COMUNE DI MALFA

CITTA' METROPOLITANA DI MESSINA

DELIBERAZIONE DELLA GIUNTA COMUNALE

☐ **ORIGINALE** ☒ **COPIA** **N. 23** **Data 28.02.23**

OGGETTO: Approvazione "valutazione d'impatto sulla protezione dei dati personali (art. 35, GDPR 2016/679), impianto di videosorveglianza per la sicurezza urbana del Comune di Malfa.

L'anno duemilaventitre, il giorno ventotto, del mese di Febbraio, alle ore 12:46 e ss., nella residenza comunale, in apposita sala, regolarmente convocata, si è riunita la Giunta comunale nelle persone dei Signori:

N.	Cognome e Nome	Carica	Presenti	Assenti
1	RAMETTA CLARA	Sindaco	P	
2	SIRACUSANO GIUSEPPE	Vice Sindaco	P	
3	CINCOTTA LORENZO	Assessore	P	
4	ZAMPOGNA GIUSEPPE	Assessore		A
5	D'AMICO LORENZO MARIA	Assessore	P	

Fra gli assenti sono giustificati i Signori: .....

Presiede il Sindaco dott.ssa Clara Rametta, ai sensi dell'art 31dello Statuto comunale.

Partecipa alla seduta il dott.ssa Irene Maria Buglisi, Segretario Comunale, anche con funzioni di verbalizzante.

Il Presidente, accertato il numero legale, dichiara aperta la seduta per la trattazione dell'oggetto sopra indicato, premettendo che sulla proposta della presente deliberazione da parte:

☒ del Responsabile del servizio interessato, in ordine alla regolarità tecnica;

☒ del Responsabile di ragioneria, in ordine alla regolarità contabile,

recante i pareri previsti dall'art. 1 della L.R. n. 48/1991, così come modificato dall'art. 12 della L.R. n. 30/2000 e dall'art. 49 del Testo Unico degli Enti Locali (T.U.E.L.).

IL PRESIDENTE

Constatato che il numero dei presenti è legale, dichiara aperta la seduta ed invita i presenti a deliberare la proposta in oggetto.

LA GIUNTA COMUNALE

Vista l'unita proposta di deliberazione, meglio descritta in oggetto, corredata dai pareri di cui all'art. 1 della L.R. n. 48/1991, così come modificato dall'art. 12 della L.R. n. 30/2000 e dall'art. 49 del Testo Unico degli Enti Locali (T.U.E.L.).

Visto lo Statuto Comunale;

Visto l'O.A.EE.LL.;

Ritenuta la stessa meritevole di approvazione;

Con voti unanimi, legalmente espressi

DELIBERA

Di approvare la proposta di deliberazione sopra riportata relativa all'argomento di cui in oggetto corredata dai pareri su di essa apposti, ai sensi dall'art. 1 della L.R. n. 48/1991, così come modificato dall'art. 12 della L.R. n. 30/2000 e dall'art. 49 del Testo Unico degli Enti Locali (T.U.E.L.).

La presente deliberazione, con separata votazione con esito favorevole unanime, viene dichiarata immediatamente esecutiva.

Alle ore 13:05 esce il Sindaco Clara Rametta.

COMUNE DI MALFA
CITTA' METROPOLITANA DI MESSINA

PROPOSTA DI DELIBERAZIONE DI GIUNTA COMUNALE

OGGETTO: Approvazione *"Valutazione d'impatto sulla protezione dei dati personali (Art. 35, GDPR 2016/679), impianto di videosorveglianza per la sicurezza urbana del Comune di Malfa"*.

IL SINDACO

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 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, il quale si occupa, prevalentemente, di informare e fornire consulenza sulla corretta applicazione della normativa, curando con particolare attenzione la formazione del personale;
- il Titolare del Trattamento, così come definito dall'art. 4, comma 7 del GDPR, rappresentato dal Sindaco *pro-tempore*, ha designato e nominato quale DPO del Comune di Malfa, il Segretario Comunale, dott.ssa Irene Maria Buglisi;

DATO ATTO CHE:

- con Deliberazione di C.C. n. 14 del 25/05/2018, il Comune di Malfa ha provveduto all'approvazione del *"Regolamento comunale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali"*;

- il Comune di Malfa ha inteso rafforzare le azioni di prevenzione e di contrasto alle forme di illegalità presenti nel territorio dotandosi di un sistema di videosorveglianza per la sicurezza urbana;
- con delibera di G.M. n. 149 del 24/11/2021 il Comune di Malfa ha approvato lo schema del "*Patto per l'attuazione della Sicurezza Urbana*", successivamente oggetto di stipulazione dal Sindaco *pro tempore* e la Prefettura UTG di Messina;
- il Consiglio Comunale con deliberazione n. 53 del 29/11/2022 ha approvato il "*Regolamento comunale per la disciplina e l'utilizzo del sistema di videosorveglianza per la sicurezza urbana*";
- con determina n. 6 del 14/02/2023 il Sindaco *pro tempore* ha nominato quale Responsabile incaricato del trattamento dei dati personale del sistema di videosorveglianza, l'Agente di Polizia Municipale, Dott.ssa Calogera Contino;

CONSIDERATO CHE:

- il sistema di videosorveglianza surriferito acquisisce dati personali e, potenzialmente, anche dati sensibili riguardanti la vita dei cittadini e che, pertanto, tali dati devono trovare opportuna tutela;
- è opportuno svolgere approfondite valutazioni ed analisi, volte ad assicurare che il sistema *de quo* in uso assicuri il rispetto dei diritti dei cittadini ripresi;
- quando il trattamento dei dati è in grado di comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o perché vengono trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il GDPR, qualora ne riconosca la sussistenza dei presupposti, obbliga il titolare del trattamento, che può essere coadiuvato dal DPO, ad 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 ovvero quando "*può comportare un rischio elevato per i diritti e le libertà delle persone fisiche*";
- a D.P.I.A. 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;
- 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 al titolare, di consultare l'Autorità di controllo nel caso in cui le misure organizzative, da loro stesso 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'analisi di rischi derivanti da trattamenti posti in essere;

DATO ATTO CHE:

- tale misura deve essere sottoposta a un continuo riesame, ripetendo la valutazione a intervalli regolari;
- la responsabilità del D.P.I.A. spetta al Titolare;

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 aprile 2017, come modificate 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 tipologie i 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 il 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"*, *"dato avente carattere estremamente personale"*, *"uso di tecnologie evolute"*;

RISCONTRATO CHE, in base alla predetta disciplina, i trattamenti di dati personali effettuati tramite i sistemi di videosorveglianza necessitano della valutazione d'impatto, poichè rientrano nel caso previsto all'art. 35, GDPR, c.3, lett c)*"la sorveglianza sistematica su larga scala di una zona accessibile al pubblico"*;

VISTA la Valutazione d'impatto (P.I.A. – *Privacy Impact Assessment*) sul sistema di videosorveglianza del Settore Amministrativo - Ufficio di Polizia Locale, relativa al trattamento operato dei dati personali acquisiti mediante l'utilizzo del sistema di videosorveglianza attivato nel territorio del Comune di Malfa, ai sensi del Reg. UE 2016/679, della Direttiva UE 2016/680, in osservanza alle disposizioni contenute nel *"decalogo"* del 8 aprile 2010 del Garante della Privacy e del Codice Nazionale sulla Privacy del D.Lgs 196/2003, come modificato dl D.Lgs 10 agosto 2018, n. 10;

DATO ATTO CHE:

- la valutazione di impatto di tale sistema di videosorveglianza pone particolare attenzione ai diritti, 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 prevenire e reprimere la commissione di atti delittuosi, o comunque illeciti, idonei a ledere la sicurezza pubblica, il decoro urbano e la quiete pubblica;

DATO ATTO ALTRESI' 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 della Protezione dei dati personali** che per il Comune di Malfa è il Segretario Comunale, Dott.ssa Irene Maria Buglisi;

- **Responsabile interno incaricato della protezione dei dati personali per il sistema di videosorveglianza**, che per il Comune di Malfa è l'Agente di Polizia Municipale, Dott.ssa Calogera Contino, nominata con determinazione n. 6 del 14/02/2023;

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) -Sistema di videosorveglianza per la sicurezza urbana del Comune di Malfa, oggetto di validazione da parte del predetto DPO*";
CONSIDERATA la valutazione di impatto coerente con le misure idonee definite dal GDPR;

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 preservare la riservatezza, è stato rilevato in tutti i casi una probabilità di rischio "limitata";

RITENUTO NECESSARIO, per quanto sopra, di provvedere all'approvazione del documento di Valutazione – D.P.I.A., relativa ai rischi di violazione del predetto sistema di videosorveglianza per la sicurezza urbana;

VISTI:
- Il decreto legislativo 18 agosto 2000, n. 267 "*Testo Unico delle leggi sull'ordinamento degli Enti Locali*";
- L'art. 1, comma 439, della legge 27 dicembre 2006, n. 296 che conferisce al Ministero dell'interno e, per sua delega, ai Prefetti la facoltà di promuovere forme di collaborazione con gli Enti Locali per la realizzazione degli obiettivi del Patto e di programmi straordinari di incremento dei servizi di polizia e per la sicurezza dei cittadini;
- Il decreto legge del 20 febbraio 2017, n. 14 recante "*Disposizioni urgenti in materia di sicurezza delle città*" convertito con modificazioni dalla legge 18 arile 2017, n. 48;
- L'art. 5 del citato testo che regolamenta i "*patti per l'attuazione della sicurezza urbana*", sottoscritti tra il Prefetto ed il Sindaco "*in relazione alla specificità dei contesti*" e indica espressamente gli "obiettivi" (comma 2, lett. a) di prevenzione e contrasto dei fenomeni di criminalità diffusa e predatoria, attraverso servizi e interventi di prossimità, nonché attraverso l'installazione di sistemi di videosorveglianza;
- La circolare del Ministero dell'Interno 558/SICPART/421.2/70/224632 del 2 marzo 2012 recante "*Sistemi di videosorveglianza in ambito comunale. Direttiva*", e gli atti ivi richiamati;
- il Provvedimento del Garante della Privacy dell'8 aprile 2010, in materia di trattamento di dati personali effettuato tramite sistemi di videosorveglianza;
- il decreto legislativo 30 giugno 2003, n.196 "*Codice in materia di protezione dei dati personali*" come modificato dal decreto legislativo 10 agosto 2018, n.101 e dalla legge 27 dicembre 2019, n.160;
- il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati - RGPD);
- il decreto del Presidente della Repubblica 15 gennaio 2018, n.15 "*Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali*

relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia";

- il decreto legislativo 18 maggio 2018, n.51 recante "*Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*";

VISTO il Regolamento comunale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, approvato con Deliberazione di C.C. n. 14 del 25/05/2018;

ACQUISITO il parere favorevole in ordine alla regolarità tecnica del Responsabile del Settore Amministrativo, ai sensi dell'art. 1, comma 1, lettera i), della legge regionale n.48/91, con le modificazioni recate dall'art. 12 della L.R. n. 30/2000, nonché dall'art. 49 del Testo Unico degli Enti Locali (T.U.E.L.);

PROPONE

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

1) Di approvare il documento di Valutazione – D.P.I.A., avente ad oggetto "*Valutazione d'impatto sulla protezione dei dati (Art. 35 GDPR 2016/679) del sistema di videosorveglianza per la sicurezza urbana del Comune di Malfa*";
2) Di disporre che il presente provvedimento sia comunicato al DPO del Comune di Malfa e al Responsabile incaricato per la protezione dei dati personali per il sistema di videosorveglianza dell'Ente;
3) Di disporre la pubblicazione del presente provvedimento sul sito web dell'Ente, Sezione "*Informatica e Trattamento dei Dati*" e Sezione "*Ordine pubblico e sicurezza pubblica*";
4) Di dichiarare, con separata e unanime votazione, la presente deliberazione immediatamente esecutiva agli effetti di legge.

COMUNE DI MALFA - PROV. ME -

PROPONENTE
Il Sindaco
Dott.ssa Clara Rametta

Valutazione d'impatto sulla protezione dei dati personali (Art. 35, GDPR 2016/679), Impianto di videosorveglianza per la sicurezza urbana del Comune di Malfa.

INFORMAZIONI SULLA PIA

Nome della PIA
Valutazione d'impatto sul sistema di videosorveglianza del Comune di Malfa
Nome Autore
Sindaco *pro-tempore*
Nome Valutatore
Responsabile del Servizio di Protezione dei dati personali per il sistema di videosorveglianza
Nome Validatore
DPO – Dott.ssa Irene Maria Buglisi

Data di creazione: 28/02/2023

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il Comune di Malfa è dotato di un sistema di videosorveglianza, basato su telecamere digitali collegate ad un apparato centralizzato di registrazione. I *files* contenenti video e immagini rientrano nella categoria dei dati personali, in particolare qualora sia possibile l'identificazione dell'interessato. L'impatto è valutato con particolare attenzione ai diritti e alle libertà degli interessati e ha come obiettivo verificare e garantire la protezione dei dati personali di tutti coloro i quali entrano in contatto o in relazione con l'attività di videosorveglianza. In attuazione del principio di necessità, il sistema di videosorveglianza e l'impianto informatico è realizzato riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità sono raggiungibili tramite anonimato o riducendo allo stretto necessario l'utilizzo dei dati personali.
L'uso dell'impianto è strumento per l'attuazione di un sistema integrato di politiche per la sicurezza urbana. Finalità del trattamento è la prevenzione e repressione di atti delittuosi, attività illecite o di episodi di microcriminalità nonchè la vigilanza sul territorio per prevenire episodi di degrado, tutelare il patrimonio pubblico e privato e, in generale, rappresentare uno strumento di deterrenza al verificarsi di atti illeciti. L'utilizzo degli impianti di videosorveglianza da parte della polizia locale e del locale Comando dei Carabinieri costituisce, inoltre, strumento di prevenzione e di razionalizzazione dell'azione di Polizia locale e Carabinieri sul territorio comunale. Tali finalità sono in conformità con quanto previsto dalla normativa in materia e dal vigente Regolamento

comunale per la disciplina e l'utilizzo del sistema di videosorveglianza per la sicurezza urbana, approvato dal Consiglio Comunale del Comune di Malfa con deliberazione n. 53 del 28/11/2022.

Quali sono le responsabilità connesse al trattamento?

Le responsabilità del trattamento sono connesse al ruolo ricoperto. Il Titolare del Trattamento dei dati personali è il Comune di Malfa, in persona del legale rappresentante *pro tempore*. Il *Data Protection Officer* è il Segretario Comunale, Dott.ssa Irene Maria Buglisi. Il Responsabile del Trattamento dei dati personali per il sistema di videosorveglianza è la Dott.ssa Calogera Contino, giusta determina sindacale di nomina n. 6 del 14/02/2023.

Ci sono standard applicabili al trattamento?

L'attività di videosorveglianza è disciplinato da specifico Regolamento comunale per la disciplina e l'utilizzo del sistema di videosorveglianza per la sicurezza urbana, approvato dal Consiglio Comunale del Comune di Malfa, con deliberazione n. 53 del 28/11/2022.

Valutazione : Accettabile

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Il sistema di videosorveglianza prevede la collocazione di punti di ripresa (telecamere speed dome e telecamere di tipo fisso a colori) collegati, mediante una rete wireless, alla centrale operativa nella quale saranno installate le apparecchiature (HW/SW) di controllo e di registrazione dei flussi video del sistema. 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 comunale. Vengono trattati i dati degli autoveicoli, targhe, persone fisiche che circolano nel campo di visione delle telecamere. Il Titolare del trattamento dei dati personali ha indicato di non effettuare riprese di dettaglio dei tratti somatici delle persone fisiche che non siano funzionali alle finalità istituzionali dell'impianto attivato.

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

I segnali video delle unità di riprese sono inviati presso l'Unità di ricezione, registrazione e visione ubicata presso gli uffici della Polizia Municipale. In questa sede le immagini potranno essere visualizzate su monitor, previa identificazione tramite password grafica, e registrate su supporto magnetico. La conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata. Il termine massimo di durata della conservazione dei dati è limitato a sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza. In ragione di esigenze investigative e su richiesta dell'Autorità Giudiziaria, il Titolare potrà disporre la conservazione delle immagini per un periodo di tempo superiore ai sette giorni, compatibilmente ai limiti strutturali del sistema, previa richiesta al Garante per la protezione dei dati personali. Il sistema è programmato in modo da operare, al momento prefissato, l'integrale cancellazione automatica delle informazioni allo scadere del termine

previsto da ogni supporto, anche tramite sovra-registrazione, con modalità tali da rendere non inutilizzabili i dati cancellati. In caso di cessazione del trattamento, i dati sono distrutti.

Quali sono le risorse di supporto ai dati?

Le telecamere consentono riprese video a colori in condizioni di sufficiente illuminazione naturale o artificiale o in bianco e nero in caso contrario. I segnali video sono inviati presso l'Unità di ricezione, registrazione e visione ubicata presso gli uffici della Polizia Municipale. Le immagini potranno essere visionate sul monitor, previa identificazione tramite password grafica da parte del Responsabile e registrate su supporto magnetico. Esiste un server di registrazione e storage, le cui chiavi sono in possesso del funzionario incaricato Responsabile. Esiste un registro delle attività di trattamento e degli accessi cartaceo, conservato nei locali dell'ufficio di Polizia Municipale, nel quale sono riportati data e ora dell'accesso, identificazione del terzo autorizzato, i dati per i quali è svolto l'accesso, gli estremi e la motivazione dell'autorizzazione all'accesso, la sottoscrizione dell'incaricato.

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento dei dati personali, acquisiti mediante il sistema di videosorveglianza gestito dall'Ente e trasmessi all'Unità di ricezione ubicata presso gli uffici comunali, si svolge nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza o all'identità personale.
Le finalità del trattamento sono esplicitate nel Regolamento comunale e sono specifiche, interessando la materia della sicurezza urbana e della prevenzione di ipotesi delittuose e di illeciti potenzialmente pregiudizievoli per la sicurezza, il decoro urbano, l'integrità del patrimonio.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica del trattamento è data dalla necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, ai sensi dell'art. 6, par. 1, lett. e), GDPR nonchè dalla finalità di perseguire un compito dato dall'autorità competente per la finalità di prevenzione, accertamento e perseguimento dei reati, salvaguardia della sicurezza urbana ai sensi dell'art. 5, D.Lgs. 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 necessari per le finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando, quando non indispensabile, immagini ingrandite, dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza. La localizzazione delle telecamere è stata stabilita in modo conseguente. Non sono effettuate riprese di dettagli somatici delle persone fisiche non funzionali alle finalità perseguite. Il Titolare ha adottato un sistema di oscuramento in relazione agli angoli di ripresa non concernenti aree comunali o, comunque, lesive della privacy.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

I dati sono esatti e aggiornati.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

I dati personali acquisiti tramite il sistema di videosorveglianza del Comune di Malfa sono conservati per un periodo di tempo non superiore a sette giorni. Decorso tale periodo, i dati sono cancellati automaticamente, mediante sovra-registrazione.

Valutazione : Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati sono sempre informati che stanno per accedere ad una zona videosorvegliata. A tal fine l'Ente utilizza il modello semplificato di informativa "minima" o di primo livello, indicante il Titolare del trattamento e la finalità perseguita, di cui al modello in materia di videosorveglianza dal Garante della Protezione dei dati personali dell'08/04/2010, aggiornato alle linee guida 3/2019 redatte dal Comitato europeo per la tutela dei dati personali, con indicazione, nel lato inferiore del cartello, del riferimento normativo "*Art. 13 del Regolamento europeo sulla protezione dei dati personali (GDPR 2016/679)*". L'informativa completa (o di II° Livello) sul trattamento dei dati personali è pubblicata sul Sito Istituzionale del Comune di Malfa e può essere acquisita presso gli Uffici di Polizia Municipale. La segnaletica permanente è affissa nelle strade e nelle piazze dove sono ubicate le telecamere, prima del raggio di azione delle stesse. La segnaletica ha un formato e 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.

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 per il trattamento dei dati.

Valutazione : Accettabile

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

In relazione al trattamento dei dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss. GDPR, su presentazione di apposita istanza, ha diritto:

- 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;
- 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;
- di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 GDPR, 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;
- 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, GDPR.

L'istanza per l'esercizio dei diritti dell'interessato è presentata al funzionario Responsabile del trattamento dei dati personali per il sistema di videosorveglianza. Per la compilazione dell'istanza è utilizzato un modello allegato al regolamento, da trasmettere *brevi manu* all'Ufficio Protocollo, a mezzo di lettera raccomanda A/R o di posta elettronica certificata, con destinatario il Titolare o il Responsabile incaricato. Nel caso di richiesta di accesso alle immagini, l'interessato provvede a indicare:

- luogo, data e fascia oraria della possibile ripresa;
- abbigliamento indossato al momento della possibile ripresa;
- eventuali accessori in uso al momento della possibile ripresa;
- eventuale presenza di accompagnatori al momento della possibile ripresa;
- eventuale attività svolta al momento della possibile ripresa;
- eventuali ulteriori elementi utili all'identificazione dell'interessato.

Il funzionario Responsabile del trattamento dei dati 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.

Qualora, ai sensi dell'art. 15, par. 3, GDPR, 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. 14, par. 4, GDPR.
I diritti di cui sopra 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.
Nell'esercizio dei diritti, l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti od organismi. L'interessato può altresì farsi assistere da persona di fiducia.
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.

Valutazione : Accettabile

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

Per i loro diritti di rettifica o cancellazione, compatibilmente con la funzione pubblica sottesa al sistema di videoregistrazione, gli interessati possono fare istanza al Responsabile del Trattamento dei dati personali per il sistema di videosorveglianza.

Valutazione : Accettabile

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

I diritti di limitazione o opposizione possono essere esercitati tramite istanza al Responsabile del Trattamento dei dati personali per il sistema di videosorveglianza.

Valutazione : Accettabile

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

Gli obblighi del Responsabile incaricato del trattamento dei dati personali del sistema di videosorveglianza sono definiti con chiarezza nella determina di nomina n. 06 del 14/02/2023.

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

Crittografia

Tutti i dati video concernenti la configurabilità, l'account e altre informazioni relative al funzionamento del sistema sono conservati in modali criptata

Valutazione : Accettabile

Tracciabilità

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

Valutazione : Accettabile

Controllo degli accessi logici

Il funzionario che intende accedere al video dalla scheda SD, deve prima inserire la password in formato crittografico in suo possesso. Anche per la mera visione del monitor è previsto l'inserimento di una password in formato grafico.

Valutazione : Accettabile

Minimizzazione dei dati

Vengono utilizzati esclusivamente i dati indispensabili per la realizzazione delle finalità dell'impianto

Valutazione : Accettabile

Vulnerabilità

Ogni telecamera è identificata con un numero ID univoco, registrato e integrato a livello di sviluppo. Una volta connessa la IP camera con il software, l'autorizzato può visualizzare in streaming in tempo reale le immagini. Esiste un canale criptato e certificato tra il client e il server.

Valutazione : Accettabile

Specifiche misure di sicurezza

Le funzionalità minime di gestione del sistema di videosorveglianza sono:
- rapida localizzazione di sequenze di immagini, attraverso funzioni di ricerca come, ad es., data, ora, numero dell'allarme, numero della telecamera o contrassegno dell'evento, con possibilità di integrazione e ricerca tramite il sistema di telecontrollo;
- visualizzazione delle immagini memorizzate come quarto d'immagine, immagine completa o quad;
- stampa delle immagini memorizzate su stampante a getto di inchiostro o laser;
- verifica sabotaggio telecamera;
- interfaccia con sistema di telecontrollo;
- visualizzazione dello storico relativo alle immagini registrate per vedere la ricostruzione dell'evento ed identificare i responsabili;
- memorizzazione permanente di immagini a colori, con uniformi risultati di alta qualità;
- definizione delle immagini fino a 704X576 pixels a 25 frames per secondo;
- alta velocità di memorizzazione a 100 immagini;
- desktop grafico interattivo, basato su menù;
- connessione LAN via Ethernet a sistemi remoti di gestione e controllo;
- gestione telecamere speed dome con richiamo funzioni di preset, autopan, percorsi e scansioni automatiche (ronda video);
- gestione e parametrizzazione da remoto delle telecamere fisse e mobili.
- salvataggio delle registrazioni video su diverse tipologie di supporti magnetici (CD-RW. DVD-R/+R/-RW/+RW);
- password multilivello con gestione gruppi utenti differenziati in base ad orario cliente di connessione o luogo di visualizzazione;
- gestione della funzione "privacy zone" nel pieno rispetto delle normative.

Valutazione: Accettabile

Lotta contro il malware

L'antimalware è regolarmente installato e aggiornato.

Valutazione : Accettabile

Sicurezza dei canali informatici

Il firewall è installato e aggiornato.

Valutazione : Accettabile

Gestione postazioni

Ad accedere alla visione e alle registrazioni delle immagini è il solo Responsabile, o altri soggetti formalmente incaricati con autorizzazione dello stesso Responsabile.

Valutazione : Accettabile

Sicurezza dell'hardware

Le chiavi del server sono in possesso, in doppia copia, del titolare e del responsabile.

Valutazione : Accettabile

Politica di tutela della privacy

Le politiche di tutela della privacy comprendono il regolamento adottato dall'ente e le disposizioni di cui al GDPR.

Valutazione : Accettabile

Gestione del personale

I dipendenti sono regolarmente invitati a partecipare a seminari formativi in materia di privacy. Sarà prevista una specifica formazione per il Responsabile del trattamento dei dati personali del sistema.

Valutazione : Accettabile

Anonimizzazione

I particolari tipi di dati personali, soprattutto quelli sensibili, sono trattati dagli autorizzati per le finalità consentati e, in ogni caso, mai oggetto si pubblicazione

Valutazione : Accettabile

Manutenzione

La manutenzione è gestita dalla ditta fornitrice del sistema, previa adozione di specifiche cautele e comnque sempre in presenza del funzionario Responsabile. I tecnici potranno accedere alle immagini solo se strettamente indispensabile. In casi del tutto eccezionali, potrà avere accesso ai locali un tecnico informatico incarica dal Comune o altro soggetto in grado di garantire la funzionalità del sistema, previa espressa individuazione da parte del soggetto incaricato.

Valutazione : Accettabile

Gestione dei rischi

Gli apparati di ripresa digitali connessi a rete informatiche sono protessi contro rischi di accesso abusivo. La trasmissione tramite rete pubblica di comunicazioni di immagini riprese dal sistema di videosorveglianza è effettuata previa applicazione tecnica crittografica che ne garantisca la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa

dotati di connessioni wireless (tecnologie WI-FI, WI Max, GPRS). I sistemi prevedono la tracciatura del log di accesso.
L'architettura di rete consente:
– espansione graduale della rete (scalabilità);
– efficiente utilizzo del mezzo trasmissivo;
– sicurezza nella gestione dei pacchetti IP per il trasporto dei dati;
– utilizzo di frequenze tali da evitare interferenze da parte di dispositivi estranei al sistema di videosorveglianza;
– trasmissione multicast per un utilizzo ottimale della rete;
– management centralizzato.

Valutazione : Accettabile

Integrare la protezione della privacy nei progetti

La gestione del sistema di videosorveglianza in materia di trattamento dei dati personali rientra a pieno titolo tra le specifiche responsabilità attribuite al personale ai sensi dell'art. 84, CCNL 2019/2021, Funzioni Locali.

Valutazione : Accettabile

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Gli uffici rispettano la normativa in materia di salute e protezione sui luoghi di lavoro di cui al D.Lgs 81/08.

Valutazione : Accettabile

Controllo degli accessi fisici

Il sistema prevede la tracciatura dei log di accesso e delle operazioni compiute, con indicazione del giorno e dell'ora di accesso.

Valutazione : Accettabile

Gestione dei terzi che accedono ai dati

Gli interessati possono prendere visione e estrapolare le immagini che li riguardano, con le modalità procedurali individuate dal regolamento, con la schermatura del video o altro accorgimento tecnico che consenta di oscurare i riferimenti a dati identificativi delle altre persone fisiche eventualmente presenti.

Valutazione : Accettabile

Protezione contro fonti di rischio non umane

Installazione e aggiornamento maleware, firewall, antivirus.

Valutazione : Accettabile

Rischi

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 sensibili

Quali sono le fonti di rischio?

fonti di rischio esterne e interne anche non umane

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Tracciabilità, Controllo degli accessi logici, Vulnerabilità, Lotta contro il malware, Sicurezza dei canali informatici, Gestione postazioni, Politica di tutela della privacy, Gestione del personale, Anonimizzazione, Gestione dei rischi, Gestione dei terzi che accedono ai dati, Controllo degli accessi fisici, Protezione contro fonti di rischio non umane

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

Rischi

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, abuso d'ufficio da parte del funzionario addetto, accesso ai dati da parte di soggetti terzi 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, Tracciabilità, Controllo degli accessi logici, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Sicurezza dei canali informatici, Gestione postazioni, Sicurezza dell'hardware, Politica di tutela della privacy, Gestione del personale, Anonimizzazione, Manutenzione, Gestione dei rischi, Integrare la protezione della privacy nei progetti, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Controllo degli accessi fisici, Gestione dei terzi che accedono ai dati, Protezione contro fonti di rischio non umane

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

Limitata, In base alle misure programmate il rischio è limitato

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

Limitata, In base alle misure programmate il rischio è limitato

Valutazione : Accettabile

Rischi

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, Perdita di dati, Uso improprio di dati, abuso d'ufficio da parte del funzionario addetto, accesso ai dati da parte di soggetti terzi non competenti e non autorizzati, diffusione di dati sensibili

Quali sono le fonti di rischio?

fonti di rischio esterne e interne anche non umane

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

Crittografia, Controllo degli accessi logici, Tracciabilità, Vulnerabilità, Minimizzazione dei dati, Lotta contro il malware, Sicurezza dei canali informatici, Gestione postazioni, Sicurezza dell'hardware, Politica di tutela della privacy, Gestione del personale, Anonimizzazione, Manutenzione, Gestione dei rischi, Integrare la protezione della privacy nei progetti, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Controllo degli accessi fisici, Gestione dei terzi che accedono ai dati, Protezione contro fonti di rischio non umane

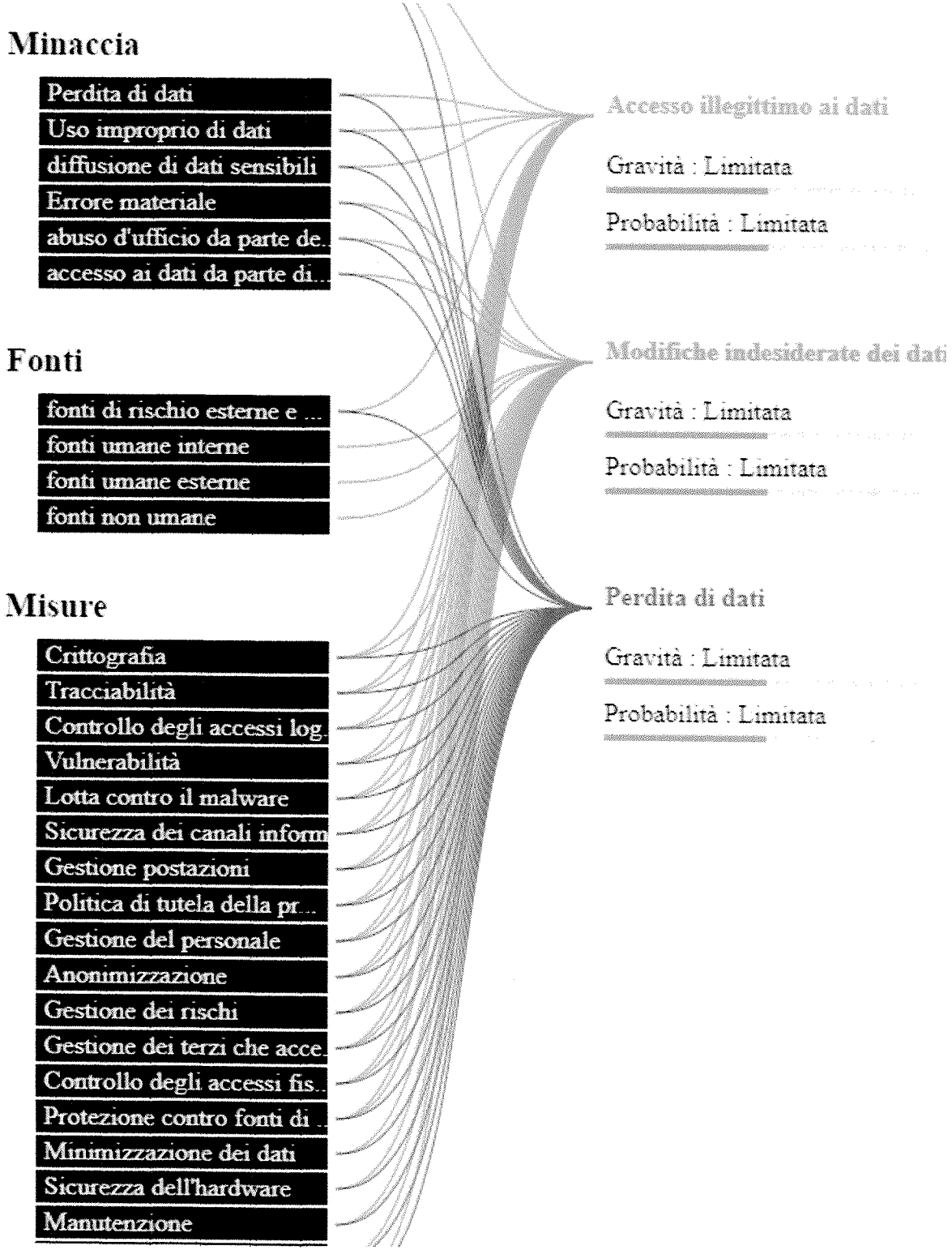
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata, In base alle misure programmate il rischio è limitato

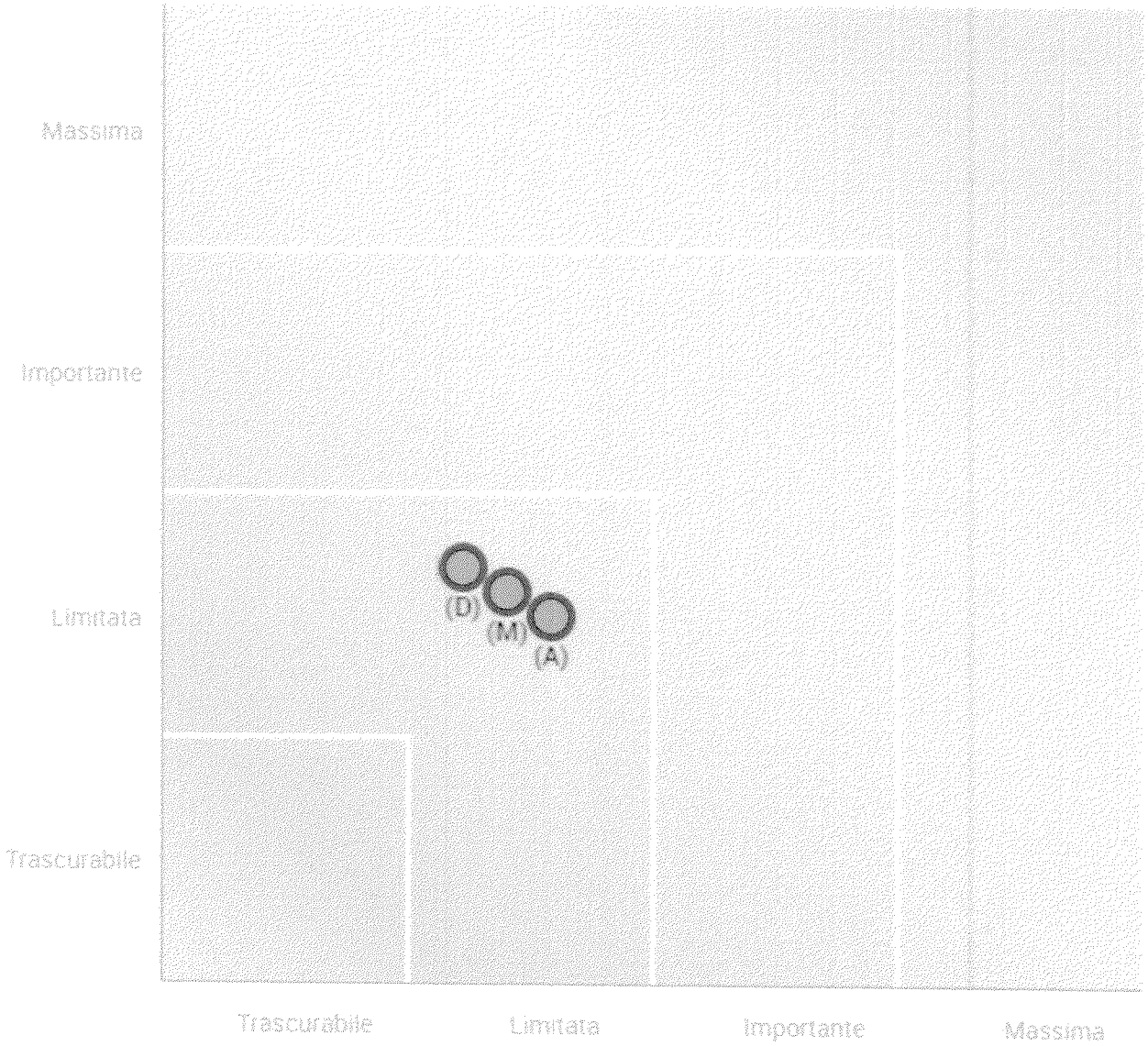
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, In base alle misure programmate il rischio è limitato

Valutazione : Accettabile


Minaccia
Perdita di dati
Uso improprio di dati
diffusione di dati sensibili
Errore materiale
abuso d'ufficio da parte de..
accesso ai dati da parte di...
Fonti
fonti di rischio esterne e ...
fonti umane interne
fonti umane esterne
fonti non umane
Misure
Crittografia
Tracciabilità
Controllo degli accessi log..
Vulnerabilità
Lotta contro il malware
Sicurezza dei canali inform
Gestione postazioni
Politica di tutela della pr...
Gestione del personale
Anonimizzazione
Gestione dei rischi
Gestione dei terzi che acce..
Controllo degli accessi fis..
Protezione contro fonti di ..
Minimizzazione dei dati
Sicurezza dell'hardware
Manutenzione
Accesso illegittimo ai dati
Gravità : Limitata
Probabilità : Limitata
Modifiche indesiderate dei dati
Gravità : Limitata
Probabilità : Limitata
Perdita di dati
Gravità : Limitata
Probabilità : Limitata

Gravità del rischio



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

Probabilità del rischio

Principi fondamentali

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

Misure esistenti o pianificate

- Crittografia
- Tracciabilità
- Controllo degli accessi logici
- Minimizzazione dei dati
- Vulnerabilità
- Lotta contro il malware
- Sicurezza dei canali informatici
- Gestione postazioni
- Sicurezza dell'hardware
- Politica di tutela della privacy
- Gestione del personale
- Anonimizzazione
- Manutenzione
- Gestione dei rischi
- Integrare la protezione della privacy nei progetti
- Gestire gli incidenti di sicurezza e le violazioni dei dati personali
- Controllo degli accessi fisici
- Gestione dei terzi che accedono ai dati
- Protezione contro fonti di rischio non umane

Rischi

- Accesso illegittimo ai dati
- Modifiche indesiderate dei dati
- Perdita di dati

Misure Migliorabili

COMUNE DI MALFA

PROVINCIA DI MESSINA

PARERI

ai sensi dell'art.1 della L.R. n. 48/1991 e ss.mm.ii, con le modificazioni recate dall'art. 12 della L.R. n. 30/2000 e ai sensi dell'art.49 del TUEL.

OGGETTO: " Approvazione "Valutazione d'impatto sulla protezione dei dati personali (Art.35, GDR 2016/679), impianto di videosorveglianza per la sicurezza urbana del Comune di Malfa".

SETTORE AMMINISTRATIVO

Per quanto concerne la regolarità tecnica si esprime parere Favorevole
Malfa, lì 28.02.2023;

COMUNE DI MALFA - Primo Settore -

Il Responsabile del Settore

SETTORE ECONOMICO-FINANZIARIO

Per quanto concerne la regolarità contabile si esprime parere Favorevole
Malfa, lì

Il Responsabile del Settore

OPPURE: Parere non dovuto in quanto il presente atto non comporta riflessi diretti o indiretti sulla situazione economico-finanziaria o sul patrimonio dell'ente.
Malfa, lì 28/02/2023;

Il Responsabile del Settore

ATTESTAZIONE AI SENSI DELL'ART. 13 DELLA L.R. N. 94/1991

Accertato l'equilibrio finanziario di gestione in funzione delle entrate e delle uscite di bilancio,

SI ATTESTA

la copertura finanziaria della spesa di cui all'allegata proposta al cap.lo
Malfa, lì

Il Responsabile del Settore

Letto, approvato e sottoscritto

▸ Il Sindaco

f.to Dott.ssa Clara Rametta

L'Assessore Anziano

f.to Lorenzo Cincotta

COMUNE DI MALFA · PROV. ME ·

▸ Il Segretario Comunale

f.to Dott.ssa Irene Maria Buglisi

PUBBLICAZIONE

In data odierna, la presente deliberazione viene pubblicata all'Albo Pretorio informatico comunale per 15 giorni consecutivi, come prescritto dall'art.11, comma 1, della L.R. n. 44/1991.

Data _____

▸L'addetto alla pubblicazione

_____

La presente deliberazione

☒ è stata dichiarata immediatamente eseguibile ai sensi dell'art. 12, comma 2 della L.R. n. 44/1991;

☐ è divenuta esecutiva il _____, decorsi dieci giorni dalla pubblicazione, come prescritto dall' art.12, comma 1 della L.R. n. 44/1991.

COMUNE DI MALFA · PROV. ME ·

▸ Il Segretario Comunale
f.to Dott.ssa Irene Maria Buglisi