Data Protection Impact Assessment

(DPIA)

Comune di Bagheria

Sorveglianza sistematica mobile su larga scala di una zona accessibile al pubblico

TRATTAMENTO DATI: Videosorveglianza Mobile

Sommario

1. Introduzione 3
2. Obiettivo del documento 3
3. Definizioni 4
4. Contesto normativo 4
5. Descrizione, caratteristiche e finalità dei trattamenti 4
6. Tipologie di dati trattati 6
7. Presupposto di liceità 6
8. Necessità, proporzionalità dei trattamenti e misure tecniche ed organizzative 8
9. Valutazione preliminare dei rischi 10
10. Misure di sicurezza 11
11. Esito della DPIA 15
12. Misure implementate e/o da implementare per la gestione del rischio 15
13. Revisione e aggiornamento 16

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 la responsabilità di adottare tutte le misure necessarie al fine di garantire la sicurezza e la protezione dei dati. La Carta dei diritti fondamentali dell'Unione Europea, nota anche come Carta di Nizza, stabilisce un certo numero di diritti che tutti i cittadini europei hanno. In particolare, l'articolo 8 della Carta riguarda la protezione dei dati personali, affermando che *"ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza"*. La protezione delle informazioni personali è di fondamentale importanza nell'Unione Europea e la Carta di Nizza fornisce una base legale per le regole del GDPR. La Carta fornisce una definizione e alcuni principi chiave che dovrebbero regolare la gestione dei dati personali, compreso il diritto di essere informati in caso di raccolta di dati e di accedervi. Secondo la Corte di Giustizia dell'UE. una legislazione in materia di protezione dei dati personali è essenziale per garantire a ciascun cittadino europeo la possibilità di esercitare i propri diritti fondamentali, sottolineando che l'adeguata protezione dei dati personali è un'esigenza primaria per l'esercizio di altri diritti fondamentali come la vita e l'onore, la libertà di espressione, la libertà di informazione e di associazione. 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. Una DPIA (*Data Protection Impact Assessment*) è un documento che descrive le misure di sicurezza che un'organizzazione deve prendere per garantire la conformità del processo in esame alle normative e alle regole sulla protezione dei dati. Per scrivere una DPIA, la prima cosa da fare è identificare le entità coinvolte, identificare le risorse da proteggere, individuare i rischi ai quali potrebbero essere esposti i dati, valutare i possibili rischi e valutare gli eventuali mezzi da implementare per prevenire tali minacce. Successivamente, devi documentare i controlli sulla sicurezza dei dati, l'accesso ai dati tramite database, l'eventuale archiviazione dei dati e i processi di gestione dei problemi di sicurezza. Una volta che tutte queste attività sono state completate, il documento può essere elaborato per segnalare le misure di sicurezza documentate. La DPIA aiuta a identificare ed eliminare i possibili rischi per la protezione dei dati personali, aiutando il Comune a raggiungere equilibrio tra le possibilità aperte, i limiti delle tecnologie e gli obblighi legali.

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 delle libertà degli interessati.

5. Descrizione, caratteristiche e finalità dei trattamenti

Come considerazione preliminare di contestualizzazione, il Comune di Bagheria intende procedere all'installazione di telecamere mobili di videosorveglianza per l'individuazione dei

responsabili di abbandono incontrollato di rifiuti e per l'inosservanza dell'eco calendario in vigore nel territorio del Comune di Bagheria. Segnatamente, si intendono sanzionare le violazioni alle norme comportamentali che sono lesive del decoro urbano per i divieti di:

a) depositare rifiuti o materie di qualsiasi specie, insudiciare o imbrattare comunque la strada e le sue pertinenze;
b) sporcare la strada e le sue pertinenze gettando rifiuti o oggetti dai veicoli in sosta o in movimento;
c) scaricare, senza regolare concessione, nei fossi e/o nelle cunette materiale o cose di qualsiasi genere o incanalare in essi acque di qualunque natura;
d) gettare dai veicoli in movimento qualsiasi cosa.

Le finalità del Trattamento, così come meglio descritti sopra, è rinvenibile nella necessità del Comune di Bagheria di garantire il decoro urbano ed evitare il degrado ambientale, nei limiti dei poteri individuati dalla normativa di settore. La tutela dell'ambiente viene sancita nella Costituzione italiana all'interno dell'Articolo 9, il quale sancisce la tutela e l'equilibrio del patrimonio ambientale come un interesse fondamentale della Repubblica. Nel medesimo articolo, inoltre, viene sancita la cessazione dei processi di degrado ambientale, anche nell'interesse delle future generazioni. Nell'articolo 117 si menzionano anche le competenze legislative e amministrative in materia ambientale che vengono ripartite tra Stato e Regioni, tra le quali la tutela dell'aria, del suolo, del territorio, del paesaggio e delle acque. Inoltre, all'interno della stessa Costituzione vengono sanciti obblighi morali, etici e giuridici in merito alla cura dell'ambiente, per garantire i diritti di tutti i cittadini. Il decoro urbano è uno degli aspetti chiave per la cura del territorio e delle città ed è, in definitiva, positiva per la collettività, sia dal punto di vista della salute, sia da quello sociale. Il contrasto all'abbandono dei rifiuti da parte dei Comuni italiani ha un valore sociale significativo, poiché contribuisce alla creazione e alla preservazione di condizioni generali di benessere nel territorio. L'abbandono dei rifiuti è causa di notevoli problemi dal punto di vista sanitario, sociale e ambientale; la presenza di materiali di rifiuto potenzialmente pericolosi può infatti rappresentare una grave minaccia per la salute e all'integrità ecologica. Secondo l'OMS, l'abbandono dei rifiuti è tra le principali cause dello sviluppo della povertà nelle nazioni in via di sviluppo. Al contrario, la rimozione dei rifiuti abbandonati contribuisce al miglioramento delle condizioni di vita di coloro che vivono nelle aree circostanti. Inoltre, interventi di rimozione e smaltimento dei rifiuti abbandonati compensano parzialmente gli effetti sociali ed ambientali della loro accumulazione, contribuendo anche a tutelare l'utilizzo degli spazi pubblici da parte della collettività.

L'Organizzazione delle Nazioni Unite (ONU) considera l'abbandono dei rifiuti come una delle principali minacce al contesto ambientale e al benessere della collettività. A livello mondiale, l'ONU pubblica diverse statistiche sull'abbandono dei rifiuti nel mondo, rilevando che milioni di tonnellate di rifiuti finiscono ogni anno nelle discariche a terra, corsi d'acqua e in mare. Per far fronte a tali situazioni e incrementare una maggiore consapevolezza dei danni ambientali e sociali causati dall'abbandono dei rifiuti, l'ONU ha introdotto una serie di piani d'azione volti a sostenere e incoraggiare le comunità nella gestione responsabile dei rifiuti. La più importante di queste è *Sustainable Development Goal n° 12*, il cui obiettivo è quello di ottenere entro il 2030 una "gestione sostenibile, ragionevole e sicura dei rifiuti", compresa la promozione della riutilizzazione, del riciclaggio, della riduzione dei rifiuti e dell'abbattimento di tutti i tipi di abbandono.

Secondo il Fondo Monetario Internazionale, l'abbandono dei rifiuti urbani comporta una serie di problemi ambientali, sociali ed economici per le comunità in tutto il mondo. Inoltre, le conseguenze dannose sono amplificate nelle nazioni a basso reddito, dove mancano spesso le infrastrutture e le

risorse necessarie per gestire una corretta gestione dei rifiuti. L'FMI incoraggia i Paesi a sviluppare programmi sostenibili per la gestione dei rifiuti urbani, con una forte focalizzazione sulla reduzione, riciclaggio e riutilizzo dei rifiuti. Inoltre, il FMI consiglia di introdurre politiche di prevenzione dell'abbandono dei rifiuti, aumentare l'efficienza nella raccolta rifiuti, investire nella ricerca e sviluppo di tecnologie più radicali per la gestione dei rifiuti, sviluppare sistemi di incentivazione ed educare i cittadini. La videosorveglianza svolge un ruolo fondamentale nel contrasto all'abbandono dei rifiuti. L'utilizzo delle telecamere per la videosorveglianza può infatti contribuire a ridurre le attività illegali di abbandono dei rifiuti, a identificare i responsabili delle violazioni e a prevenirne altre. L'utilizzo della videosorveglianza può, inoltre, aiutare a individuare tempestivamente le aree della città frequentate da persone che abbandonano i rifiuti, generare allarmi per prevenire tali azioni e individuare i trasgressori. L'utilizzo della videosorveglianza per contrastare l'abbandono dei rifiuti può essere anche utile per monitorare i materiali di rifiuto pericolosi, dimostrandosi quindi un ottimo strumento per la prevenzione dei rischi ambientale.
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 e financo penale.

6. Tipologie di dati trattati

I Trattamenti delle immagini videoregistrate verranno effettuati mediante videosorveglianza mobile *e-Killer Flex 2.0* installate dal Corpo della Polizia Municipale del Comune di Bagheria anche tramite il supporto di operatori specializzati debitamente individuati come autorizzati al trattamento per il posizionamento e la consegna delle schede SD.
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. 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.

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. Inoltre, il Testo unico delle leggi sull'ordinamento degli enti locali, prevede che il Sindaco, quale rappresentante della comunità locale, in relazione all'urgente necessità di interventi volti a superare situazioni di grave incuria o degrado del territorio, dell'ambiente e del patrimonio culturale o di pregiudizio del decoro e della

vivibilità urbana possa adottare ordinanze contingibili ed urgenti. Non è prevista alcuna comunicazione dei dati raccolti, salvo le ipotesi di obbligo di legge oppure richieste dall'Autorità. Tali dati potranno comunque essere visualizzati in tempo reale ma comunque con accesso controllato e con registrazione dei log che riportano gli orari di accesso – uscita dal sistema. 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, anche 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 di seguito riportato:

8. Necessità, proporzionalità dei trattamenti e misure tecniche ed organizzative

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.

In generale, l'articolo 32 del GDPR richiede che il titolare del trattamento adotti misure tecniche ed organizzative adeguate per assicurare un livello di sicurezza adeguato al rischio. Le misure tecniche possono includere l'utilizzo di crittografia, divisione dei dati, limitazione degli accessi autorizzati, notifica di incidenti di sicurezza, e il monitoraggio e il rilevamento degli accessi non autorizzati. Le misure organizzative possono includere le procedure documentate per affrontare attacchi informatici, definire responsabilità di sicurezza, la formazione dei dipendenti, controlli a campione, l'assistenza contabile, la gestione del ciclo di vita dei dati e l'applicazione di penalità per il mancato rispetto delle politiche. Le misure tecniche e organizzative adottate dipendono dall'entità coinvolta e dall'entità dei dati trattati.

Per quanto attiene alle misure di sicurezza si precisa che le “foto trappole” installate presso luoghi sensibili del territorio. Al fine di ridurre i rischi da furto doloso dei file video è dotato di sistema di sicurezza ed ancoraggio consistente in una gabbia metallica in acciaio inox che previene sia il furto della strumentazione e di conseguenza dei dati contenuti al suo interno. La SD non è facilmente accessibile per l’utente e per accedervi si rende necessario aprire il dispositivo con degli attrezzi. L’utente, infatti, non avrà mai la necessità di accedervi fisicamente ma utilizzerà per questo, l’accesso all’interfaccia di gestione della telecamera. Solo dall’interfaccia abilitata, potrà estrapolare i filmati per i secondi/minuti, utili alle finalità di utilizzo dello strumento.

Tale protezione di livello fisico non esclude completamente il rischio concreto di accesso ai dati e quindi, si è pensato di adottare ulteriori misure di sicurezza, introducendo la modalità di scrittura dei dati sulla memoria interna (micro – SD da 256 GB) attraverso l’uso della crittografia: AES 256 bit. La crittografia è importante per la privacy, poiché fornisce un modo sicuro per proteggere le informazioni sensibili online. Se un utente decide di crittografare i propri dati, questi verranno criptati in modo che solo l'utente che conosce la chiave può accedervi. Ciò rende più difficile (se non impossibile) per gli hacker o gli intrusi non autorizzati leggere, rubare o usare le informazioni. La crittografia aiuta anche a mantenere l'anonimato e la riservatezza dei dati personali. AES 256 (Advanced Encryption Standard) è un cifrario a blocchi crittografico a chiave simmetrica che viene utilizzato per proteggere le comunicazioni dati sotto forma di testo, audio e video. Algoritmi di crittografia robusti aggiungono minimo 256 bit di lunghezza ai dati di input, consentendo di cifrare i dati in modo che non possano essere decifrati senza la chiave appropriata. La lunghezza della chiave viene espansa per sensibilmente aumentare la sicurezza e l'AES 256 bit fornisce una maggiore sicurezza ai dati rispetto ai sistemi con una chiave più breve.

Qualora venisse rimossa la micro-SD contenente i video ed eventuali foto registrate dalla telecamera non sarà possibile leggerli attraverso l’uso di un computer e un player (VLC, Windows Mediaplayer ecc…). Per limitare il raggio di visualizzazione della zona controllata, i nostri sistemi sono dotati di ottiche zoommate e non di ottiche grandangolari, per limitare così il raggio di azione della telecamera e avere maggiore dettaglio sulla zona di interesse. In aggiunta qualora l’apparato dovesse inquadrare aree non oggetto di controlli, è possibile attivare zone di privacy masking che possono essere oscurate o mosaicizzate una volta completato il puntamento. Le zone interessate da privacy masking non verranno registrate. L’accesso alle due videocamere può avvenire:

- mediante wi-fi, in cui la chiave di accesso alla rete WiFi avviene tramite Encryption: WPA2-PSK con password di almeno 11 caratteri e con la possibilità di limitare l'accesso alla rete wi-fi soltanto a

determinati *MAC ADDRESS*, profilabili all'interno del menu di sicurezza wireless del router contenuto all'interno del sistema; - ed in remoto: 1) con sistema P2P per il reindirizzamento dell'indirizzo IP dinamico della strumentazione (*il sistema P2P permette di rilevare l'indirizzo della telecamera dotata di Sim con doppio nat e nessun indirizzo IP pubblico statico e quindi di accedere ad essa attraverso software specifico del produttore*); 2) Tramite la realizzazione di una VPN, tra router a bordo telecamera e client; 3) tramite IP statico sulla Sim della videocamera: in questo caso la stessa sarà accessibile da remoto, utilizzando un IP pubblico statico con porte assegnate per l'accesso e quindi non sarà quindi necessario installare nessun software (client VPN) sul computer destinato all'utilizzo della strumentazione. L'accesso all'interfaccia web avviene tramite inserimento di nome utente e password. L'utente admin ha accesso a tutte le funzioni della telecamera e alla vista live e Playback. Possono essere creati diversi altri utenti e possono essere profilati ed autorizzati soltanto all'accesso in live, alle registrazioni e alle funzionalità avanzate. 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 mediante sovrascrittura delle SD. Definire un periodo di conservazione dei dati è importante perché aiuta a ridurre il rischio di accesso non autorizzato e abuso dei dati. Inoltre, definire un periodo di conservazione più breve significa che sarà più facile rimuovere i dati non più necessari. I titolari hanno la responsabilità di assicurarsi che i dati vengano archiviati in modo appropriato e i periodi di conservazione di solito variano a seconda della natura dei dati trattati, della legge e dei requisiti contrattuali. 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. Il principio di proporzionalità del trattamento dei dati personali è un principio stabilito dal GDPR che richiede che i titolari del trattamento considerino l'equilibrio tra la natura dei dati personali da trattare, l'entità dei dati da trattare, la portata dei potenziali rischi presentati e l'interesse pubblico. Nello specifico, è importante che un titolare del trattamento non usi tecniche troppo invasive quando non è necessario farlo. Ad esempio, il titolare del trattamento dovrebbe utilizzare solo le tecniche necessarie per far fronte a una determinata situazione e non tutte le misure possibili. 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, mediante sovrascrittura delle micro-SD da 256 GB, 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 del soggetto che abbia trasgredito a norme inerenti al deposito illecito di rifiuti. 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. Secondo le Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video dell'EDPB, devono essere prese misure adeguate per prevenire abusi, assicurare la riservatezza e la protezione dei dati raccolti. Le Linee Guida chiamano in causa anche la documentazione, contestualizzando come i titolari del trattamento devono motivare l'utilizzo dei

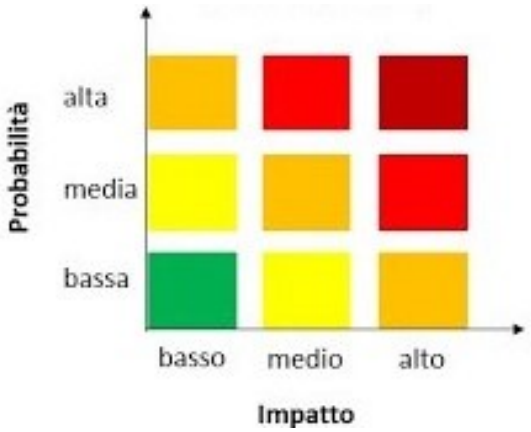
dispositivi video, descrivere come i dati raccolti dalle telecamere saranno trattati, e limitare la durata della loro conservazione. Altre misure utili descritte nelle linee guida comprendono i requisiti di trasparenza, la regolamentazione dell'accesso ai dispositivi video, l'impegno nei confronti della privacy e della sicurezza dei dati, l'applicazione di misure di sicurezza informatica conformi ai requisiti GDPR come la privacy by design, l'uso di processi di gestione dei dati sicuri, e la creazione di meccanismi di notifica per avvisare le persone interessate in caso di violazione. 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. Il sistema di videosorveglianza, in particolare le fototrappole sono installate nei punti della Città Metropolitana.

9. 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.



10. 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: AES 256 - **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 in maniera automatizzata mediante sovrascrittura delle SD, vista la loro caratteristica di rispondere ai principi di necessità e minimizzazione.

Tipologia di rischio	Misure di mitigazione del rischio
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, 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
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
	✓ Definizione anticipata dei profili autorizzativi rispetto all'avvio delle	

Minacce rilevanti per il Rischio Privacy	Misure di sicurezza	Livello di probabilità
Abuso di privilegi di accesso	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 11 caratteri alfanumerici ✓ Generazione randomica della password di primo accesso in 11 caratteri alfanumerici	Basso
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 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

Minacce rilevanti per il Rischio Privacy	Misure di sicurezza	Livello di probabilità
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 ✓ AES 256-bit	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 ✓ AES 256-bit	Medio
Intercettazione delle comunicazioni	✓ Requisiti di sicurezza del sistema	Basso
Utilizzo improprio di software o servizi	✓ Registrazione degli accessi degli utenti ai sistemi ✓ Registrazione e revisione delle attività svolte dagli operatori	Basso
Perdita disponibilità per guasto HW	✓ Indicazioni rispetto alla modalità di protezione e conservazione dei supporti di backup ✓ Soluzione in alta affidabilità	Basso
Cancellazione volontaria o accidentale dei dati	✓ Misure di sicurezza in caso di change o sviluppo del sistema	Basso

11. Esito della DPIA

Considerato tutto quanto sopra esposto, con particolare riferimento alle finalità del 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.

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
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

12. 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 BASSO. 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).

13. Revisione e aggiornamento

Il Titolare si impegna trascorso il periodo di un anno dalla data di approvazione della suddetta DPIA, a riesaminare la stessa, 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.

Bagheria, 09 dicembre 2022