P and DS-7632NI-K2/16P provide 16 network interfaces with PoE function.

Index	Description	Index	Description
1	AUDIO IN	7	USB 3.0 Interface.
2	AUDIO OUT	8	GND
3	VGA Interface	9	100 to 240 VAC power supply
4	HDMI Interface	10	Power Switch
5	Controller Port, Alarm In/Alarm Out	11	Network Interfaces with PoE function
6	LAN Network Interface		

Available Models

DS-7608NI-K2/8P, DS-7616NI-K2/16P, DS-7632NI-K2/16P

HIKVISION

Headquarters

Hikvision USA | Hikvision Europe | Hikvision Middle East | Hikvision Russia | Hikvision India

Hikvision Italy | Hikvision France | Hikvision Spain | Hikvision Poland | Hikvision UK

Hikvision Singapore | Hikvision Oceania | Hikvision Canada | Hikvision Korea | Hikvision Brazil

Hikvision Africa | Hikvision Hong Kong

All. 4

DH-IPC-HUM8230

2MP Covert Pinhole Network Camera

- 1/2.8" 2Megapixel progressive scan STARVIS™ CMOS
- H.265&H.264 triple-stream encoding
- 25/30fps@1080P(1920×1080)
- Day/Night(Electronic), 3DNR,AWB,AGC,BLC
- Smart detection
- 2.8mm Fixed Lens
- Micro SD memory, PoE

System Overview

Dahua covert camera used modular design, provide an independent main unit and a miniature sensor unit (with 8-meters cable), with cylindrical pinhole lens and cylindrical standard lens for the customers to choose,It can be easily installed into any indoor environments, make this camera ideal for the ATMs(Automatic Teller Machines), banks, stores, hotels and offices.

Functions

Intelligent Video System (IVS)

Dahua camera has a built-in video analysis based on intelligent algorithms and can achieve the following:Tripwire,Intrusion,Abandoned/ Missing can timely, quickly and accurately respond to monitoring events in specific area. It enhances monitoring efficiency. At the same time, the camera can support face detection,it can quickly capture a face and upload the image to the server. In addition the camera also supports intelligent tamper detection,through dramatic changes in the scene it will send out warning information to ensure effective monitoring.

Protection

Supporting ±30% input voltage tolerance, this camera suits even the most unstable conditions for outdoor applications. Its 6KV lightning rating provides effective protection for both the camera and its structure against lightning.

HEVC (H.265)

H.265 ITU-T VCEG is a new video coding standard. H.265 Following standard developed around the existing video coding standard H.264 , some retain the original technology , while some of the relevant technology to improve the new technology uses advanced technology to improve the relationship between the code stream , encoding quality , and the delay between algorithm complexity , optimize settings specific contents include : Improve compression efficiency , improve the robustness and error recovery capabilities, real-time to reduce the delay, reduce channel acquisition time and a random access delay , reduce complexity , etc

Smart H.265+

Deliver high quality video without straining the network, Smart H.265+ is the optimized implementation of H.265. The Smart H.265+ encoding technology includes a scene adaptive encoding strategy, dynamic GOP, dynamic ROI, flexible multi-frame reference structure and intelligent noise reduction, providing saving of up to 70% of bandwidth and storage when compared with standard H.265.

Technical Specification

Camera

Image Sensor	1/2.8" 2Megapixel progressive scan CMOS
Effective Pixels	1920(H)x1080(V)
RAM/ROM	256MB/32MB
Scanning System	Progressive
Minimum Illumination	L1: 0.07Lux/F2.4 (Color), 0.007Lux/F2.4 (B/W) L3: 0.009Lux/F1.8 (Color), 0.001Lux/F1.8 (B/W)
S/N Ratio	More than 50dB
IR Distance	N/A
IR On/Off Control	N/A
IR LEDs	N/A

Lens

Lens Type	Fixed
Mount Type	Board-in
Focal Length	2.8mm
Max. Aperture	Sensor Unit L1:F2.4 Sensor Unit L3:F1.8
Angle of View	Sensor Unit L1 H:104° ,V:57° Sensor Unit L3 H:118° ,V:60°
Optical Zoom	N/A
Focus Control	Fixed
Close Focus Distance	N/A

Pan/Tilt/Rotation

Pan/Tilt/Rotation Range	N/A

Intelligence

IVS (optional)	Tripwire, Intrusion, Object Abandoned/Missing
Advanced Intelligent Functions	Face Detection

Video

Compression	H.265+/H.265/H.264+/H.264
Streaming Capability	3 Streams
Resolution	1080P(1920×1080)/ 1.3M(1280x960)/ 720P(1280x720)/ D1(704×576/704x480)/ VGA(640x480)/ CIF(352×288/342x240)
Frame Rate	Main Stream: 1080P(1~25/30fps) Sub Stream: D1 (1 ~ 25/30fps) Third Stream: 1080P(1~25/30fps)
Bit Rate Control	CBR/VBR
Bit Rate	H.264: 24Kbps~ 9472Kbps H.265: 14Kbps~ 5632Kbps
Day/Night	Electronic
BLC Mode	BLC / HLC / DWDR
White Balance	Auto/Natural/Street Lamp/Outdoor/Manual
Gain Control	Auto/Manual
Noise Reduction	3D DNR
Motion Detetion	Off / On (4 Zone, Rectangle)
Region of Interest	Off / On (4 Zone)
Electronic Image Stabilization (EIS)	N/A
Smart IR	N/A
Defog	N/A
Digital Zoom	16x
Flip	0°/90°/180°/270°
Mirror	Off / On
Privacy Masking	Off / On (4 Area, Rectangle)

Audio

Compression	G.711a/ G.711Mu/ AAC/ G.726

Network

Ethernet	RJ-45 (10/100Base-T)
Protocol	HTTP;HTTPs;TCP;ARP;RTSP;RTP;UDP;SMTP;FTP;DHCP;DNS;DDNS;PPPOE;IPv4/v6;QoS;UPnP;NTP;Bonjour;802.1x;Multicast;ICMP;IGMP;SNMP
Interoperability	ONVIF, PSIA, CGI
Streaming Method	Unicast / Multicast
Max. User Access	10 Users/20 Users
Edge Storage	NAS Local PC for instant recording Mirco SD card 128GB
Web Viewer	IE, Chrome, Firefox, Safari
Management Software	Smart PSS, DSS, Easy4ip
Smart Phone	iOS, Android

Certifications

Certifications	CE (EN 60950:2000) UL:UL60950-1 FCC: FCC Part 15 Subpart B

Interface

Video Interface	N/A
Audio Interface	1/1 channel In/Out
RS232	1 port
Alarm	2/2 channel In/Out

Electrical

Power Supply	DC12V, PoE(802.3af)(Class 0)
Power Consumption	≤6W

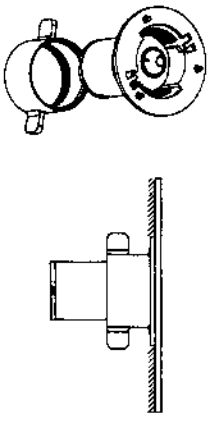
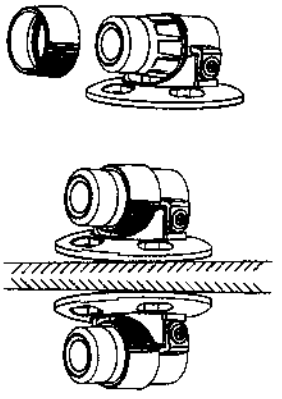
Environmental

Operating Conditions	-30° C ~ +60° C (-22° F ~ +140° F) / Less than 95% RH
Strorage Conditions	-30° C ~ +60° C (-22° F ~ +140° F) / Less than 95% RH
Ingress Protection	N/A
Vandal Resistance	N/A

Construction

Casing	Metal
Dimensions	Main Unit:110.0mm×82.7mm×24.0mm (4.33"×3.26"×0.95") Sensor Unit L1:Φ26.5mm×48.31mm(Φ1.04"×1.9") Sensor Unit L3:Φ26.5mm×50.38mm(Φ1.04"×2.0")
Net Weight	Main Unit:0.2Kg (lb) Sensor Unit L1:0.22Kg (lb) Sensor Unit L3:0.23Kg (lb)
Gross Weight	Main Unit:0.36Kg (lb) Sensor Unit L1:0.31Kg (lb) Sensor Unit L3:0.32Kg (lb)

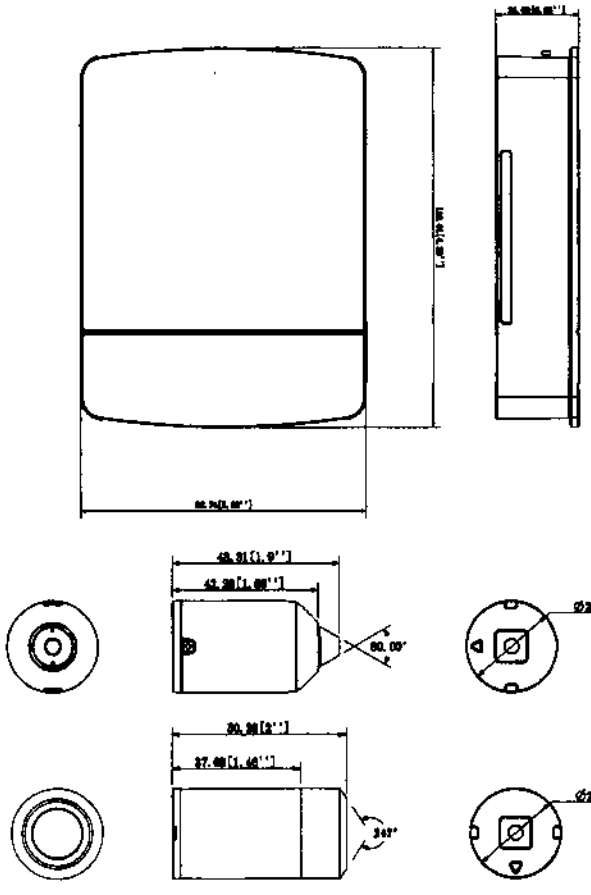
Accessories

Wall/Ceiling Mount	Plane Mount
	

Ordering Information

Type	Part Number	Description
2MP camera	DH-IPC-HUM8230P-E1	2MP Covert Pinhole Network Camera, Main Unit,PAL
	DH-IPC-HUM8230N-E1	2MP Covert Pinhole Network Camera, Main Unit,NTSC
	IPC-HUM8230P-E1	2MP Covert Pinhole Network Camera, Main Unit, PAL
	IPC-HUM8230N-E1	2MP Covert Pinhole Network Camera, Main Unit, NTSC
	IPC-HUM8230-L1	2MP Cylindrical Sensor Unit,Pinhole Lens with 8 meters Cable
	IPC-HUM8230-L3	2MP Cylindrical Sensor Unit,Standard Lens with 8 meters Cable
Accessories (Included)	Sensor Unit L1	Pinhole Wall/Ceiling Mounting Bracket
	Sensor Unit L3	Pinhole Plane Mounting Bracket

Dimensions (mm/inch)



ALL 5

HIKVISION

iVMS-4200

Overview

iVMS-4200 is versatile video management software for DVRs, NVRs, IP cameras, encoders, decoders, VCA devices, etc. It provides several functionalities, including real-time live view, video recording, remote search and playback, file backup, alarm receiving, etc. for connected devices, and meets the needs of small and medium-sized projects.

With a flexible distributed structure and easy-to-use operations, the iVMS-4200 client software is widely applied to surveillance projects in financial, public security, military, telecommunications, transport, electricity, education, water conservancy industries, etc.

Main Features

General
- Applicable to local and wide area networks
- E-map function
- Remote configuration for added devices
- Management of user permissions
- Password-protected device activation
- Resetting of password via device's QR code
- Security Control Panel and Video Intercom management support
- Support for communication with the iVMS-4200 Access Control Client
- Hardware decoding support for live view and playback

Network
- Connection of encoding devices, decoding devices, Hik-Connect P2P Cloud devices, stream media server, third-party encoding devices, transcoder, cascading server, super NVR connectable
- Online user verification
- NTP time synchronization protocol
- Search active online devices
- Device addition via the IP Server; batch importing of encoding devices
- QR code generation for encoding devices
- Two-way audio and broadcast function

Live View
- Newly-added support for H.265 and H.264+ video encoding formats
- Viewing of settings and instant playback
- Main/auxiliary screen live view
- Maximum support for a 64-window standard-screen division (48-window sub-stream), and a 48-window wide-screen division
- Custom window division configuration
- Live view in Fisheye mode for fisheye cameras
- Disconnecting of background videos when live viewing one camera
- Support for PC keyboard shortcuts to conveniently access commonly used actions
- Extra channels for simultaneous HD live view on a 64-bit operating system
- Live view of offline cameras via configured stream media server
- Fisheye camera and speed dome linkage function

PTZ Control
- Remote PTZ control, preset, patrol, and pattern settings
- 3D positioning, auxiliary focus, and wiper function
- Analog speed dome local menu display via the PTZ control panel
- Support for PTZ control of one-touch patrol and one-touch park

Alarm Management
- Multiple camera linkage actions supported
- Device arming and alarm output control
- Alarm configuration for camera event, alarm input, zone event, and device exceptions
- Support for combined, mixed-traffic detection, and CVR alarms
- Search and export of linked alarm log pictures
- Possibility to view latest priority alarm when viewing alarm information in the alarm pop-up window
- Support for custom alarm sounds

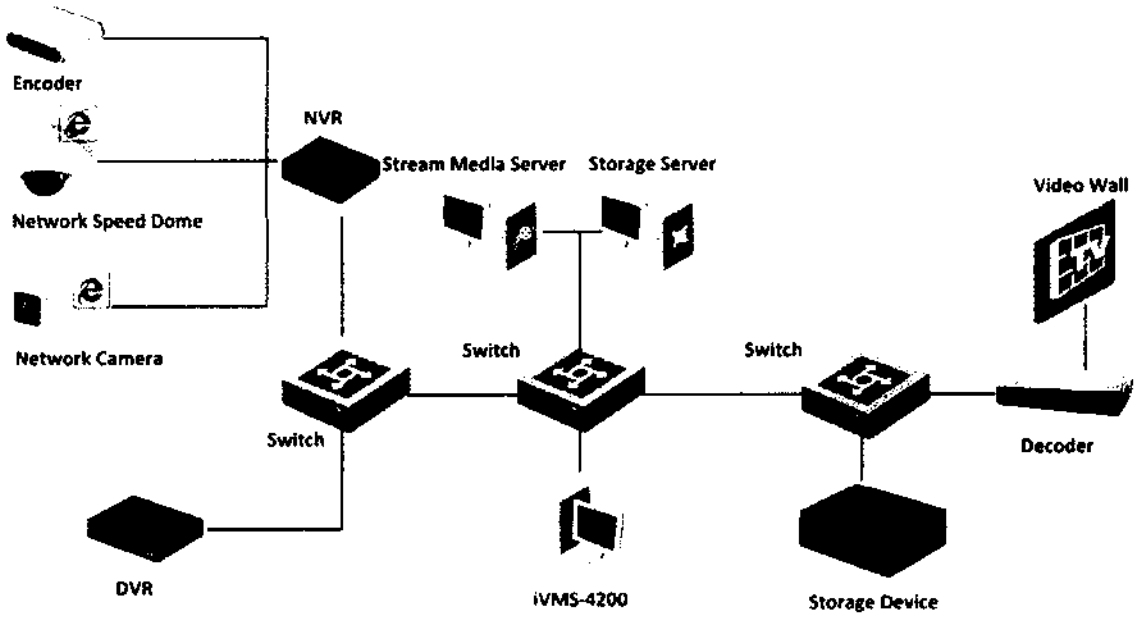
Recording
- Support for H.265 and H.264+ video encoding formats
- Support for main stream and sub-stream recording playback
- Remote manual recording support
- Recording schedule for continuous, event, and command recording
- SAN and CVR configuration for CVR device
- Video file overwriting and expired video deletion

Playback
- Local and remote playback
- Instant, normal, alarm input, event, ATM, VCA, and fisheye playback
- Maximum of 16-ch synchronous playback supported
- Pre-play time setting for event playback
- Filtering of searched video via advanced searching during VCA playback
- Support for skipping irrelevant video during VCA playback
- Support for searching video files that contain POS information
- Frame extracting support for high-speed playback
- Video Player for viewing of downloaded video files included in the installation directory

Backup
- Downloading of video files to PC
- Exporting of video files via remote configuration
- Search and backup log
- Import and export of configuration file
- Support for merging video files that are downloaded by date

Statistics
- Heat map, people counting, counting, road traffic, face retrieval, license plate retrieval, behavior analysis, and face capture data statistics

Typical Application



System Requirements

Client Requirements for H.264 Encoding Format

Minimum	**Processor**	Intel® Core™ i3-2100 @ 3.10 GHz
	Memory	2 GB of RAM
	Operating System	Microsoft® Windows 7 (64-bit)
	NIC	Realtek® PCIe GbE Family Controller
	Video Card	NVIDIA GeForce GTS 430
Recommended	**Processor**	Intel® Core™ i5-4590 @ 3.30 GHz
	Memory	8 GB of RAM
	Operating System	Microsoft® Windows 7 (64-bit)
	NIC	Realtek® GbE Network Interface Card
	Video Card	Intel HD Graphics 4600/2G
High Performance	**Processor**	Intel® Core™ i7-5930K @ 3.50 GHz
	Memory	16 GB of RAM
	Operating System	Microsoft® Windows 7 (64-bit)
	NIC	Intel® Ethernet Connection (2) I218-V
	Video Card	NVIDIA GeForce GTX970

Maximum Number of Cameras Viewed per Client (Software Decoding)

Encoding Format	Resolution	Bit Rate (Mbps)	Frame Rate (fps)	Maximum Number of Cameras Viewed Simultaneously		
				Minimum	Recommended	High Performance
H.264	4CIF	1	25	16	32	48
	HD720p	2	25	12	16	32
	1080p	4	25	4	8	16
	600W	11	25	4	5	6
H.264+	HD720p	2	25	13	17	32
	1080p	4	25	6	7	19
H.265	HD720p	2	25	8	9	26
	1080p	4	25	3	4	13

Maximum Number of Cameras Viewed per Client (Software Decoding and Hardware Decoding Combined)

Encoding Format	Resolution	Bit Rate (Mbps)	Frame Rate (fps)	Maximum Number of Cameras Viewed Simultaneously	
				Intel® Xeon CPU E3-1225 V3 8 GB of RAM Windows® Embedded Standard (64-bit) Intel® HD Graphics P4600/P4700	Intel i7-4790K 8 GB of RAM Microsoft® Windows 7 (64-bit) NVIDIA GeForce GTX970
H.264	HD720p	2	25	48	32
	1080p	4	25	30	16

Note: The above parameters are estimated and for reference only. Under same resolution and frame rate, the bitrate of different camera manufacturers may be different. Moreover, the decoding performance may also be different for different manufacturers.

Server Requirements (Stream Media Server)

Minimum	Processor	Intel® Core™ 2 Duo E6850 3.0 GHz
	Memory	4 GB of RAM
	HDD	80 GB Hard Drive
	NIC	100/1000 Mbps Ethernet Network Interface Card
	Video Card	Standard SVGA Video Card
Recommended	Processor	Quad Core Intel® Xeon® E5640 2.66 GHz
	Memory	16 GB of RAM
	Operating System	64-bit Operating System
	HDD	80 GB SATA II Hard Drive
	NIC	GbE Network Interface Card
	Video Card	Standard SVGA Video Card

Specifications

Model		iVMS-4200
Client	Encoding Device	Maximum of 256 encoding devices supported
	Group	Maximum of 256 groups supported Maximum of 256 channels can be imported to each group
	Channel	Maximum of 1024 channels can be imported to all groups
	Stream Media Server	Maximum of 16 stream media servers supported
	Decoding Device	Maximum of 64 decoding devices supported
	Playback	Maximum 16-channel playback. For best performance, 1 to 4 cameras at a time are recommended for remote playback
	Live View	Maximum of 4 output screens supported, maximum 32 live views recommended
	Auxiliary Screen Preview	Maximum of 4 auxiliary screens supported for live view
	User	Maximum of 50 users and one super user supported
	Playback	Maximum of 16-ch playback supported at a time
	Synchronous Playback	Maximum of 16-ch synchronous playback supported
	E-map	Maximum of 256 E-maps can be added
	Download	Maximum of 16 downloading tasks supported at a time
Stream Media Server	Incoming/Outgoing Stream	Maximum of 64-ch incoming video streams supported. Maximum of 200-ch outgoing video stream supported

ALL. 6

steam service

Specialisti nella protezione dei tuoi Valori.

·Informatica ·Domotica ·Sistemi di Sicurezza ·Assistenza

Le misure di sicurezza adottate su e-Killer Flex per la protezione dei dati sono:

1. Conservazione delle immagini limitata alla capacità della memoria di massa (micro SD), installata appositamente da 128 GB per limitare le registrazioni di e-Killer (da 3 a 5 giorni in base alle impostazioni). Successivamente, le immagini, vengono automaticamente distrutte dalla registrazione di nuove immagini (operazione di sovrascrittura). È Possibile comunque formattare la memoria micro SD da remoto (anche quindi in caso di rilevazione furto videocamera a seguito cambiamento inquadratura o allarme/GPS tracker/visualizzazione in diretta da remoto) purchè in presenza di collegamento dati con la telecamera tramite la Sim Card installata;
   In ogni caso la memoria micro sd viene automaticamente formattata dopo 7 giorni pertanto non è possibile conservare le registrazioni all'interno della memoria per un periodo superiore ai 7 giorni.

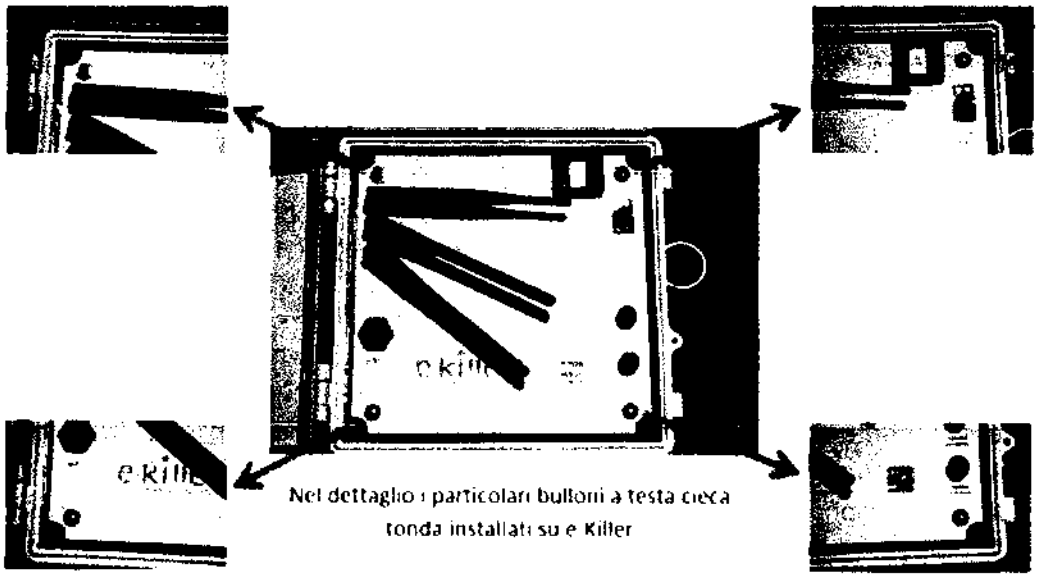
2. Il responsabile ed ogni singolo incaricato saranno dotati di proprie credenziali di accesso (login e password) ad e-Killer. I singoli incaricati, dovranno autonomamente variare la propria password almeno ogni 6 mesi.

3. L'accesso ai dati può essere effettuato esclusivamente da operatori muniti di credenziali di accesso valide e strettamente personali, inizialmente rilasciate da Steam Service ed immediatamente modificabili in autonomia da parte del responsabile del trattamento dei dati. Con queste credenziali, è possibile individuare diversi livelli di accesso ad ogni singolo operatore a seconda dei compiti attribuiti, permettendo unicamente di effettuare le operazioni di propria competenza. Quindi si possono distinguere coloro che sono unicamente abilitati a visionare le immagini, dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. visionare le registrazioni, copiarle e/o cancellarle). La gestione di e-Killer è affidata a specifici addetti all'interno del Corpo della Polizia Municipale;

4. L'accesso al sistema avviene esclusivamente da postazioni dedicate situate all'interno della sede del Comando di Polizia Municipale. In queste postazioni, già munite di loro credenziali d'accesso, viene installato un software per gestire e-Killer, il quale ha ulteriori credenziali di accesso univoche per ogni addetto che vi accede;

STEAM Service
di Stefano Amato
P.zza Bagolino 14
91011 - Alcamo (TP)
Tel: 0924 21765
Cell: 338 8553341
info@steamservice.it
www.steamservice.it
P.Iva 02035430814
C.F. MTASFN78T02A176S
REA N° TP-140814

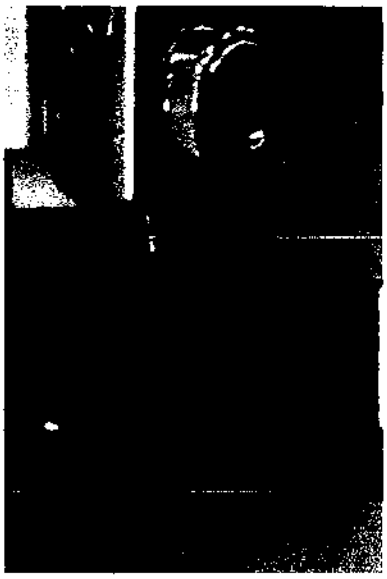
5. L'accesso fisico alla memoria micro SD, contenente le registrazioni, è possibile soltanto al tecnico specializzato di Steam Service (azienda produttrice di e-Killer), in possesso di particolare attrezzatura dedicata. Per aprire il dispositivo, il tecnico, dovrà seguire una specifica procedura che gli consentirà di accedere alla parte interna del dispositivo considerato che è protetto grazie all'uso di particolari bulloni a testa cieca tonda che ne impediscono l'apertura e quindi riducono il rischio di accesso non autorizzato all'alloggio della scheda micro SD. Tale scheda micro SD, è protetta da crittografia, pertanto non è possibile leggere la memoria su altri dispositivi



Nel dettaglio i particolari bulloni a testa cieca tonda installati su e-Killer

6. Il dispositivo e-Killer, al momento dell'istallazione nel luogo prescelto da videosorvegliare, viene debitamente mimetizzato, nascosto e chiuso con una doppia chiusura dell'involucro della videocamera e con dei lucchetti esterni. Inoltre e-Killer viene fissato con una gabbia di ancoraggio ed una catena ad un palo (o qualcosa di simile). Quindi, per aprire il dispositivo, bisogna essere in possesso delle due chiavi che chiudono le serrature di sicurezza;

7. La rete Wi-Fi generata da e-Killer per collegarsi al dispositivo, può essere nascosta, tramite apposito tasto fisico, per evitare accessi illegali alla rete. Inoltre, tale rete, anche se visibile, usa un protocollo di protezione di tipo WPA2 ed una crittografia AES 128bit.
   In aggiunta, il dispositivo è sprovvisto di tasto WPS per il collegamento;



8. Un ulteriore accorgimento contro l'accesso non autorizzato ad e-Killer consiste nella funzione "Illegal Access" che è in grado di bloccare il dispositivo dopo 5 tentativi di inserimento credenziali errate. Tale evento può essere segnalato tramite e-mail al responsabile del servizio.

Letto. approvato e sottoscritto

IL SINDACO

L'ASSESSORE ANZIANO

IL SEGRETARIO GENERALE

CERTIFICATO DI PUBBLICAZIONE

La presente deliberazione viene pubblicata per 15 giorni consecutivi all'Albo Pretorio online del Comune, sul sito istituzionale dell'Ente: **www.comune.modica.gov.it.**

Modica li - 7 GIU. 2022

Il Segretario Generale

Si attesta che copia della presente deliberazione è stata pubblicata all'Albo Pretorio online del Comune di Modica, senza opposizioni e reclami, dal - 9 GIU. 2022 al 2 4 GIU 2022, ed è repertoriata nel registro delle pubblicazioni al n. _____.

Modica li

Il Responsabile della pubblicazione

ATTESTAZIONE DI ESECUTIVITA'

☒ La presente deliberazione:

E' stata dichiarata immediatamente esecutiva ai sensi dell'art.12, comma 2, della L.R. 44/91.

☐ E' divenuta esecutiva il _____ ai sensi dell'art. 12, comma 1, della L.R. 44/91, trascorsi dieci giorni dall'inizio della pubblicazione.

Modica li - 7 GIU. 2022

Il Segretario Generale

Per copia conforme all'originale ad uso amministrativo.

Modica li

Il Segretario Generale