p_pa Città Metropolitana di Palermo RGP
Allegato n.1 al PROT 0059519 del 26/07/2024
CL 9.13.6.0.0.0/1/2022 - 26/07/2024

Città Metropolitana di Palermo
Direzione Polizia Metropolitana e Protezione Civile

Via Roma n. 19 - 90139 Palermo - Tel. 091 6628798
MAIL: polizia@cittametropolitana.pa.it - PEC: polizia@cert.cittametropolitana.pa.it

DATA PROTECTION IMPACT ASSESSMENT

-

VALUTAZIONE D'IMPATTO

UTILIZZO DI IMPIANTI DI VIDEOSORVEGLIANZA NEL TERRITORIO DELLA CITTÁ METROPOLITANA DI PALERMO

Sommario

Allegato N. 1
INFORMAZIONI TECNICHE INERENTI AL SISTEMA DI VIDEOSORVEGLIANZA

Informazioni sulla DPIA

Nome della DPIA

VIDEOSORVEGLIANZA DELLA CITTA'
DATA CREAZIONE

1. Premessa

1.1 **Scopo del documento**

La DPIA si rende necessaria, a norma dell'art. 35, ogniqualvolta dal trattamento possa conseguire un rischio elevato per i diritti e le libertà delle persone interessate, anche durante un trattamento già in corso di esecuzione, qualora si verifichi un mutamento nelle finalità di quest'ultimo o una modifica dei dati stessi che comporti una maggiore percentuale di rischio.
La valutazione di impatto privacy è necessaria nel caso di sistemi integrati – sia pubblici, sia privati – che collegano telecamere tra soggetti diversi, o nel caso di sistemi intelligenti, capaci di analizzare le immagini ed elaborarle, per rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli. È il caso, soprattutto della videosorveglianza pubblica, che consente la visione delle immagini a soggetti diversi e che si avvalgono di appositi software per l'analisi delle immagini e per il lancio degli allarmi in caso di riscontrate anomalie.
La valutazione d'impatto sulla protezione dei dati è sempre richiesta, in particolare, in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico (articolo 35, paragrafo 3, lettera c) del Gdpr) e negli altri casi indicati dal Garante con il provvedimento 467 dell'11 ottobre 2018. In quest'ultima deliberazione, l'Autorità Garante per la Privacy ha individuato un elenco delle tipologie di trattamenti, comunque non esaustivo, da sottoporre a valutazione d'impatto.
Il modello della presente DPIA è stato estratto, senza rielaborazioni sostanziali, dallo strumento PIA (valutazione di impatto sulla protezione dei dati) progettato dalla Commission Nationale de l'Informatique et des Libertés (CNIL v. 2.3.0), autorità di controllo francese, esplicitamente validato e suggerito anche dal Garante per la protezione dei dati personali italiano.

1.2 **Visibilità del documento**

Il documento è principalmente indirizzato alle persone coinvolte nel lavoro di attuazione della normativa in materia di protezione dati.

1.3 **Definizioni, acronimi e abbreviazioni**

Espressione/Acronimo	Definizione/Significato
Servizio	Utilizzo degli impianti di videosorveglianza attivati nel territorio della Città Metropolitana (PA)
Titolare del trattamento	Ovvero anche solo "Titolare" è secondo l'art. 4 del RGPD è "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". Nel contesto di questo documento, il titolare è la Città Metropolitana di Palermo, cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali
Responsabile del trattamento	Soggetto/Azienda Fornitrice del servizio, eventualmente nominata Responsabile del trattamento ai sensi dell'art. 28 del Reg. UE 2016/679
Interessato	La persona fisica cui si riferiscono i dati personali oggetto di trattamento.

	Trattasi di una persona fisica identificata ovvero identificabile in modo diretto o indiretto
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come ad esempio la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (GDPR, Articolo 4, Comma 2).
Rischio	Nel contesto del presente documento, il prodotto tra la probabilità di ledere i diritti e le libertà delle persone fisiche a cui i dati personali trattati si riferiscono e l'impatto su tali diritti e libertà che si verrebbe a produrre per l'interessato ove l'evento temuto (c.d. "minaccia") si dovesse verificare.
DPIA/PIA	General Data Protection Regulation. 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)

2. Contesto

2.1 **Panoramica del trattamento**

2.1.1 **Quale è il trattamento in considerazione?**

Il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza (VDS) attivati nel territorio dell'Ente, operato dalla Città Metropolitana di Palermo, avviene da parte del Sindaco pro tempore, e dei soggetti specificatamente autorizzati.

Per le immagini riprese e/o registrate nella Città Metropolitana di Palermo, il titolare dei dati è la Città Metropolitana medesima. A tal fine è rappresentata dal Sindaco, a cui compete ogni decisione circa le modalità del trattamento, ivi compreso il profilo della sicurezza. Per le immagini riprese e/o registrate in altri Comuni, eventualmente convenzionati, il titolare dei dati è il Comune convenzionato.

Le finalità di utilizzo degli impianti di videosorveglianza sono conformi alle funzioni istituzionali attribuite all'Ente Locale dalla legge 7 marzo 1986, n. 65 sull'ordinamento della Polizia Locale, dallo statuto e dai regolamenti, dalla direttiva UE 2016/680 attuata con decreto lgs. 18 maggio 2018, n. 51 nonché dal decreto-legge n. 14 del 20 febbraio 2017 convertito in legge n. 48 del 13 aprile 2017 "disposizioni urgenti in materia di sicurezza delle città" e successive modificazioni ed integrazioni e dalle altre disposizioni normative applicabili alla Città Metropolitna di Palermo.

Il trattamento dei dati personali mediante sistemi di videosorveglianza è effettuato ai fini di:

- **tutela della sicurezza urbana e della sicurezza pubblica**

- attività di prevenzione, indagine, accertamento e perseguimento di atti delittuosi e/o attività illecite, tutelare l'ordine, il decoro e la quiete pubblica, monitorare le aree oggetto di deturpazione da parte dell'utenza al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" e dei poteri attribuiti al Sindaco in qualità di autorità locale;

- **tutela del patrimonio della Città Metropolitana di Palermo**
  - vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato;
- **tutela della sicurezza stradale e controllo della circolazione dei veicoli**
  - monitorare e controllare la viabilità e i flussi di traffico, accertamento delle violazioni delle norme di comportamento del Codice della Strada;
- **tutela ambientale e polizia amministrativa**
  - controllare aree specifiche del territorio della Città Metropolitnana per prevenire e reprimere ogni tipo di illecito, di natura penale o amministrativa, in particolare legato a fenomeni di degrado, di discarica di materiale e di sostanze pericolose o di abbandono di rifiuti, oltre che svolgere controlli volti ad accertare le violazioni delle norme contenute nei regolamenti dell'Ente;
- unicamente in qualità di **polizia giudiziaria**, prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nell'ambito di attività di P.G.

Nel rispetto delle finalità previste, dalle immagini di videosorveglianza potranno essere acquisiti elementi strettamente necessari alla verbalizzazione di violazioni amministrative, nel rispetto del principio di minimizzazione ex art. 5 RGPD e delle vigenti normative e regolamenti.

2.1.2 **Quali sono le responsabilità connesse al trattamento?**

Le responsabilità connesse al trattamento come sopra identificato, sono ascrivibili alla gestione delle attività di accesso, salvataggio, archiviazione, nonché nelle attività manutentive legate all'utilizzo degli impianti VDS.
Il trattamento effettuato mediante il prodotto tecnologico si configura come potrebbe potenzialmente configurarsi come sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
La presente analisi garantisce che il trattamento dei dati personali, effettuato mediante l'attivazione di sistemi di videosorveglianza gestiti e impiegati dala Città Metropolitana nel proprio territorio, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale; garantisce, altresì, i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento, avuto riguardo anche alla libertà di circolazione nei luoghi pubblici o aperti al pubblico.
La presente valutazione di impatto viene svolta in quanto si intende valutare i rischi associati al trattamento, le misure identificate per attenuarli al fine di evitare che il trattamento effettuato mediante l'utilizzo dello strumento tecnologico messo a disposizione possa, potenzialmente, ledere i diritti e le libertà degli interessati ai quali i dati si riferiscono.

2.1.3 **Ci sono standard applicabili al trattamento?**

Non pare siano presenti standard applicabili direttamente al trattamento; tuttavia, l'attività di videosorveglianza, è disciplinata da numerosi provvedimenti:

- Provvedimento generale in materia di videosorveglianza in ambito pubblico e privato del 08 aprile 2010 del Garante della protezione dei dati personali (G.U. n. 99 del 29/04/2010);
- Linee guida sulla Videosorveglianza negli enti locali dell'ANCI del 09 novembre 2010;
- Circolare del Ministero dell'Interno inerente i Sistemi di videosorveglianza e relative specifiche tecniche per i Comuni del 02 marzo 2012 e successive indicazioni;
- Regolamento UE Generale sulla Protezione dei Dati 2016/679 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" (anche "RGPD/GDPR");
- Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali" some modificato ed integrato dal D.Lgs 101/2018;
- Allegato 1 al provvedimento n. 467 dell'11 ottobre 2018, pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018, inerente all'elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto del Garante della protezione dei dati personali;
- Direttiva UE 2016/680 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", recepita con il D.lgs. 51/2018;
- riferimento agli articoli 7 del D.lgs. 51/2018 (sul trattamento di categorie particolari di dati personali), 6 c. 7 del D.L. 11/2009 (sule Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori") e 54 del D.lgs. 267/2000 (Testo Unico Enti Locali);
- DPR del 15 gennaio 2018, n. 15, recante "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";
- Decreto-legge 20 febbraio 2017, n. 14, convertito, con modificazioni, dalla legge 18 aprile 2017, n. 48, recante "Disposizioni urgenti in materia di sicurezza delle città" e successive modificazioni ed integrazioni del D.L. 14.06.19 n. 53 convertito con modifiche con L. 8 agosto 2019 n. 77.
- Linee guida 03/2019 v.2 del 29 gennaio 2020 pubblicate dall'EDPB, inerenti al trattamento di dati personali attraverso dispositivi video;
- Le regole per installare telecamere del 05 dicembre 2020, il vademecum e le FAQ in materia di videosorveglianza del 03 dicembre 2020 del Garante della protezione dei dati personali.
- Regolamento per lo svolgimento dell'attività di videosorveglianza della Città Metropolitana di Palermo approvato con decreto del Sindaco Metropolitano N.32 del 13/03/2024

2.2 **Dati, processi e risorse di supporto**

2.2.1 **Quali sono i dati trattati?**

Costituisce videosorveglianza quel complesso di strumenti finalizzati alla vigilanza in remoto, che si realizza a distanza mediante dispositivi di ripresa video, captazione di immagini ed eventuale conseguente analisi, collegati a un centro di controllo.
I dati personali sono raccolti attraverso riprese video e captazione di immagini effettuate da sistemi di telecamere installate in luoghi pubblici ed aperti al pubblico e lungo le arterie stradali del territorio provinciale ubicati nel territorio di competenza.
Gli impianti riprendono e registrano immagini che permettono di identificare in modo diretto o indiretto le persone riprese. Inoltre, sono trattati i dati degli autoveicoli (n. targa) e persone fisiche che circolano in prossimità delle telecamere.

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

Il ciclo di vita dei dati prevede i seguenti trattamenti:
acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto, interconnessione, limitazione, pseudonimizzazione.
L'impianto di VDS in esame consente riprese video e foto, diurne e notturne, in condizioni sufficienti di illuminazione naturale ed artificiale. L'impianto è sempre in funzione ed è configurato per la registrazione continuativa.
Inoltre le telecamere non sono dotate di microfono né di sensori di rilevamento e biometrico.
Per le informazioni inerenti al numero delle telecamere, schede tecniche di dettaglio, luogo di installazione, finalità perseguita, si rimanda alla tabella allegata alla presente D.P.I.A. (all. 1).
Le telecamere consentono riprese video e sono collegate alla sala di controllo del Comando di Polizia Metropolitana della Città Metropolitana di Palermo.
Le immagini sono visualizzate in tempo reale su due monitor direttamente presso la sala di controllo ubicata presso il comando di polizia metropolitana, da personale autorizzato. Il sistema è a circuito chiuso, senza possibilità di accesso da remoto.
Le videocamere sono accessibili tramite app dedicata e criptata da cellulare di servizio in dotazione al personale autorizzato addetto Servizio di Videosorveglianza.
Il luogo di salvataggio delle immagini si trova presso la sala di controllo del Comando di Polizia Metropolitana della Città Metropolitana di Palermo. Il salvataggio avviene su server dedicato e su due dispositivi di archiviazione mobile custoditi in una armadio di sicurezza tutti ubicati all'interno della sala di controllo.

Il sistema VDS in uso al Comando di Polizia Metropolitana comprende apparecchi quali:

- telecamere posizionate presso il territorio della Città Metropolitana di Palermo la cui finalità è la prevenzione di atti criminosi quali attività di prevenzione, indagine, accertamento e perseguimento di atti delittuosi e attività illecite
- sistemi mobili di videosorveglianza da posizionare in località difficilmente accessibili o sorvegliabili, al solo titolo esemplificativo zone di campagna, strade interpoderali o aree urbane oggetto di degrado. La finalità dell'utilizzo di tali sistemi di controllo è quella di monitorare le aree oggetto di deturpazione da parte dell'utenza laddove non è possibile farlo diversamente, ai fini sia dell'accertamento delle eventuali violazioni amministrative, sia ai fini della deterrenza alla prosecuzione di azioni di degrado da parte della cittadinanza e dell'utenza di passaggio;
- apparecchi per l'accertamento delle violazioni delle norme di comportamento del Codice della Strada, che consentono la determinazione dell'illecito in tempo successivo, poiché il veicolo oggetto del rilievo è a distanza dal posto di accertamento o comunque nell'impossibilità di essere fermato in tempo utile o nei modi regolamentari, siano esse in postazione fisse o mobili, in presenza o meno dell'operatore. I sistemi elettronici di rilevamento delle infrazioni inerenti violazioni del codice della strada vanno obbligatoriamente segnalate da cartello/informativa anche in base alla disciplina di settore. L'utilizzo di tali sistemi è lecito se sono raccolti solo dati pertinenti e non eccedenti per il perseguimento delle finalità istituzionali del titolare, delimitando a tal fine la dislocazione e l'angolo visuale delle riprese. La ripresa del veicolo non deve comprendere (o deve mascherare), per quanto possibile, la parte del video o della fotografia riguardante soggetti non coinvolti nell'accertamento amministrativo (es. eventuali pedoni o altri utenti della strada). Le fotografie o i video che attestano l'infrazione non devono essere inviati al domicilio dell'intestatario del veicolo, ma l'interessato, ossia la persona eventualmente ritratta nelle immagini, può richiederne copia oppure esercitare il diritto di accesso ai propri dati (fermo restando che dovranno essere opportunamente oscurati o resi comunque non riconoscibili i passeggeri presenti a bordo del veicolo);

Per quanto riguarda gli apparati di videosorveglianza modulare riposizionabili, questi vengono installati secondo necessità, nei luoghi teatro di illeciti penali; possono essere utilizzati per accertare illeciti amministrativi, solo qualora non siano altrimenti accertabili con le ordinarie metodologie di indagine e non si possa fare ricorso a strumenti e sistemi di controllo alternativi e nel rispetto del principio di minimizzazione.
Le immagini sono visualizzate in tempo reale su monitor, direttamente presso il Comando della Polizia Metropolitana, da personale autorizzato e vengono salvate su un server comunale presente presso la sala di controllo. Il sistema è a circuito chiuso, senza possibilità di accesso da remoto.
Possono essere autorizzati all'accesso alla sala di controllo solo incaricati di servizi rientranti nei compiti istituzionali dell'Ente o Organismo di appartenenza e per scopi connessi alle finalità individuate nell'apposito regolamento comunale, nonché il personale addetto alla manutenzione degli impianti ed alla pulizia dei locali, preventivamente individuato dal titolare o dal designato al trattamento.
L'accesso alla sala, da parte di soggetti diversi da quelli indicati sopra è subordinato al rilascio, da parte del Titolare, di un'autorizzazione scritta, motivata e corredata da specifiche indicazioni in ordine ai tempi ed alle modalità dell'accesso. L'accesso avviene in presenza di incaricati della Città Metropolitana di Palermo.
Gli autorizzati al trattamento e i preposti sono gli unici dotati di proprie credenziali di autenticazione di accesso al sistema. Il sistema dovrà essere fornito di "log" di accesso. Infatti, l'accesso ai sistemi che gestiscono i dati oggetto dello specifico trattamento, può essere effettuato esclusivamente da operatori muniti di credenziali di accesso valide e strettamente personali, rilasciate su disposizione del designato del trattamento come individuato.
L'accesso ai sistemi di registrazione prevede l'adozione di sistemi idonei alla registrazione degli accessi logici degli incaricati e delle operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei designati da parte del titolare, comunque non inferiore a sei mesi.
L'accesso alla sala operativa, collocata presso gli uffici della P. M., è protetto da sistemi di sicurezza fisici quali: sistema di allarme e armadio rack protetto da chiave.

Il personale autorizzato della sala controllo del Comando di Polizia Locale potrà visionarle esclusivamente per il perseguimento dei fini istituzionali:
a) sulla base di denunce di atti criminosi da parte dei cittadini, per il successivo inoltro delle eventuali fonti di

prova all'autorità giudiziaria;
b) sulla base di segnalazioni relative ad atti criminosi accertate direttamente dagli organi di polizia in servizio sul territorio provinciale;
c) sulla base di atti criminosi che vengono rilevati direttamente dagli operatori di polizia nel visionare le immagini trasmesse in diretta dalle telecamere, nell'esercizio delle proprie funzioni;
d) sulla base di richieste specifiche per indagini da parte dell'autorità giudiziaria;
e) sulla base di ogni altra richiesta di specifici organi/autorità che siano espressamente autorizzati, secondo specifiche norme di legge.

Le immagini rilevanti ogni sorta di infrazione o reato vengono scaricate in locale attraverso il dispositivo di memoria di massa e messe a disposizione in caso di necessità agli operatori di giustizia.
Qualora la presa in carico delle immagini e delle videoriprese venga effettuata tramite riversamento dai supporti di memoria presenti negli strumenti di acquisizione, i file contenenti dati devono essere rimossi dai supporti una volta acquisiti i dati. In caso di dismissione di supporti di memorizzazione, questi devono essere resi inutilizzabili tramite danneggiamento fisico irreparabile, in modo che non sia non consentito in alcun modo il recupero dei dati trattati.

Le immagini videoregistrate sono conservate:
- per il periodo ordinariamente non superiore a 7 giorni successivi alla rilevazione, che possono essere estesi fino a 90 giorni tenuto conto delle esigenze specifiche e documentate di indagine e di prevenzione dei reati, con particolare su esplicita richiesta dell'Autorità. L'estensione dei tempi di conservazione, fino a 90 giorni, devono essere sostenute da specifiche ed evidenti esigenze investigative e di polizia giudiziaria nonché specifiche richieste da parte dell'Autorità prefettizia e giudiziaria, tenuto conto di eventuali ulteriori necessità di conservazione in caso di ricorsi;
- per le telecamere a tutela del solo patrimonio provinciale per un periodo non superiore a 48 ore successive alla rilevazione, fatte salve speciali e diverse esigenze debitamente documentate.

Al termine del periodo stabilito il sistema di videoregistrazione provvede in automatico alla loro cancellazione - ove tecnicamente possibile - mediante sovra-registrazione, con modalità tali da rendere non più utilizzabili i dati cancellati.

In caso di esercizio dei diritti da parte dell'interessato, svolte secondo le procedure come dettagliate nei paragrafi a seguire, in ogni caso di accoglimento delle richieste, l'addetto incaricato dal Titolare del trattamento dei dati deve lasciare traccia delle operazioni eseguite al fine di acquisire i filmati e riversarli su supporto digitale, in modo da garantire la genuinità dei dati stessi.

2.2.3 **Quali sono le risorse di supporto ai dati?**
Persone:
- Sindaco;
- Personale interno formato ed autorizzato (Comandante Dott. Giuseppe La Manno, Vice Comandante Comm. Capo Giovanna Costa, Isp. Capo Michele Megna, Ag. Luca Distefano, Ag. Autore Renato, Ag. Antonino Parisi).

Hardware – Software:
- Infrastruttura HW e SW come da scheda tecnica allegata.

3. **Principi Fondamentali**

3.1 **Proporzionalità e necessità**

3.1.1 **Gli scopi del trattamento sono specifici, espliciti e legittimi?**
Il trattamento dei dati personali, acquisiti mediante l'impianto di VDS gestito dall'Ente e collegato alla centrale di controllo ubicata presso gli Uffici dell'Ente, si svolge nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.
L'utilizzo dell'impianto comporta esclusivamente il trattamento di dati personali rilevati mediante le riprese

video e foto che, in relazione ai luoghi di installazione delle telecamere, interessano i soggetti ed i mezzi di trasporto che transitano nell'area oggetto di sorveglianza.

3.1.2 **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) del Regolamento UE e Direttiva UE 680/2016, nonché dalla necessità di eseguire un compito di un'autorità competente per le finalità di prevenzione, accertamento e prevenzione dei reati, salvaguardia e prevenzione contro minacce alla sicurezza pubblica (art. 5 D. Lgs. 51/2018).
In ossequio al disposto di cui sopra, il trattamento dati è effettuato dalla Città Metropolitana di Palermo esclusivamente per lo svolgimento delle funzioni istituzionali.

3.1.3 **I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?**
In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. minimizzazione) di cui all'art. 5 par. 1, lett. c) del GDPR, il sistema di videosorveglianza, i sistemi informativi ed i programmi informatici utilizzati, sono configurati per ridurre al minimo l'utilizzazione di dati personali e identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. Pertanto, deve essere escluso ogni uso superfluo, nonché evitati eccessi e ridondanze nei sistemi di VDS. Inoltre, qualora non sia necessario individuare le persone, i sistemi devono essere configurati, già in origine, in modo da poter impiegare solo i dati anonimi, con riprese di insieme e, il software utilizzato deve preventivamente essere impostato per cancellare periodicamente ed autonomamente i dati registrati.
Nel rispetto del principio di non eccedenza i sistemi sono configurati in modo da raccogliere esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo di visuale delle riprese ed evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari rilevanti. La localizzazione delle telecamere e le modalità di ripresa saranno quindi stabilite in modo conseguente.
Nel rispetto del principio di necessità, in ambito pubblico è bene precisare che la rilevazione dei dati non potrà essere estesa ad ambiti, aree o attività che non presentino rischi concreti o non caratterizzate da esigenze di dissuasione e deterrenza. Allo stesso modo, laddove la finalità venga individuata nella protezione del bene o dei beni a fronte di atti di vandalismo, il posizionamento di sistemi di videosorveglianza potrà essere considerato lecito solo laddove sia stata valutata l'inefficacia di misure alternative e meno impattanti, quali ad esempio controlli da parte del personale di sicurezza, sistemi di allarme, misure di sicurezza apposte agli ingressi o autorizzazioni all'accesso fisico degli edifici.
In attuazione del principio di proporzionalità, nella commisurazione tra la necessità del sistema di videosorveglianza ed il grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra un'effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo qualora altre misure siano state preventivamente ponderatamente valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti (es. controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi). In ogni caso l'Ente garantisce che il trattamento deve essere effettuato con modalità tali da limitare l'angolo di visuale all'area effettivamente da controllare e/o proteggere.

3.1.4 **I dati sono esatti e aggiornati?**
I dati vengono aggiornati periodicamente, almeno su base annuale e incrociati con le banche dati nazionali.

3.1.5 **Qual è il periodo di conservazione dei dati?**
I dati personali oggetto di trattamento sono conservati presso la sala di controllo, alla quale può accedere il solo personale autorizzato secondo istruzioni che devono essere impartite in forma scritta dal designato del trattamento dei dati.
I dati personali registrati mediante l'utilizzo dell'impianto di VDS di cui alla presente analisi, sono conservati per un periodo di tempo non superiore a sette giorni dalla data della rilevazione. Decorso tale periodo, i dati registrati sono sovrascritti automaticamente oppure tramite accesso manuale con password da parte dei

soggetti autorizzati. Più precisamente, le immagini videoregistrate sono conservate:

- per il periodo ordinariamente non superiore a 7 giorni successivi alla rilevazione, che possono essere estesi fino a 90 giorni tenuto conto delle esigenze specifiche e documentate di indagine e di prevenzione dei reati. L'estensione dei tempi di conservazione, fino a 90 giorni, devono essere sostenute da specifiche ed evidenti esigenze investigative e di polizia giudiziaria nonché specifiche richieste da parte dell'Autorità prefettizia e giudiziaria, tenuto conto di eventuali ulteriori necessità di conservazione in caso di ricorsi;
- per le telecamere a tutela del proprio patrimonio (o per altre telecamere non collegate alla centrale operativa del Corpo di Polizia Locale) per un periodo non superiore a 48 ore successive alla rilevazione, fatte salve speciali e diverse esigenze debitamente documentate.

I dati personali registrati mediante l'utilizzo dell'impianto di VDS di cui alla presente analisi, sono conservati per un periodo di tempo non superiore a sette giorni dalla data della rilevazione. Decorso tale periodo, i dati registrati sono sovrascritti automaticamente oppure tramite accesso manuale con password da parte dei soggetti autorizzati, il periodo di conservazione può essere esteso fino a 90 giorni tenuto conto delle esigenze specifiche e documentate di indagine e di prevenzione dei reati. L'estensione dei tempi di conservazione, fino a 90 giorni, deve essere sostenuta da specifiche ed evidenti esigenze investigative e di polizia giudiziaria nonché specifiche richieste da parte dell'Autorità prefettizia e giudiziaria, tenuto conto di
eventuali ulteriori necessità di conservazione in caso di ricorsi.
Gli strumenti e i supporti elettronici utilizzati sono dotati del sistema di protezione informatica quale log-in e password per accesso alle apparecchiature.

3.2 **Misure a tutela dei diritti degli interessati**

3.2.1 **Come sono informati del trattamento gli interessati?**

Gli interessati sono informati mediante:

- pubblicazione del regolamento elaborato e adottato dall'Ente, comprensivo dei dettagli e di altra documentazione relativa alle zone video-sorvegliate e foto-sorvegliate, sul sito web istituzionale dell'Ente;
- installazione di apposita segnaletica permanente, contenente l'informativa breve, nelle aree in cui sono concretamente posizionate le telecamere;
- informativa completa, contenente gli elementi di cui agli articoli 12-13-14 del GDPR, disponibile agevolmente e senza oneri per gli interessati, sul sito web e nei locali dell'Ente, in modo da essere resa facilmente accessibile anche con strumenti informatici o telematici.

La segnaletica viene collocata prima del raggio di azione di ogni telecamera, o nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; la stessa è predisposta in modo da avere un posizionamento chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di VDS sia eventualmente attivo in orario notturno. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, sono installati più cartelli informativi.
L'Ente, in qualità di Titolare del trattamento, provvede ad informare la comunità cittadina dell'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di VDS, dell'eventuale incremento dimensionale dell'impianto stesso e successiva cessazione per qualsiasi causa del trattamento medesimo e si obbliga ad affiggere la richiamata segnaletica permanente, nelle strade e nelle piazze in cui sono posizionate le telecamere.
L'informativa di cui sopra non è dovuta nel caso di utilizzo di telecamere a scopo investigativo a tutela dell'ordine e sicurezza pubblica, prevenzione, accertamento o repressione di reati.

3.2.2 **Ove applicabile: come si ottiene il consenso degli interessati?**

Considerato che il Titolare del trattamento è una pubblica amministrazione che eroga servizi pubblici legalmente attribuiti, non è tenuto all'acquisizione del consenso al trattamento dei dati; nel caso in cui questo sia dovuto, viene acquisito per iscritto.

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

Gli interessati potranno esercitare i propri diritti rivolgendosi al Titolare del trattamento secondo le modalità da lui stesso individuate e comunicate agli interessati attraverso l'informativa predisposta.
Il Titolare, qualora lo ritenga necessario, richiederà l'eventuale intervento del Responsabile del trattamento; lo stesso avverrà come indicato nel contratto di nomina, ad es. fornendo supporto nell'estrazione dei dati in formato strutturato.
In relazione al trattamento dei dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli articoli 15 e ss. Del 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 del 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 del GDPR.

L'istanza per l'esercizio dei diritti, da parte dell'interessato, è presentata al DPO dell'Ente, ai sensi dell'art. 38 par.4 del GDPR ovvero al Responsabile del trattamento eventualmente individuato e può essere presentata mediante lettera raccomandata inoltrata all'indirizzo del Titolare ovvero posta certificata: polizia@cert.cittametropolitana.pa.it

In caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare:

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

Il Responsabile individuato, appositamente autorizzato al trattamento dei dati personali, avrà cura di accertare l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; in caso di accertamento positivo, fisserà il giorno, l'ora ed il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano.
Qualora l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, ai sensi dell'art. 15 par. 3 del GDPR, 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 (art. 15 par. 4 del GDPR).

I diritti come sopra esplicitati, riferiti ai dati personali concernenti persone decedute, possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato per ragioni familiari meritevoli di protezione.
Nell'esercizio dei diritti, l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti associazioni od organismi. L'interessato potrà altresì farsi assistere da persona di fiducia.
Qualora non sia possibile identificare l'interessato (o in caso di richieste eccessive o manifestamente infondate) il designato – previa adeguata motivazione ed entro i termini di 7 giorni dalla richiesta – informerà l'interessato dell'impossibilità di dare seguito alla richiesta.
In caso di esito negativo all'istanza dell'interessato, quest'ultimo potrà rivolgersi al Garante della protezione dei dati personali per il reclamo, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Al fine di:

- non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;
- non compromettere l'attività di prevenzione, indagine, accertamento e perseguimento di reati o

l'esecuzione di sanzioni penali;
- proteggere la sicurezza pubblica;
- proteggere la sicurezza nazionale;

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

3.2.4 **Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?**
In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo.
Per esercitare il diritto alla cancellazione, se possibile in ragione dell'obbligo dell'Ente di conservazione delle informazioni, gli interessati possono contattare direttamente il Titolare del trattamento ovvero il DPO ovvero il responsabile esterno eventualmente individuato, recandosi direttamente presso l'Ente, mediante invio di raccomandata ovvero di posta certificata, ai canali di contatto indicati dal Titolare all'interno dell'informativa.

3.2.5 Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?
Per esercitare il diritto di limitazione o opposizione, se possibile in ragione degli obblighi in capo all'Ente, gli interessati possono contattare direttamente il Titolare del trattamento ovvero il DPO ovvero il responsabile esterno eventualmente individuato, recandosi direttamente presso l'Ente, mediante invio di raccomandata ovvero di posta certificata, ai canali di contatto indicati dal Titolare all'interno dell'informativa.

3.2.6 **Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?**
Il rapporto di responsabilità tra il Titolare ed il responsabile esterno eventualmente individuato è definito e disciplinato da un contratto di appalto dei relativi servizi ovvero mediante specifica comunicazione.
Inoltre, gli obblighi derivanti dal trattamento incidentale dei dati trattati mediante l'utilizzo dell'impianto, sono disciplinati in apposito allegato per la nomina conforme alle disposizioni previste dall'art. 28 Reg. UE 2016/679.

3.2.7 **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 dello spazio SEE.

4. **Rischi**

4.1 **Misure esistenti o pianificate**

4.1.1 **Anonimizzazione**
I dati particolari, i c.d. sensibili, eventualmente rilevati vengono trattati in maniera riservata unicamente dal personale strettamente necessario e a questo autorizzato. I dati oggetto di trattamento vengono resi sempre anonimi.

4.1.2 **Controllo degli accessi logici e tracciabilità**
- Individuazione di postazione informatica dedicata dotata di username e password personale di accesso per ogni operatore (unico e tracciabile);
- il software prevede la registrazione e conseguente tracciabilità degli accessi logici e delle operazioni effettuate dagli autorizzati al trattamento dei dati.
- Assegnazione, ad uso esclusivo, di una o più credenziali di autenticazione agli operatori;
- Assegnazione di parole chiave che rispondono ai requisiti di sicurezza e che sono modificate ciclicamente;
- Aggiornamento periodico delle credenziali di autenticazione;
- Attivazione di uno screensaver automatico, dopo pochi minuti di non utilizzo, con inserimento

password per la prosecuzione del lavoro;
- Disattivazione delle credenziali di autenticazione nel caso di inutilizzo perdurato ovvero in caso di perdita di qualità dell'incaricato.
-

4.1.3 **Sicurezza dei documenti cartacei**
I documenti cartacei vengono conservati dai dipendenti dell'ufficio in conformità a quanto previsto dalle procedure aziendali di riferimento, in maniera tale da garantire la riservatezza e la non visibilità a terzi non autorizzati.

4.1.4 **Protezione contro il malware e vulnerabilità**
- Installazione e aggiornamento periodico di sistemi antivirus e antimalware;
- Aggiornamento costante dei software utilizzati;
- Utilizzo di un sistema Firewall sugli elaboratori ed aggiornamento periodico;
- Aggiornamento periodico dei programmi antivirus;
- Utilizzo di filtro anti-spam ed aggiornamento periodico;
- Protezione della posta elettronica con disposizione di verifica della provenienza delle e-mail e di non esecuzione dei file allegati ai messaggi senza preventiva scansione antivirus;
- Disposizione di utilizzo della casella di posta elettronica dell'ufficio come strumento di lavoro e dunque esclusivamente per esigenze lavorative;
- Controllo degli accessi a siti internet non sicuri;
- Divieto di scaricare software e di installare programmi da siti poco attendibili o non ufficiali;
- Disposizione di tenere sempre attiva l'opzione del browser "richiedi conferma" per l'installazione e il download di oggetti sulla propria macchina;
- Reinstallazione dei programmi danneggiati o distrutti.

4.1.5 **Crittografia**
La crittografia avanzata è applicata alle informazioni che transito dalle videocamere al server presente presso gli uffici della Polizia Metropolitana.

4.1.6 **Minimizzazione dei dati**
Vengono raccolti e conservati unicamente i dati necessari e non sono richiesti dati eccedenti le finalità individuate.

4.1.7 **Archiviazione e Backup**
L'archiviazione dei dati personali trattati avviene in conformità alle procedure di riferimento della Cittaà Metropolitana di Palermo, garantendo la riservatezza e l'integrità dei dati personali trattati. Ogni dipendente, autorizzato al trattamento, è tenuto ad archiviare i documenti cartacei negli appositi raccoglitori e a conservare/salvare i documenti digitali sulle apposite apparecchiature in uso, protette da password di accesso.
Inoltre, le immagini rilevate dal sistema di VDS non sono oggetto di back-up.
Il sistema di back-up è presente soltanto sui client delle immagini esportate.

4.1.8 **Controllo degli accessi fisici**
- Gli accessi fisici agli uffici sono limitati e controllati;
- Chiavi dei locali custodite dal solo personale della Polizia Metropolitana;
- Serratura porta esterna e porta interna della Sala di Controllo;

4.1.9 **Sicurezza dell'hardware e prevenzione delle fonti di rischio**
- Manutenzione programmata degli strumenti;
- Distruzione di tutti i supporti removibili non utilizzati;
- Estintori e loro revisione periodica;
- Accordo di assistenza continuativa con ditta di sicurezza;
- Manutenzione costante impianti e apparecchiature elettriche ed elettroniche;
- Monitoraggio e impegno della direzione nel controllo delle regole in materia di salute e sicurezza sui luoghi di lavoro.

4.1.10 **Manutenzione**

- Manutenzione programmata degli strumenti;
- Manutenzione costante impianti e apparecchiature elettriche ed elettroniche;
- Controllo sull'operato degli addetti alla manutenzione.

4.1.11 **Sicurezza dei canali informatici**

- Sicurezza dell'infrastruttura di sistema;
- La crittografia avanzata è applicata alle informazioni che transito dalle videocamere al server presente presso gli uffici della Polizia Metropolitana;
- Controlli periodici sul sistema di protezione nella trasmissione dei dati;
- Installazione ed aggiornamento periodico del Firewall.

4.1.12 **Politica di tutela della privacy**

Relativamente alla propria organizzazione, l'Ente, partendo dall'analisi del proprio organigramma, ha ritenuto necessario predisporre una struttura interna per la gestione della privacy, con identificazione dei ruoli, distribuzione dei compiti e delle responsabilità. All'interno della struttura, il trattamento viene effettuato solo da soggetti che hanno ricevuto un formale incarico mediante designazione per iscritto di ogni singolo incaricato (o per categorie omogenee di trattamento). Le responsabilità sono dettagliate per iscritto nella lettera di nomina.

Inoltre, sono adottate misure quali:

- Formazione sugli aspetti principali della Regolamento Europeo al momento dell'ingresso in servizio;
- Formazione periodica e in occasione di cambiamenti di mansioni o di introduzione di nuovi strumenti per il trattamento dei dati e la loro protezione;
- Istruzioni agli incaricati, finalizzate al controllo e alla custodia dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento senza l'ausilio di strumenti elettronici;
- Istruzioni in merito alla protezione dello strumento elettronico in caso di assenza temporanea durate le sessioni di lavoro;
- Istruzioni in merito alla segretezza e alla custodia delle credenziali di autenticazione;
- Istruzioni in merito all'accesso agli archivi digitali;
- Istruzioni organizzative e tecniche per la custodia dei supporti removibili su cui sono memorizzati i dati;
- Individuazione del profilo di autorizzazione anteriormente all'inizio del trattamento;
- Aggiornamento periodico o al verificarsi di eventuali modifiche della lista degli incaricati e dei profili di autorizzazione;
- Procedure di verifica sull'operato degli incaricati;
- Definizione di responsabilità e sanzioni disciplinari;
- Definizione delle procedure di convalida delle operazioni a rischio nell'ambito dell'incarico assegnato;
- Controllo degli accessi ai dati e programmi;
- Controllo sull'operato degli addetti alla manutenzione;
- Definizione di procedure per le copie di sicurezza, la loro custodia e il ripristino dei dati;
- Monitoraggio continuo delle sessioni di lavoro;
- Formazione professionale.

4.1.13 **Misure di sicurezza specifiche**

Ai sensi di quanto previsto dall'art. 24 del GDPR, i dati personali acquisiti mediante l'impiego dell'impianto VDS sono protetti da misure di sicurezza tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato e trattamento non consentito o non conforme alle finalità di qui al par. 2.1.1. del presente documento.

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

- vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento ("controllo dell'accesso alle attrezzature");
- impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate ("controllo dei supporti di dati");

- impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione ("controllo della conservazione");
- impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati ("controllo dell'Utente") e garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali ci si riferisce la loro autorizzazione d'accesso ("controllo dell'accesso ai dati");
- garantire la possibilità di verificare e accertare gli organismi ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione dei dati ("controllo della trasmissione");
- garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il moment della loro introduzione e la persona che l'ha effettuata ("controllo dell'introduzione");
- impedire che i dati personali possano essere letti, copiati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati ("controllo del trasporto");
- garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati ("recupero");
- garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati ("affidabilità") e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema ("integrità").

4.2 **Accesso illegittimo ai dati**

4.2.1 **Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?**
Diffusione non autorizzata, intercettazione di informazioni in rete, pregiudizio alla reputazione.

4.2.2 **Quali sono le principali minacce che potrebbero concretizzare il rischio?**
Abuso di privilegi, accesso non autorizzato ai sistemi aziendali per operazioni non consentite/non autorizzate, furto nei locali aziendali, vulnerabilità degli assets, azione di virus informatici o di programmi suscettibili di recare danno, distruzione totale o parziale e/o diffusione non autorizzata e/o inibizione dell'accesso ai dati, spamming o tecniche di sabotaggio.

4.2.3 **Quali sono le fonti di rischio?**
Fonti di rischio interne ed esterne anche non umane come attacchi informatici, Virus e Malware.

4.2.4 **Quali misure fra quelle individuate contribuiscono a mitigare il rischio?**
Anonimizzazione, Controllo degli accessi logici e tracciabilità; Sicurezza dei documenti cartacei; Protezione contro i malware e vulnerabilità; Crittografia; Minimizzazione dei dati; Controllo degli accessi fisici; Manutenzione; Sicurezza dei canali informatici, Politica di tutela della privacy; Misure di sicurezza specifiche.

4.2.5 **Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?**
In considerazione dei dati oggetto di trattamento, il rischio individuato è da considerarsi Basso.

4.2.6 **Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?**
Limitata. Le misure individuate, pianificate ed adottate contribuiscono a mitigare i rischi individuati.

4.3 **Modifiche indesiderate dei dati**

4.3.1 **Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?**
Alterazione dei dati, negazione dell'accesso a servizi, pregiudizio alla reputazione.

4.3.2 **Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?**
Accesso ai dati da parte di soggetti non autorizzati e/o accesso ai dati per trattamenti non consentiti, sottrazione di credenziali di autenticazione, accesso ai dati da parte di soggetti in orari non consentiti, errore

umano, carenza di consapevolezza, disattenzione, incuria o indisponibilità, comportamenti contrari ai principi di sicurezza e protezione dei dati, comportamenti sleali o fraudolenti, operazioni accidentali non consentite e/o contrarie ai principi di sicurezza e protezione dei dati.

4.3.3 **Quali sono le fonti di rischio?**
Utenti e esterni all'organizzazione, attacchi informatici.

4.3.4 **Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?**
Controllo degli accessi logici e tracciabilità; Protezione contro i malware e vulnerabilità; Crittografia; Minimizzazione dei dati; Archiviazione e back-up; Controllo degli accessi fisici; Sicurezza dei canali informatici, Politica di tutela della privacy; Misure di sicurezza specifiche.

4.3.5 **Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?**
In considerazione dei dati oggetto di trattamento, il rischio individuato è da considerarsi Basso.

4.3.6 **Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?**
Limitata. Le misure individuate, pianificate ed adottate contribuiscono a mitigare i rischi individuati.

4.4 **Perdita di dati**

4.4.1 **Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?**
Indisponibilità dei dati, danno reputazionale.

4.4.2 **Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?**
Errori umani nella gestione della sicurezza fisica, eventi distruttivi, naturali o artificiali, nonché dolosi, accidentali o dovuti ad incuria, malfunzionamento, guasti, eventi naturali, alterazioni delle trasmissioni, indisponibilità o degrado degli strumenti, guasto ai sistemi complementari, sottrazione di strumenti contenenti dati, comportamenti sleali o fraudolenti, errore materiale, sottrazione di credenziali di autenticazione, azione di virus informatici o di programmi suscettibili di recare danno.

4.4.3 **Quali sono le fonti di rischio?**
Utenti e esterni all'organizzazione, attacchi informatici, eventi calamitosi, malfunzionamenti.

4.4.4 **Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?**
Controllo degli accessi logici e tracciabilità; Protezione contro i malware e vulnerabilità; Crittografia; Minimizzazione dei dati; Archiviazione e back-up; Controllo degli accessi fisici; Sicurezza dell'hardware e prevenzione delle fonti di rischio; Sicurezza dei canali informatici, Politica di tutela della privacy; Misure di sicurezza specifiche.

4.4.5 **Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?**
In considerazione dei dati oggetto di trattamento, il rischio individuato è da considerarsi Basso

4.4.6 **Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?**
Limitata. Le misure individuate, pianificate ed adottate contribuiscono a mitigare i rischi individuati.

Palermo, lì 10.05.2024