Data Protection Impact Assessment (DPIA)
Comune di Bagheria

Sorveglianza sistematica su larga scala di una zona accessibile al pubblico

TRATTAMENTO DATI: Sistema Videosorveglianza Comunale

Sommario

1. Introduzione

Con l'entrata in vigore del nuovo Regolamento Europeo 2016/679 "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" (di seguito, "GDPR" o il "Regolamento"), applicabile a partire dal 25 maggio 2018, incombe sul titolare del trattamento di dati personali la responsabilità di adottare tutte le misure necessarie al fine di garantire la sicurezza e la protezione dei dati.
L'art. 35 del GDPR, impone altresì al titolare del trattamento lo svolgimento di una valutazione preventiva dell'impatto dei trattamenti previsti sulla protezione dei dati, anche in considerazione di possibili rischi per i diritti e le libertà delle persone fisiche (di seguito, "DPIA").

2. Obiettivo del documento

Questa DPIA è stata redatta nel rispetto e secondo quanto previsto dalle indicazioni delle Autorità per la Protezione dei Dati Europee (di seguito "DPA"), fornite nelle "Linee guida sulla Valutazione di Impatto sulla Protezione dei dati e sulla determinazione del concetto di rischio elevato ai fini del Regolamento (UE) 2016/679" del 4 aprile 2017 emanate dal Working Party ex art. 29 direttiva 95/46/CE (di seguito "WP29"), e nel rispetto e in esecuzione di quanto previsto dal Regolamento (UE) 2016/679 (di seguito il "GDPR") e in particolare in ottemperanza di quanto incoraggiato dai considerando 78, 90, 91 e previsto dagli articoli 25 e 35.

3. Definizioni

Di seguito è illustrata la definizione dei principali termini utilizzati nell'ambito della DPIA:

- **Probabilità:** valutazione della frequenza di accadimento di una minaccia, in funzione delle vulnerabilità in essere e di eventuali contromisure implementate;
- **Impatto:** indicazione della gravità di un incidente che comprometta la riservatezza, l'integrità e la disponibilità di processi, dati, informazioni incluse nel perimetro di applicazione della normativa privacy;
- **Minaccia:** evento potenziale, accidentale o deliberato, che, nel caso accadesse, produrrebbe un danno per l'interessato;
- **Vulnerabilità:** debolezza intrinseca del sistema informativo o del sistema informatico che, qualora si realizzasse una minaccia che la sfrutti, produrrebbe un danno all'interessato;
- **Rischio Privacy:** combinazione di impatto per l'interessato e della probabilità di accadimento di una minaccia che possa compromettere la riservatezza, l'integrità o la disponibilità di un dato personale ad esso riferito;
- **Contromisure:** soluzioni organizzative, procedurali o tecnologiche che possono essere implementate al fine di mitigare il Rischio Privacy associato ad ogni sistema o archivio e quindi diminuire il Rischio;
- **Soglie di accettazione del rischio:** definizione del livello massimo di rischio accettato superato

il quale si rende necessaria l'implementazione delle contromisure.

4. Contesto normativo

L'art. 35, comma 7, GDPR, prevede che la DPIA contenga almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati;

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

5. Descrizione, caratteristiche e finalità dei trattamenti

Come considerazione preliminare di contestualizzazione, il Comune di Bagheria intende procedere all'installazione di un sistema di videosorveglianza allo scopo di:

a) attività di polizia giudiziaria svolta ai sensi del C.P.P. per la prevenzione e repressione dei reati;
b) prevenire e ricostruire eventuali atti di vandalismo o danneggiamento agli immobili del patrimonio comunale, di disturbo alla quiete pubblica e sicurezza interna del Comando P.M. ed eventuali altri uffici comunali;
c) la protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, l'ordine e sicurezza pubblica, la prevenzione, la razionalizzazione e miglioramento dei servizi al pubblico volto anche ad accrescere la sicurezza degli utenti;
d) l'acquisizione di fonti di prova per finalità di polizia giudiziaria;

Le finalità del Trattamento, così come meglio descritti sopra, è rinvenibile nella necessità del Comune di Bagheria di garantire l'incolumità pubblica e la sicurezza urbana, il decoro urbano, nei limiti dei poteri individuati dalla normativa di settore *(cfr. art. 54 d.lgs. 18 agosto 2000, n. 267; d.m. 5 agosto 2008; art. 6, comma 7, d.l. 23 febbraio 2009, n. 11, convertito, con modificazioni, dalla legge 23 aprile 2009, n. 38)* anche relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia di cui al DPR del 15 gennaio 2018, n. 15.

Inoltre, l'utilizzo di tale sistema di videosorveglianza consentirà una sorta di prevenzione generale nei confronti dei consociati operando una dissuasione nel tenere tali condotte illecite nei confronti della comunità e del decoro urbano. E nell'ipotesi di violazione emerge la possibilità di irrogare la relativa sanzione con certezza al soggetto responsabile della trasgressione la quale può assumere una rilevanza amministrativa, risarcitoria e financo penale.

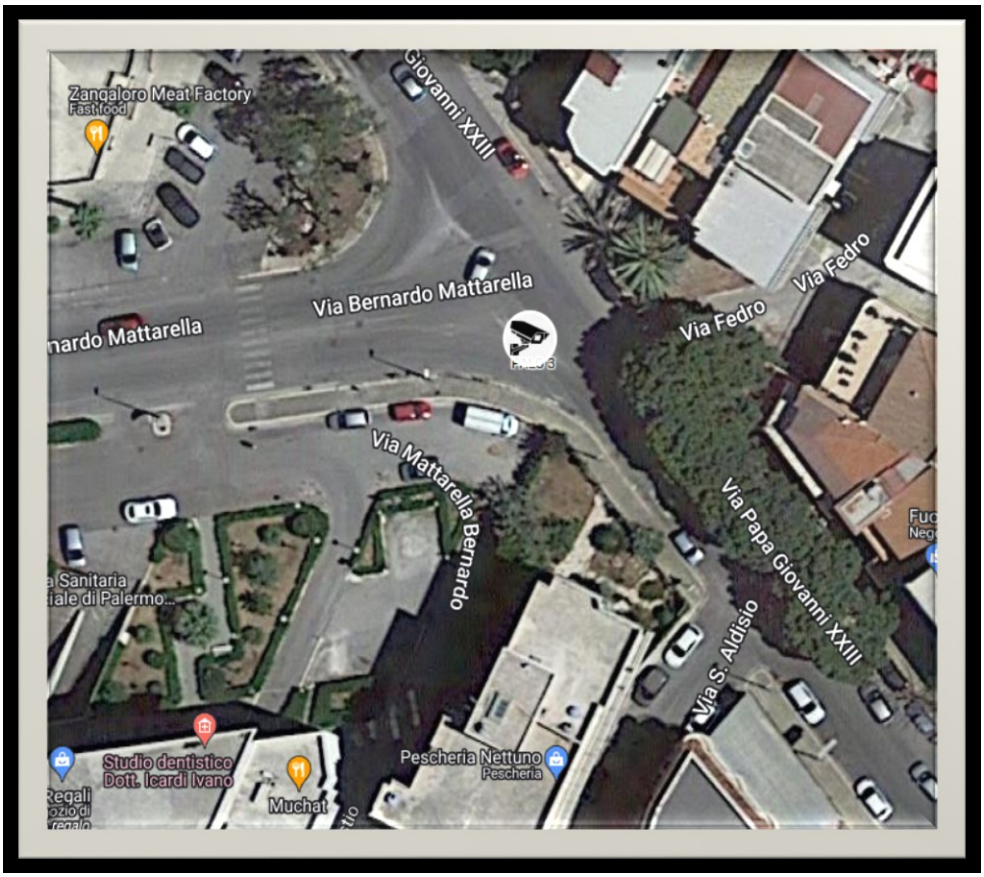
6. Tipologie di dati trattati

In tale sezione saranno analizzati i sistemi di videosorveglianza di Bagheria installati in 13 punti distribuiti strategicamente su tutto il territorio Comunale e di seguito riportati:

- Svincolo autostradale che riprende parte della circonvallazione direzione Via De Spuches e direzione Via San Giovanni Bosco-Incorvino e Via Filippo Buttitta;
- SS. 113 - Villa cattolica;
- Via B. Mattarella - Via Papa Giovanni XXIII;
- Via Dante – Viale Ing. Giuseppe Bagnera;
- Corso Umberto I - Piazza matrice;
- Corso Umberto I - Via Diego d'amico;
- Corso Butera angolo Via Liberta';
- SS 113 incrocio torremuzza (a confine con il comune di Santa Flavia – ambo le direzioni);
- Via consolare – Via Papa Giovanni XXIII
- Corso Italia (a confine con Comune di Ficarazzi);
- Incrocio SP87 (vallone del fonditore – limite territorio Comune di Ficarazzi);
- Via Filippo Buttitta – Via Ignazio lanza di Trabia;
- Corso Baldassare Scaduto

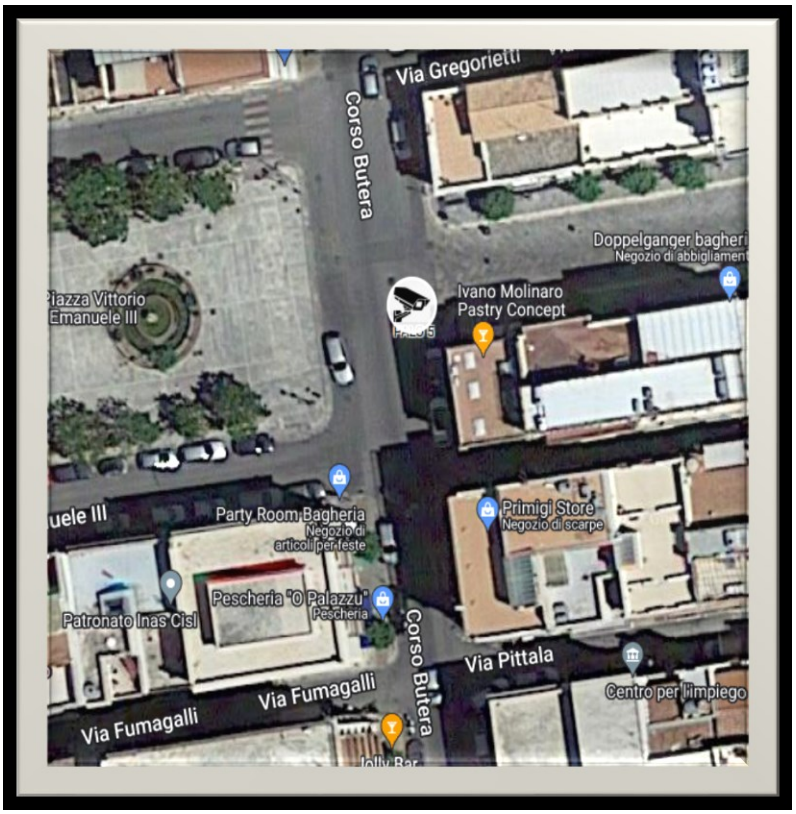
Gli stessi sono rappresentati graficamente di seguito:


Conad - Via Passo del Carretto 93
Take Away Pollo Alla Brace Con Patatine...
Pizzeria La Spiga D'oro Panificio
Bata
Negozio di scarpe
Via Dottor Filippo Buttitta
Bar Diva
Via Leonardo Sciascia


Zangaloro Meat Factory
Fast food
Giovanni XXIII
Via Bernardo Mattarella
Via Fedro
Via Mattarella Bernardo
Via Papa Giovanni XXIII
Via S. Aldisio
Studio dentistico Dott. Icardi Ivano
Muchat
Pescheria Nettuno
Pescheria


Ristorante Pizzeria
"I VIVANDIERI"
S.da Statale 113
SS113
Via Rammacca
S.da Sta
Ristorante Pizzeria
Tarabaralla
Il Giardino dei Limoni
Chiuso temporaneamente
Sanfilippo Simone
Pescheria


Happy Yogurt
Frozen yogurt
Via Dante Alighieri
Via Dante Alighieri
Via Dante Alighie
Via Città di Palermo
Dott.ssa Margherita Lupi
VintiReci
Ellevi Group
Di Lo Iacono Vincenzo...

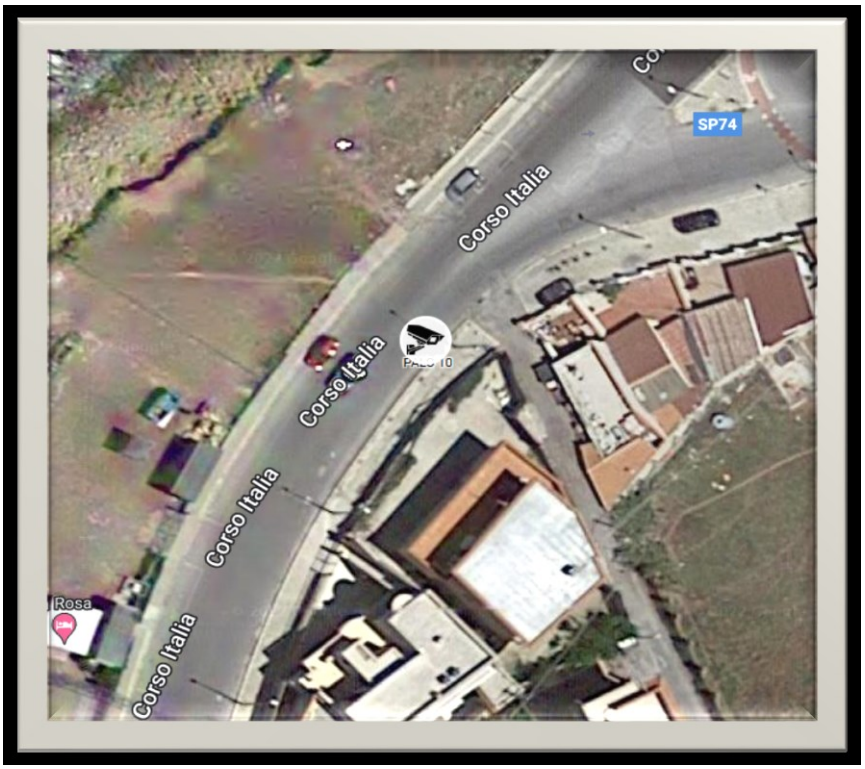

Via Gregorietti
Corso Butera
Doppelganger bagheri
Negozio di abbigliament
Ivano Molinaro
Pastry Concept
Party Room Bagheria
Negozio di articoli per feste
Primigi Store
Negozio di scarpe
Pescheria "O Palazzu"
Pescheria
Patronato Inas Cisl
Via Pittala
Centro per l'impiego
Via Fumagalli
Via Fumagalli
Corso Butera

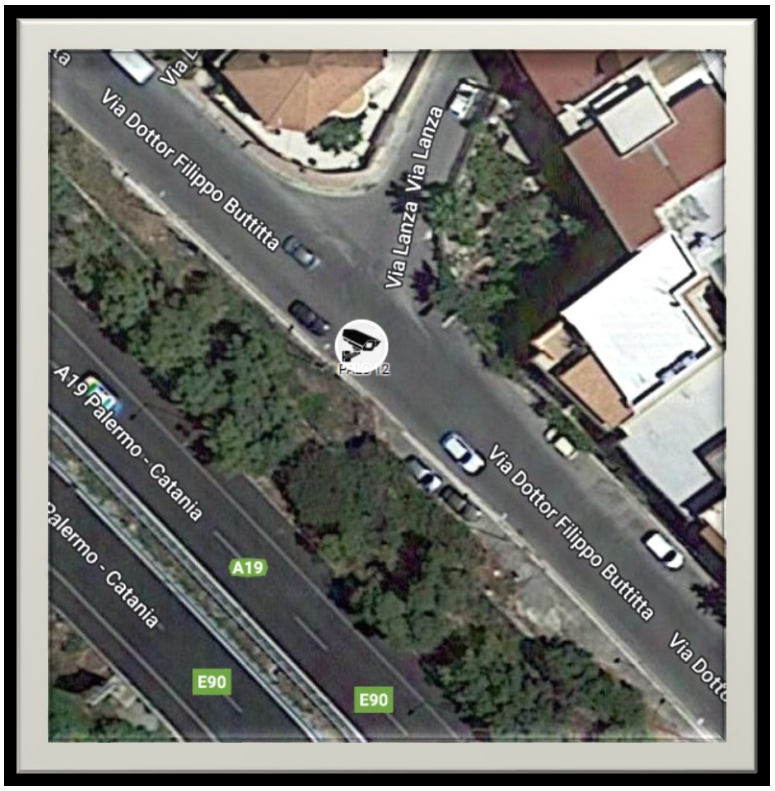

S.da Statale 113
SS113

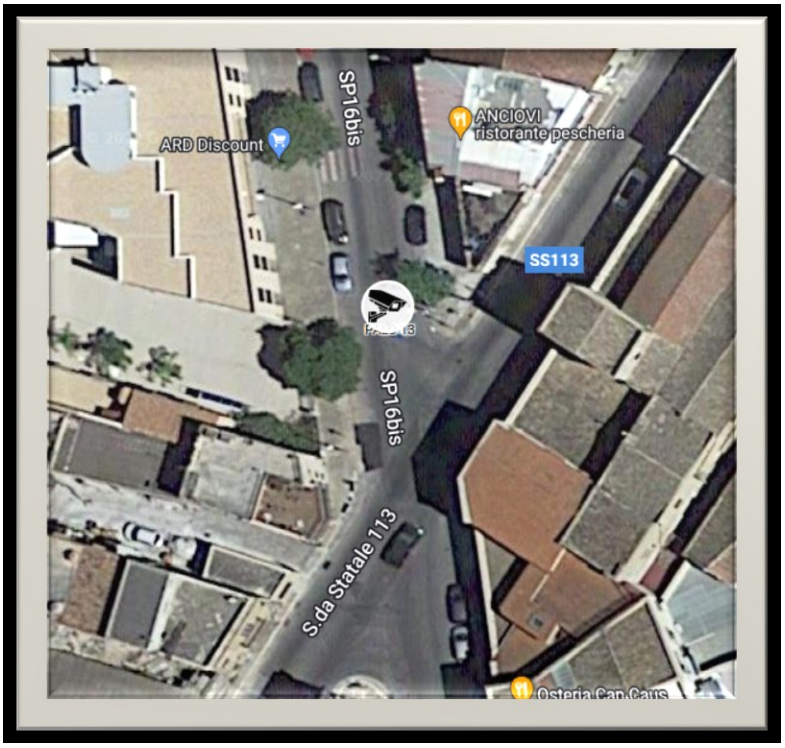

Piazza Garibaldi
Casa Dei Giovani
Via D. d'Amico
Md. Abeer hossain
Edicola Paolo Cangialosi
Edicola
Antico Chiosco Don Gino
Corso Umberto I
Corso Umberto I


Sandro Ferrone
Negozio di abbigliamento donna
Cafè & Caffè Di Lo Verso Vincenzo
Sicily Shop
Negozio di abbigliamento
V.le della Libertà
Corso Butera
Via Quattrociocchi
Bertini Group
Negozio di abbigliamento uomo
Sicilvillas.it
Pescheria Porticello Fish
Pescheria
S Store
Negozio di abbigliamento
Lo Buglio Salvatore
Amat
LES ENFANTS CHIC - Comunioni...
Negozio di abbigliamento per bambini
Corso Butera
Via Collegio


Via Consolare
Via Consolare
Via Catullo
Via Catullo
Via Papa Giovanni XXIII
Comunità Gesuiti


SP74
Corso Italia
Corso Italia
Corso Italia
Corso Italia
Rosa


Via Dottor Filippo Buttitta
Via Lanza
Via Lanza
A19 Palermo - Catania
Palermo - Catania
A19
E90
E90
Via Dottor Filippo Buttitta


SP16bis
ARD Discount
ANCIOVI
ristorante pescheria
SS113
SP16bis
S.da Statale 113
Osteria Can Caus

Le zone di posizionamento corrispondono al centro e le vie principali con 3 telecamere posizionate sul mare. Ogni installazione a palo, comprende 3 telecamere con caratteristiche diverse. Ogni installazione ha integrato un sistema DVR con memorizzazione dei dati. Il sistema comunica con la sede centrale. Una volta raccolte le informazioni per le quali si intende adottare i sistemi descritti, le stesse confluiranno nelle schede SD e visualizzate esclusivamente da personale precedentemente individuato ed autorizzato in tal senso.

Ogni punto è dotato di n.3 telecamere e di n.1 DVR di registrazione, controllati a distanza nella sala di controllo della Polizia Municipale di Bagheria. Presso la centrale operativa è possibile visualizzare le immagini live dei 13 punti collocati nelle aree del comune.

7. Presupposto di liceità

Per quanto attiene al presupposto di liceità è bene rammentare la necessaria sussistenza nel settore pubblico di una norma di legge, anche di rango regolamentare, che in uno stato di diritto deve prevedere e delimitare il perimetro di intervento da parte della pubblica amministrazione in attuazione del principio di legalità sostanziale.

Ed a tal fine il D.L. 23/02/2009, n. 11, all'art. 6, co. 7 espressamente prevede che per la tutela della sicurezza urbana, i Comuni possono utilizzare sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico. Nel caso di specie, il sistema di videosorveglianza è stato oggetto di specifica approvazione da parte della Giunta Comunale con deliberazione n. 312 del 23 dicembre 2021. Non è prevista alcuna comunicazione dei dati raccolti, salvo le ipotesi di obbligo di legge oppure richieste dall'Autorità e dalle Forze di Polizia giudiziaria.

Per quanto attiene al trattamento descritto può essere effettuato senza che sia necessario acquisire il consenso degli interessati, emergendo in relazione all'installazione di un sistema di videosorveglianza l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Comune di Bagheria.

È stata designata la figura di Amministratore di sistema, per quanto concerne il suddetto trattamento, che si occupa della gestione e del controllo dei sistemi utilizzati e delle misure tecniche atte a garantire la sicurezza dei dati acquisiti. L'operato dell'Amministratore di sistema viene controllato costantemente dal Titolare del trattamento dei dati.

Il Comune di Bagheria provvederà a fornire agli interessati coinvolti dai descritti trattamenti, **un'informativa** comprensiva di tutti gli elementi contenuti nell'articolo **13 del GDPR** (es. tipologia di dati, finalità e modalità del trattamento, compresi i tempi di conservazione, etc..) da pubblicare sul sito web del Comune e raggiungibile tramite *QrCode* inserito nel cartello Videosorveglianza secondo le Linee guida EDPB, affisso nei luoghi in cui è effettuata la sorveglianza.

8. Necessità e proporzionalità dei trattamenti

Il Comune di Bagheria raccoglierà e tratterà solo ed unicamente quei dati personali che sono strettamente necessari al perseguimento delle anzidette finalità e che gli stessi sono adeguati, pertinenti e non eccedenti in relazione alle stesse.
È in ogni caso vietata la comunicazione a soggetti non legittimati alla visione delle immagini e la

diffusione su qualsiasi piattaforma informatica delle suddette immagini in maniera illecita potrà essere fonte di responsabilità di natura amministrativa, risarcitoria e penale.
Con riferimento ai suddetti trattamenti di sorveglianza sistematica su larga scala di una zona accessibile al pubblico il Comune di Bagheria ha impostato un periodo di conservazione dei dati trattati pari a 7 giorni, al decorrere dei quali i dati saranno automaticamente e definitivamente cancellati dai sistemi. Quanto ai tempi di conservazione dei dati raccolti si ritiene che la tempistica individuata (7 giorni) in relazione allo scopo di ricostruire dettagliatamente la violazione delle norme regolamentari, sia conforme ai menzionati principi di necessità e proporzionalità. Le immagini possono essere conservate per un periodo più lungo per necessità di esercizio di un diritto in sede giudiziaria nell'ipotesi di condotte che possano integrare norme aventi rilevanza penale, in particolare nel settore dei delitti contro l'ambiente. Tale periodo di **conservazione** è aderente al dettato normativo (D.L. 23/02/2009, n. 11, co. 8) secondo il quale la conservazione dei dati, delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza è limitata ai sette giorni successivi alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione. In generale, il soggetto designato dal Comune di Bagheria potrà accedere al sistema (ed ai dati di videosorveglianza) esclusivamente per finalità di identificazione dell'identità a seguito di eventi lesivi del patrimonio urbano e per finalità di indagini. Il Comune di Bagheria si atterrà, in quanto applicabili, alle prescrizioni ed alle raccomandazioni previste nelle **FAQ** in tema di videosorveglianza del Garante Privacy ed alle **Linee guida 3/2019** sul trattamento dei dati personali attraverso dispositivi video dell'EDPB. L'accesso ai dati trattati è consentito ai soli autorizzati del Comune che, in ragione delle mansioni svolte o degli incarichi affidati, possono prenderne legittimamente conoscenza.

9. Misure tecniche ed organizzative

In base al Regolamento, i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.
Al riguardo, l'art. 32 del Regolamento stabilisce che tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento *ex* art. 28 GDPR, *Tecnotel Energy Srl*, mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.
I dati raccolti dal DVR o storage sono cifrati; lo streaming verso la centrale è realizzato mediante flussi di rete sicuri e cifrati; l'installazione degli apparati superano l'altezza di 3 metri che risulta essere adeguata contro agevoli tentativi di furto; è presente un sistema antifurto collegato con un servizio di vigilanza e pronto intervento. Il data processor, da contratto, si occuperà di mantenere, aggiornare e garantire le misure di sicurezza logiche e fisiche.
Il sistema di autenticazione implementato dal Comune di Bagheria garantisce idonee misure di sicurezza relativamente al formato delle password ed alla memorizzazione delle stesse nel database. Le password utilizzate per l'autenticazione degli operatori non sono infatti memorizzate in chiaro all'interno del data base ma con algoritmo di *hash* SHA 256 composte da 8 caratteri alfanumerici e cambio password degli operatori con scadenza a tre mesi. Il data base è crittografato mediante standard AES per la crittografia simmetrica a 256 bit e le chiavi non sono conservate sullo stesso server dei dati crittografati. Inoltre, risulta implementato un meccanismo che consente la tracciabilità sia degli accessi avvenuti con successo che dei tentativi non riusciti nonché delle

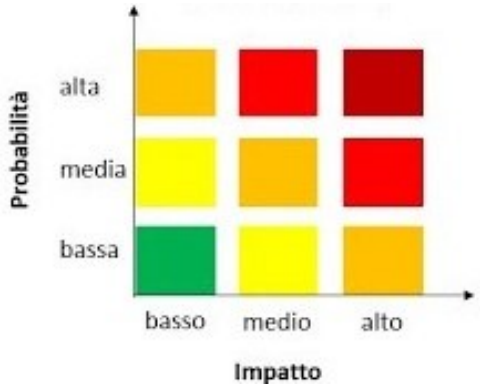
operazioni effettuate (log applicativo) dagli utenti del sistema sui dati personali, siano essi amministratori di sistema ovvero operatori di back office e operatori. Tale accorgimento permette la possibilità di effettuare verifiche *ex post* sull'operato degli addetti rispetto al trattamento informatizzato di un grande volume di dati relativi a un elevato numero di interessati, dati che possono potenzialmente prestarsi a usi fraudolenti in loro danno.

10. Valutazione preliminare dei rischi

Al fine di valutare gli impatti sui diritti e le libertà dei soggetti interessati dalle attività di trattamento di cui alla presente DPIA, la tabella di seguito proposta evidenzia i principali rischi inerenti i dati personali che possono derivare dai Trattamenti in esame. Ogni rischio è valutato sulla base di due elementi: la probabilità che si verifichi in concreto e il livello di impatto. Sulla base di tali elementi è associato il rischio complessivo.

Rischio implicito identificato	Probabilità	Gravità dell'impatto	Livello di rischio generale
Violazione di sicurezza dei dati (*data breach*)	Media	Elevata	Medio
Assenza di un valido presupposto di liceità	Media	Media	Medio
Inadeguatezza delle misure volte alla trasparenza del trattamento (*inidonea informativa*)	Media	Media	Medio
Trattamento per finalità difformi da quelle dedotte	Media	Elevata	Medio
Conservazione dei dati superiore ai limiti di quanto strettamente necessario	Media	Media	Medio
Ostacolo all'esercizio dei diritti degli interessati	Bassa	Media	Medio

Ogni rischio è valutato sulla base di due elementi: la probabilità che si verifichi in concreto e il livello di impatto. Sulla base di tali elementi è associato il rischio complessivo.



11. Misure di sicurezza

Tipologia di rischio	Misure di mitigazione del rischio
Violazione di sicurezza dei dati (*data breach*)	- **Elevato livello di sicurezza dei dati.** Il Comune di Bagheria assicura un elevato livello di misure di sicurezza

Tipologia di rischio	Misure di mitigazione del rischio
	- **Confidenzialità.** Il Comune di Bagheria assicura che solo il personale autorizzato potrà accedere ai dati e trattarli. Ai sensi del GDPR gli stessi sono vincolati da un dovere giuridico alla riservatezza *ex* art. 29 del GDPR
Assenza di un valido presupposto di liceità	- **Base giuridica del trattamento.** Esercizio pubblici poteri.
Inadeguatezza delle misure volte alla trasparenza del trattamento (*inidonea informativa*)	- **Fornire idonea informativa agli interessati**. Gli interessati dovranno ricevere, dal titolare del trattamento, notizia, anche attraverso pubblicazione sul sito web dei dati trattati, delle finalità perseguite, dei tempi di *retention*, della possibilità di esercitare i propri diritti e di ogni ulteriore informazione ritenuta necessaria per un trattamento di dati personali in linea con il principio di trasparenza ai sensi del GDPR.
Trattamento per finalità difformi da quelle dedotte	- **Il trattamento dei dati deve essere limitato all'analisi descritta.** Il Comune di Bagheria non potrà procedere ai Trattamenti per finalità differenti da quelle prese in esame all'interno della presente Valutazione.
Conservazione dei dati superiore ai limiti di quanto strettamente necessario	- **Implementazione di processi di cancellazione automatica.** Il Comune di Bagheria dovrà applicare i periodi di *retention* dei dati descritti nel presente documento vista la loro caratteristica di rispondere ai principi di necessità e minimizzazione.
Ostacolo all'esercizio dei diritti degli interessati	- **Implementare meccanismi per facilitare l'esercizio dei diritti.** Agli interessati deve essere consentito di esercitare i propri diritti di accesso, rettifica, portabilità, opposizione e cancellazione ai sensi del GDPR e di ogni ulteriore disposizione in materia di protezione dei dati personali.

Alla luce delle misure in essere il rischio residuo è stato identificato per ciascuna minaccia significativa identificata secondo quanto riportato di seguito.

Minacce rilevanti per il rischio privacy	Livello di probabilità	Impatto	Rischio Residuo
Attacchi informatici	Medio	Medio	Medio
Abuso di privilegi di accesso	Medio	Alto	Medio
Modifica non autorizzata dei dati	Basso	Alto	Medio
Errori nei processi di elaborazione dei dati	Basso	Alto	Medio
Inefficiente gestione del dato	Basso	Alto	Medio
Perdita integrità per guasto HW	Basso	Alto	Medio
Interrogazioni improprie su basi dati	Medio	Alto	Medio
Furto di apparati hardware principali	Basso	Alto	Medio
Furto o smarrimento dispositivi di acquisizione	Medio	Basso	Medio

Minacce rilevanti per il rischio privacy	Livello di probabilità	Impatto	Rischio Residuo
Intercettazione delle comunicazioni	Basso	Alto	Medio
Utilizzo improprio di software o servizi	Basso	Alto	Medio
Perdita disponibilità per guasto HW	Basso	Medio	Medio
Cancellazione volontaria o accidentale dei dati	Basso	Medio	Medio

Per la riduzione del rischio inerente, sono al momento implementate le seguenti misure di sicurezza:

Minacce rilevanti per il Rischio Privacy	Misure di sicurezza	Livello di probabilità
Attacchi informatici	✓ Monitoraggio degli eventi di sicurezza ✓ Gestione degli incidenti di sicurezza informatica	Medio
Abuso di privilegi di accesso	✓ Definizione anticipata dei profili autorizzativi rispetto all'avvio delle attività di trattamento ✓ Controllo periodico, almeno semestrale, sulla sussistenza delle condizioni per la conservazione dei profili autorizzativi ✓ Adozione procedure per la gestione del ciclo di vita delle credenziali ✓ Disattivazione delle credenziali dell'incaricato al trattamento nel caso in cui non sia più sussistente il presupposto o l'esigenza sottesa al rilascio delle credenziali stesse	Medio
Modifica non autorizzata dei dati	✓ Utilizzo di differenti profili associati alle diverse utenze Adozione di utenze nominali e revisione delle stesse da parte dei relativi responsabili ✓ Obbligo di adozione di password alfanumerica pari a non meno di 8 caratteri alfanumerici ✓ Generazione randomica della password di primo accesso in 8 caratteri	Basso

Minacce rilevanti per il Rischio Privacy	Misure di sicurezza	Livello di probabilità
	alfanumerici	
Errori nei processi di elaborazione dei dati	✓ Strumenti di Data Loss Prevention ✓ Comunicazione del sistema con gli altri sistemi ✓ Predisposizione di apposite nomine con specifiche istruzioni per responsabilizzare le persone autorizzate al trattamento	Basso
Inefficiente gestione del dato	✓ Adeguato periodo di conservazione dei backup dei dati ✓ Adeguata frequenza dei test di restore di backup dati ✓ Adeguata protezione e conservazione dei file di log ✓ Regole di utilizzo sicuro degli strumenti e dei supporti elettronici	Basso
Perdita integrità per guasto HW	✓ Soluzione in alta affidabilità ✓ Regole di utilizzo sicuro degli strumenti e dei supporti elettronici	Basso
Interrogazioni improprie su basi dati	✓ Utilizzo di differenti profili associati alle utenze	Medio
Furto o smarrimento di apparati hardware principali	✓ Soluzioni di sicurezza dei luoghi e delle postazioni di lavoro / dispositivi utilizzati ✓ Crittografia	Basso

Minacce rilevanti per il Rischio Privacy	Misure di sicurezza	Livello di probabilità
Furto o smarrimento dispositivi di acquisizione	✓ Soluzioni di sicurezza delle postazioni di lavoro e dei dispositivi mobili ✓ Crittografia	Medio
Intercettazione delle comunicazioni	✓ Requisiti di sicurezza del sistema	Basso

Minacce rilevanti per il Rischio Privacy	Misure di sicurezza	Livello di probabilità
Utilizzo improprio di software o servizi	✓ Registrazione degli accessi degli utenti ai sistemi ✓ Registrazione e revisione delle attività svolte dagli Amministratori di Sistema	Basso
Perdita disponibilità per guasto HW	✓ Indicazioni rispetto alla modalità di protezione e conservazione dei supporti di backup ✓ Soluzione in alta affidabilità ✓ Adeguata frequenza di backup ✓ Adeguata tipologia di backup effettuati	Basso
Cancellazione volontaria o accidentale dei dati	✓ Misure di sicurezza in caso di change o sviluppo del sistema	Basso

12. Esito della DPIA

Considerato tutto quanto sopra esposto, con particolare riferimento alle finalità dal Comune di Bagheria di efficientare l'utilizzo delle proprie risorse, di erogare un servizio di elevata qualità ai propri utenti e di razionalizzazione dei processi di intervento e assistenza, nonché in considerazione delle misure e degli accorgimenti che il Comune di Bagheria intende implementare, si ritiene di poter sostenere che lo svolgimento dei Trattamenti, nei limiti e con tutte le cautele e tutele esposte nella presente DPIA, non presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati coinvolti.

Tale sistema di videosorveglianza, non comporta, in concreto, un pregiudizio rilevante per l'interessato, idoneo a determinare effetti particolarmente invasivi sulla sua sfera di autodeterminazione e, più in generale, sui suoi diritti e libertà fondamentali. Infatti, non risulta che il sistema attivi ulteriori funzionalità, anche eventualmente legate al comportamento dell'interessato ripreso, quali, ad esempio, la capacità di rilevare i percorsi, l'analisi audio, la geolocalizzazione o il riconoscimento tramite incrocio con ulteriori specifici dati personali o confronto con una campionatura precostituita ovvero tramite sistemi di riconoscimento facciale. A tal proposito, la tabella sotto riportata rende evidenza dei differenti livelli di rischi inerenti i dati personali prima e dopo l'implementazione delle misure di mitigazione descritte nella tabella precedente.

Rischio implicito identificato	Livello di rischio generale pre-implementazione	Livello di rischio generale post-implementazione
Violazione di sicurezza dei dati (*data breach*)	Medio	Basso
Assenza di un valido presupposto di liceità	Medio	Basso

Rischio implicito identificato	Livello di rischio generale pre-implementazione	Livello di rischio generale post-implementazione
Inadeguatezza delle misure volte alla trasparenza del trattamento (*inidonea informativa*)	Medio	Basso
Trattamento per finalità difformi da quelle dedotte	Medio	Basso
Conservazione dei dati superiore ai limiti di quanto strettamente necessario	Medio	Basso
Ostacolo all'esercizio dei diritti degli interessati	Basso	Basso

13. Misure implementate e/o da implementare per la gestione del rischio

Le misure idonee per la gestione del rischio sono implementate. Il livello di rischio generale risultante risulta MEDIO. Ulteriori misure, atte a garantire un continuo miglioramento della sicurezza dei dati oggetto del trattamento, saranno implementate. Inoltre, alla luce della DPIA effettuata, non si ritiene necessario inviare il presente documento per la condivisione con l'Autorità Garante (obbligo sussistente solo in assenza di misure di sicurezza idonee ad attenuare i rischi connessi al trattamento dei dati).

14. Revisione e aggiornamento

Il Titolare si impegna a riesaminare la presente DPIA per verificare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati e almeno quando si registra una variazione del relativo rischio.