Comune di Andria

VALUTAZIONE D'IMPATTO
SULLA PROTEZIONE DEI DATI PERSONALI

Autore:
dott. Francesco Capogna
Revisore:
avv. Paolo Somma
Validatore:
avv. Giovanna Bruno

Richiesta del parere degli interessati:
non è stato richiesto il parere degli interessati in quanto la base giuridica del trattamento, ai sensi dell'art. 6, comma 1, lettera e) del Reg. UE 2016/679, è rappresentata dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare.

Titolo: DPIA per il sistema di videosorveglianza

Panoramica del trattamento

Quale è il trattamento in considerazione?

Questa DPIA è atta alla valutazione dell'impatto connesso all'uso di nuove tecnologie al fine di rilevare filmati/immagini mediante sistemi integrati di videosorveglianza per la sicurezza urbana, per la lettura delle targhe dei veicoli e per l'emergenza videocamere nel territorio del comune di Andria.

Le operazioni di trattamento dati che il comune di Andria esegue sul territorio attraverso i diversi sistemi di videosorveglianza, perseguono le seguenti finalità:

a) tutela della sicurezza urbana, intesa, secondo la definizione del Decreto del Ministero dell'Interno del 5 agosto 2008, riformulata dall'art. 4 del D.L. 20 febbraio 2017, n. 14, convertito, con modificazioni, nella Legge 18 aprile 2017, n. 48, come il bene pubblico che afferisce alla vivibilità e al decoro delle città da perseguire anche attraverso interventi di riqualificazione e recupero delle aree o dei siti più degradati, l'eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità, in particolare di tipo predatorio, da potenziare con accordi o patti locali ispirati ad una logica di gestione consensuale ed integrata della sicurezza;

b) attività di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, rafforzare la cooperazione giudiziaria in materia penale e di polizia nonché a svolgere attività di prevenzione, accertamento di illeciti amministrativi in particolare modo in materia ambientale;

c) rilevazione e controllo targhe dei veicoli in transito attraverso telecamere in grado di leggere le targhe e trasformarle in una stringa alfanumerica, al fine di poter disporre di utili elementi per l'avvio di eventuali accertamenti connessi con la sicurezza urbana;

d) ricostruzione della dinamica degli incidenti stradali ed eventuale accertamento di violazioni alle norme sulla circolazione stradale attraverso le immagini rilevate dagli impianti di videosorveglianza, anche del traffico urbano, qualora non siano l'unico strumento di accertamento dei fatti, ai sensi dell'art. 13 della Legge 24 novembre 1981, n. 689, rientrando dette immagini tra gli atti di accertamento idonei a ricostruire episodi, situazioni e comportamenti individuali, anche nell'ambito del procedimento sanzionatorio;

e) tutela delle persone attraverso sistemi attivabili per l'emergenza;

L'attività di videosorveglianza eseguita dal comune di Andria è esercitata per lo svolgimento di funzioni e poteri pubblici ed il raggiungimento delle finalità istituzionali

come sopra rappresentate e precisate, consentendo quindi di garantire ai cittadini il rispetto delle regole civili, penali ed amministrative nonché di civile educazione che consentono la normale convivenza e coabitazione nella condivisione di uno spirito di reciproco rispetto e di rispetto delle Istituzioni e delle loro funzioni.

I sistemi di videosorveglianza utilizzati dal comune di Andria sono, infatti, proporzionati ed efficaci rispetto alle finalità prefissate e sono tali da non comportare rischi ultronei rispetto a quelli inseriti in un contesto di normale funzionalità dei sistemi tecnologici delle tipologie in uso, avuto anche riguardo alla utilizzazione dei medesimi strumenti anche in altri contesti urbani, considerazione questa che consente di accrescere la fiducia e la credibilità degli strumenti stessi.

Gli strumenti tecnologici in uso sono i seguenti:

1) sistema di videosorveglianza con telecamere fisse posizionate agli accessi all'area urbana e nel territorio, finalizzata al presidio del territorio stesso nonché alla vigilanza del traffico veicolare e pedonale, anche con dispositivi idonei alla lettura targhe;

2) sistema di videosorveglianza ambientale con "fototrappole" amovibili posizionate in prossimità dei luoghi destinati al gettito di rifiuti ovvero in aree presso le quali è stato rilevato ovvero potrebbe verificarsi il gettito irregolare e abusivo di rifiuti;

3) "dash cam" posizionate all'interno dei veicoli di servizio della Polizia Locale;

4) "body cam" sui giubbotti di servizio del personale della Polizia Locale.

Quali sono le responsabilità connesse al trattamento?

La complessità delle azioni e dei possibili risvolti in termini di violazione della privacy implica una collaborazione fattiva tra le varie parti in causa. Queste sono, in particolare:

1. il **Titolare del trattamento**: il Comune di Andria, rappresentato ai fini previsti dal GDPR dal Sindaco *pro tempore*, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare").

2. Il Titolare è responsabile dell'osservanza dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

3. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al GDPR. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare

l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 GDPR nonché le comunicazioni e le informazioni occorrenti per il loro esercizio. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di PEG, previa apposita analisi preventiva della situazione in essere, tenuto conto dei corsi d'attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

4. Il Titolare adotta misure appropriate per fornire all'interessato:

a) le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 GDPR, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.

5. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, GDPR, considerando la natura, l'oggetto, il contesto e le finalità del medesimo trattamento.

6. Il Titolare, inoltre, provvede a:

a) designare i "Delegati al trattamento" nelle figure dei Dirigenti/Responsabili P.O. e dei Funzionari delle singole strutture in cui si articola l'organizzazione comunale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza;

b) nominare il Responsabile della protezione dei dati;

c) nominare quale Responsabile (esterno) del trattamento i soggetti pubblici e privati affidatari di attività e servizi per conto dell'Amministrazione comunale anche relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali.

7. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali o regionali, allorché due o più Titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, essi sono contitolari del trattamento ex art. 26 GDPR. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema

di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del GDPR, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

8. Il Comune favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Delegato (interno) al trattamento:

1. In relazione alle dimensioni organizzative del Comune, sono designati "Delegati al trattamento" i Dirigenti dei settori in cui si articola l'organizzazione comunale, in quanto in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative volte a garantire che i trattamenti siano effettuati in conformità al GDPR.

2. I "Delegati al trattamento" provvedono, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti loro affidati dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvedono:

- a collaborare alla gestione del registro delle attività di trattamento del Comune;
- all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- a collaborare alle richieste di accesso, di limitazione ed opposizione degli interessati relative a trattamenti di dati personali;
- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
- ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

3. I "Delegati al trattamento", sono designati, mediante decreto di incarico del Sindaco, nel quale sono tassativamente disciplinati:
- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
- il tipo di dati personali oggetto di trattamento e le categorie di interessati; - gli obblighi ed i diritti del Titolare del trattamento.
4. I "Delegati al trattamento", possono altresì designare altri soggetti "Incaricati al trattamento dei dati personali", identificandoli nei Titolari di P.O., nei Responsabili di Servizio e nei collaboratori, ciascuno per il proprio ambito operativo.

Responsabili (esterni) del trattamento:
1. I Responsabili esterni del trattamento sono le persone fisiche, giuridiche, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo esterno all'Amministrazione comunale che possono essere nominati - dai "Delegati al trattamento" e previa autorizzazione scritta da parte del Titolare - su un determinato trattamento attenendosi, nelle operazioni svolte, alle istruzioni ricevute.
2. Detti soggetti, in qualità di Responsabili esterni del trattamento, devono fornire le garanzie di cui al precedente art. 3 attraverso la stipulazione di atti/contratti in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del Responsabile del trattamento e le modalità di trattamento.
3. Gli atti di cui innanzi devono in particolare contenere quanto previsto dall'art. 28, p. 3, GDPR; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

Ci sono standard applicabili al trattamento?

Attualmente non sono stati rinvenuti standard, certificazioni o codici di condotta applicabili al caso in esame.

Valutazione : Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati trattati consistono in immagini e video - che ritraggono persone fisiche e/o numeri di targa di autoveicoli - registrati sul piano operativo; la registrazione è attiva sulle 24 ore e le immagini registrate vengono salvate solamente dal personale incaricato qualora vi sia una situazione di particolare criticità che necessita la documentazione video degli eventi.

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

Per ciclo di vita del dato s'intende l'insieme delle fasi in cui un dato si può trovare durante la sua esistenza ovverosia:

a) la Raccolta: il ciclo di vita inizia con la raccolta delle informazioni. I dati possono entrare nel perimetro comunale;

b) il salvataggio: una volta che i dati sono entrati all'interno del perimetro comunale dovranno essere memorizzati in appositi luoghi fisici e/o virtuali in modo tale che poi possano essere utilizzati;

c) l'a**nalisi:** in questa fase si analizzano gli esiti dell'attività di raccolta per determinare la qualità dei dati da utilizzare. Vi è quindi un confronto tra *output desiderato* e *output effettivo* per, eventualmente, pianificare migliorie e attività correttive che abbiano impatti sulle fasi precedenti;

d) il filtraggio dei dati: in seguito agli esiti dei risultati della fase c), i dati vengono filtrati e modificati in modo da rispecchiare gli *output desiderati;*

e) l'utilizzo: in questa fase i dati vengono effettivamente utilizzati per le anzidette finalità;

f) l'archiviazione: in questa fase i dati vengono memorizzati in attesa di essere dismessi e/o riutilizzati;

g) la cancellazione o anonimizzazione: in questa fase il periodo di conservazione è ormai scaduto e quindi: o si cancella il dato personale, oppure lo si rende anonimo.

l trattamento dei dati personali, dunque, è effettuato a seguito dell'attivazione di tutti gli impianti/sistemi/presidi di videosorveglianza installati sul territorio cittadino.

La disponibilità tempestiva di immagini presso la sala operativa della Polizia Locale costituisce uno strumento di prevenzione e di razionalizzazione dell'azione delle pattuglie dislocate sul territorio comunale, anche in raccordo con altre Forze dell'Ordine.

Attraverso tali strumenti l'ente persegue l'intento di tutelare la popolazione ed il patrimonio comunale, garantendo quindi un elevato grado di sicurezza nei luoghi di

maggiore aggregazione, nelle zone più appartate, nei siti di interesse storico, artistico e culturale, negli edifici pubblici, nel centro storico, negli ambienti in prossimità delle scuole e nelle strade ad intenso traffico veicolare.
A tal fine il comune, previa intesa o su richiesta della autorità di Pubblica Sicurezza e degli organi di Polizia, dispone l'utilizzo del sistema di videosorveglianza in dotazione alla Polizia Locale, compresi i sistemi di lettura targhe e ZTL, ai fini di prevenzione e repressione di atti delittuosi anche nell'ambito del più ampio concetto di "sicurezza urbana", così individuata secondo il Decreto Ministro Interno 5 agosto 2008 decreto legge 20 febbraio 2017, n. 14 recante "Disposizioni urgenti in materia di sicurezza delle città" convertito con legge n. 48/2017.
Tutto il sistema di videosorveglianza comporterà esclusivamente il trattamento di dati personali rilevati mediante le riprese video e che, in relazione ai luoghi di installazione delle videocamere, interessano i soggetti ed i mezzi di trasporto che transiteranno nell'area interessata.
L'attività di videosorveglianza raccoglie esclusivamente i dati strettamente necessari per il raggiungimento delle finalità succitate, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando, quando non indispensabili, immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza.
L'uso dei dati personali nell'ambito di cui trattasi non necessita del consenso degli interessati in quanto viene effettuato per lo svolgimento di funzioni istituzionali che sono assoggettate alla normativa vigente in materia di "privacy" con un'apposita regolamentazione.

Quali sono le risorse di supporto ai dati?

Le immagini vengono gestite da un server NON collegato a internet e con rete separata rispetto ai servizi dell'ente.

Valutazione : Accettabile

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

La liceità è data dall'art. 6 par. 1 del GDPR, in quanto "il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" in particolare, con riferimento, al D.Lgs. 18 agosto 2000, n. 267, dal D.P.R. 24 luglio 1977, n. 616, concernente trasferimento e deleghe delle funzioni amministrative dello Stato, al D.Lgs. 31 marzo 1998, n. 112, relativo al conferimento di funzioni e compiti amministrativi dello Stato alle regioni ed agli enti locali, dal 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, dalla Legge 7 marzo 1986, n. 65 sull'ordinamento della Polizia Locale, dal Codice di procedura penale, allo Statuto e dai regolamenti comunali nonché ai sensi dell'art. 1 comma 2 del D.lgs. 18 maggio 2018, n. 51 "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché' alla libera circolazione di tali dati.

Il comune di Andria, attraverso il comando di Polizia Locale, effettua il trattamento di dati personali mediante impianti di videosorveglianza urbana, sia di osservazione che di contesto, ed altri sistemi di ripresa immagini di dati personali quali telecamere per lettura targhe, comprese quelle poste agli accessi della ZTL, fototrappole e Street control.

Possono altresì essere previsti altri sistemi di videosorveglianza.

In particolare, l'uso di tutti i sistemi e tipologie di videosorveglianza del territorio comunale è finalizzato a:

a) tutelare la sicurezza urbana di cui alla L. n. 38/2009 ss.mm.ii, Decreto del Ministro dell'Interno del 05 agosto 2008 e decreto legge 20 febbraio 2017, n. 14 nonché secondo le modalità previste dal capitolo n. 5.1 del Provvedimento del Garante Privacy in materia di videosorveglianza dd. 08/04/2010;

b) prevenire e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale secondo le modalità previste dal capitolo n. 5.1 del Provvedimento del Garante Privacy in materia di video-sorveglianza dd. 08/04/2010;

c) tutelare gli immobili di proprietà o in gestione dell'amministrazione comunale ed a prevenire eventuali atti di vandalismo o danneggiamento;

d) controllare determinate aree e/o specifici siti comunali potenzialmente esposti a rischi di vandalismo o danneggiamento quali, a mero titolo esemplificativo, parchi, impianti sportivi e strutture ludico-ricreative;
e) al monitoraggio del traffico veicolare, al fine di prevenire o gestire problematiche inerenti la viabilità;
f) tutelare in particolare coloro che più necessitano di attenzione: bambini, giovani e anziani, garantendo un adeguato grado di sicurezza nelle zone anche per le finalità previste dal “Decreto sicurezza" approvato con Decreto Legge 23 febbraio 2009, n. 11 e convertito nella legge 23 aprile 2009, n. 38 (atti sessuali con minorenni, violenza sessuale di gruppo e atti persecutori);
g) controllare ed accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose nonché per monitorare il rispetto delle disposizioni concernenti modalità, tipologia dei rifiuti scaricati ed orario di deposito dei rifiuti, la cui violazione è sanzionata amministrativamente (art. 13, legge 24 novembre 1981, n. 689), secondo le previsioni di cui al capitolo n. 5.2 del Provvedimento del Garante Privacy in materia di video-sorveglianza dd. 08/04/2010;
h) prevenire eventuali atti di vandalismo e/o danneggiamento ovvero spaccio di sostanze stupefacenti presso istituti scolastici in casi di stretta indispensabilità ed attivando gli impianti interni esclusivamente negli orari di chiusura degli Istituti secondo le modalità previste dal capitolo n. 4.3 del Provvedimento del Garante Privacy in materia di videosorveglianza dd. 08/04/2010.
i) rilevare violazioni al Codice della strada, contestati nella immediatezza, mediante l’uso di sistemi per il riconoscimento delle targhe veicolari;
l) tutelare l’ordine e la sicurezza pubblica e prevenire, accertare e reprimere i reati mediante il controllo dei veicoli in transito; le informazioni delle targhe inserite in “liste di controllo” particolari potranno essere condivise con le altre Forze dell’Ordine a seguito di specifico “Protocollo operativo” predisposto e sottoscritto dal Comitato provinciale per l’ordine e la sicurezza pubblica;
m) supportare operazioni di protezione civile.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica del trattamento eseguito con i sopracitati strumenti di videosorveglianza - ai sensi dell'articolo 6, comma 1, lettera e) del Regolamento (UE) 2016/679 - è rappresentata dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del Trattamento e il Comando di Polizia Locale del comune di Andria.

Valutazione : Accettabile

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

I dati personali vengono raccolti solo ed esclusivamente per:

a) tutela della sicurezza urbana, intesa, secondo la definizione del Decreto del Ministero dell'Interno del 5 agosto 2008, riformulata dall'art. 4 del D.L. 20 febbraio 2017, n. 14, convertito, con modificazioni, nella Legge 18 aprile 2017, n. 48, come il bene pubblico che afferisce alla vivibilità e al decoro delle città da perseguire anche attraverso interventi di riqualificazione e recupero delle aree o dei siti più degradati, l'eliminazione dei fattori di marginalità e di esclusione sociale, la prevenzione della criminalità, in particolare di tipo predatorio, da potenziare con accordi o patti locali ispirati ad una logica di gestione consensuale ed integrata della sicurezza;

b) svolgere attività di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, rafforzare la cooperazione giudiziaria in materia penale e di polizia nonché a svolgere attività di prevenzione, accertamento di illeciti amministrativi in particolare modo in materia ambientale;

c) rilevare e controllare le targhe dei veicoli in transito attraverso telecamere in grado di leggere le targhe e trasformarle in una stringa alfanumerica, al fine di poter disporre di utili elementi per l'avvio di eventuali accertamenti connessi con la sicurezza urbana;

d) ricostruzione della dinamica degli incidenti stradali ed eventuale accertamento di violazioni alle norme sulla circolazione stradale attraverso le immagini rilevate dagli impianti di videosorveglianza, anche del traffico urbano, qualora non siano l'unico strumento di accertamento dei fatti, ai sensi dell'art. 13 della Legge 24 novembre 1981, n. 689, rientrando dette immagini tra gli atti di accertamento idonei a ricostruire

episodi, situazioni e comportamenti individuali, anche nell'ambito del procedimento sanzionatorio.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

I dati sono esatti e aggiornati in quanto vengono rilevati con l'ausilio di strumentazione regolarmente manutenute e i software utilizzati vengono costantemente aggiornati.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

I dati raccolti dai vari dispositivi vengono trasmessi al Comando di Polizia Locale di Andria tramite un flusso di dati crittografati e memorizzati dal personale autorizzato dall'ente in una cartella di rete del server del Comune di Andria, idoneamente backuppata periodicamente, il cui accesso è limitato al personale preposto.
Se i dati oggetto di trattamento sono pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti vengono successivamente trattati, sono conservati per un periodo non superiore a 7 giorni successivi alla rilevazione. Detti termini potranno essere estesi per un ulteriore periodo di tempo strettamente necessario all'eventuale applicazione di una sanzione e/o alla definizione del possibile contenzioso e/o per eventuali esigenze derivanti da una specifica richiesta investigativa di Polizia Giudiziaria o dell'Autorità Giudiziaria.
I dati acquisiti nell'ambito dei rilievi degli incidenti stradali potranno essere conservati per periodi di tempo maggiore per attività di analisi, studio, divulgazione e prevenzione, a condizione che i soggetti ripresi non siano riconoscibili e siano rispettati i principi di essenzialità del dato conservato.

Valutazione : Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Nelle zone in cui sono posizionate le telecamere è affissa adeguata segnaletica permanente (cartelli informativi) prevista dall'EDPB - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - adottate il 29 gennaio 2020.

E' stato già programmato l'aggiornamento dei cartelli di informativa mediante la graduale sostituzione dei precedenti avvisi con cartelli conformi alle indicazioni dell'Autorità Garante. Si specifica inoltre che nella sezione "privacy" del sito web istituzionale del comune di Andria viene riportata l'informativa completa sul trattamento dei dati di videosorveglianza ai sensi dell'art. 13 del reg. 679/16.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Non è previsto il consenso da parte degli interessati in quanto il trattamento rientra tra i compiti di interesse pubblico di cui è investito il Titolare.

Valutazione : Accettabile

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

Attraverso adeguata segnaletica permanente (informativa di primo livello) posizionata in prossimità delle zone interessate nonché attraverso l'informativa completa pubblicata sul sito istituzionale del comune di Andria, l'interessato viene messo a conoscenza delle del fatto che in qualunque momento, potrà esercitare i propri diritti [accesso alle informazioni (art.15), rettifica o integrazione (art.16), cancellazione (art.17), limitazione del trattamento (art.18), portabilità dei dati (art.20), il diritto di opporsi al trattamento dei dati per motivi particolari (art. 21) ai sensi del Regolamento UE n. 2016/679] mediante comunicazione scritta da inviare a mezzo pec al seguente indirizzo *protocollo@cert.comune.andria.bt.it*, a mezzo email all'indirizzo *contatto.rpd@gmail.com* oppure a mezzo raccomandata all'indirizzo del Titolare del trattamento dei dati [Città di Andria - Palazzo di Città - Piazza Umberto I - 76123 - Andria (BT)].

Poiché i dati acquisiti possono essere anche trattati per le finalità di polizia giudiziaria nonché di protezione di persone e/o cose, non è previsto il diritto di limitazione ed

opposizione per tali finalità; inoltre le istanze di cancellazione e opposizione potranno essere accolte solo qualora non siano più sussistenti le finalità di interesse pubblico.

Valutazione : Accettabile

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

Attraverso adeguata segnaletica permanente (informativa di primo livello) posizionata in prossimità delle zone interessate nonché attraverso l'informativa completa pubblicata sul sito istituzionale del comune di Andria, l'interessato viene messo a conoscenza delle del fatto che in qualunque momento, potrà esercitare il proprio diritto di cancellazione ex art. 17 del Regolamento UE n. 2016/679 mediante comunicazione scritta da inviare a mezzo pec al seguente indirizzo *protocollo@cert.comune.andria.bt.it*, a mezzo email all'indirizzo *contatto.rpd@gmail.com* oppure a mezzo raccomandata all'indirizzo del Titolare del trattamento dei dati [Città di Andria - Palazzo di Città - Piazza Umberto I - 76123 - Andria (BT)].

Valutazione : Accettabile

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

Attraverso adeguata segnaletica permanente (informativa di primo livello) posizionata in prossimità delle zone interessate nonché attraverso l'informativa completa pubblicata sul sito istituzionale del comune di Andria, l'interessato viene messo a conoscenza delle del fatto che in qualunque momento, potrà esercitare il proprio diritto di cancellazione ex art. 17 del Regolamento UE n. 2016/679 mediante comunicazione scritta da inviare a mezzo pec al seguente indirizzo *protocollo@cert.comune.andria.bt.it*, a mezzo email all'indirizzo *contatto.rpd@gmail.com* oppure a mezzo raccomandata all'indirizzo del Titolare del trattamento dei dati [Città di Andria - Palazzo di Città - Piazza Umberto I - 76123 - Andria (BT)].

Valutazione : Accettabile

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

Ogni qualvolta si rendesse necessario nominare un responsabile esterno del trattamento, il comune di Andria stipulerà un accordo scritto all'interno del quale il responsabile del trattamento così nominato si obbligherà a:

1. trattare i dati nel rispetto dei principi del trattamento dei dati previsti nel regolamento e solo per i fini indicati dal contratto di affidamento;

2. trattare i dati secondo le istruzioni documentate del Titolare del trattamento dei dati;

3. garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate formalmente alla riservatezza o abbiano un adeguato obbligo legale di riservatezza e abbiano ricevuto la formazione necessaria in materia di protezione dei dati personali;

4. redigere, ai sensi dell'art. 30, GDPR, qualora ne ricorrano i presupposti, il registro delle attività di trattamento;

5. 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, a mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a. la pseudonimizzazione e la cifratura dei dati personali;

b. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

6. mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi del presente accordo o contratto e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto da questi incaricato;

7. informare e coinvolgere tempestivamente il Titolare del trattamento di tutte le questioni riguardanti il trattamento dei dati personali ed in particolare nel caso di richieste di informazioni, controlli, ispezioni ed accessi da parte del Garante per la protezione dei dati personali;
8. tenendo conto della natura del trattamento, ad assistere il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
9. assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento ed in particolare a collaborare nelle comunicazioni di violazioni di dati personali, negli adempimenti della valutazione di impatto e consultazione preventive;
10. concordare con il Titolare del trattamento dei dati il testo dell'informativa privacy e assistere il Titolare del trattamento al fine di soddisfare l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato.
Il Responsabile esterno del trattamento, inoltre, non potrà ricorre ad un altro Responsabile se non previa autorizzazione scritta, del Titolare del trattamento. Nel caso in cui il Responsabile del trattamento (Responsabile primario) ricorra ad un altro Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento, su tale altro Responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel presente atto per il Responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento.
Nel caso in cui l'altro Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento.
Il Responsabile del trattamento dovrà, altresì, informare immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione violi il regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Nel caso in cui il Responsabile esterno del trattamento dei dati non sia stabilito in UE dovrà designare, ai sensi dell'art. 27, p. 3, un rappresentante in Italia.
Il Responsabile del trattamento, infine, su scelta del Titolare del trattamento, è tenuto a cancellare o a restituire tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati.

Valutazione : Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I dati non saranno oggetto di trasferimento al di fuori dell'Unione Europea. Resta in ogni caso inteso che il comune di Andria, ove lo ritenga necessario, avrà facoltà di mutare l'ubicazione dei server in Paesi extra-UE. In tal caso, il comune di Andria assicura sin d'ora che il trasferimento dei dati in Paesi extra-UE che non assicurino livelli di tutela adeguati saranno eseguiti solo previa conclusione, tra l'Ente stesso e detti soggetti, di specifici contratti contenenti clausole di salvaguardia e garanzie appropriate per la protezione dei dati personali (es. clausole contrattuali standard approvate dalla Commissione europea) ovvero solo in presenza di altro requisito conforme alla normativa italiana ed europea applicabile (es. decisione di adeguatezza dell'Autorità di controllo).

Valutazione : Accettabile

Misure esistenti o pianificate

Controllo degli accessi logici

L'accesso ai server VMS (video management sistem) avviene soltanto da specifiche reti autorizzate. Per l'accesso ai filmati è necessario nome utente e password personale. Sono presenti politiche di accesso alle immagini (policy access control) in grado di parzializzare gli accessi ai flussi video necessari all'utente che opera.
È prevista la revoca degli accessi da parte del gestore su indicazioni dell'ente.

Valutazione : Accettabile

Crittografia

Le immagini viaggiano su rete crittografata. Le immagini vengono salvate e archiviate in maniera crittografata su server fisici su rete dedicata (NO INTERNET) e separata dagli altri servizi comunali.
L'accesso da reti esterne viene effettuato tramite tecnologia VPN.

Valutazione : Accettabile

Tracciabilità

Tracciamento degli accessi logici al sistema.

Valutazione : Accettabile

Archiviazione

Tutta la documentazione digitale e/o analogica relativa all'attività di rilevazione di filmati/ immagini è salvata su server fisici dedicati nonché regolata dalla normativa vigente in materia di archiviazione nella pubblica amministrazione, contenente indicazioni specifiche per gli enti pubblici.

Valutazione : Accettabile

Vulnerabilità

L'accesso a internet è bloccato per le telecamere di videosorveglianza.
Vengono effettuati aggiornamenti automatici di Windows server. L'ente è in possesso di licenze per l'aggiornamento del software VMS.
Risulta installato un firewall di rete perimetrale che limita gli accessi alle sole reti autorizzate.
L'accesso al locale tecnico è controllato fisicamente.

Valutazione : Accettabile

Lotta contro il malware

Installazione software antivirus Windows defender sui server VMS nonché accesso da reti autorizzate.

Valutazione : Accettabile

Gestione postazioni

Le immagini sono visualizzate da postazioni gestite dall'ente ovvero dalla postazione di controllo.

Valutazione : Accettabile

Backup

Il back up della configurazione del sistema eseguito ogni notte.

Valutazione : Accettabile

Controllo degli accessi fisici

L’accesso ai server è consentito solo ai soggetti autorizzati.

Valutazione : Accettabile

Sicurezza dell'hardware

I server sono ubicati in un ambiente dedicato esclusivamente ai medesimi e tenuti sotto chiave all'interno di una stanza singola con sistema di climatizzazione in cui vi può accedere solo personale dipendente autorizzato.
Le postazioni operative sono soggette al controllo degli accessi.
E' presente un gruppo di continuità elettrico volto a evitare i rischi di black out.

Valutazione : Accettabile

Manutenzione

Viene effettuata regolarmente una attività di manutenzione nei confronti dei sistemi hardware e software del comune di Andria. Il responsabile CED e il responsabile esterno garantisce inoltre il corretto funzionamento dei software utilizzati dall'ente.

Valutazione : Accettabile

Contratto con il responsabile del trattamento

I responsabili esterni del trattamento vengono nominati tali tramite la stipula di un contratto, ai sensi degli Artt. 28 e 29 del Reg. Ue 679/2016.

Valutazione : Accettabile

Politica di tutela della privacy

L'amministrazione ha messo in atto una serie di misure orientate all'adeguamento della stessa alla normativa vigente.

I dipendenti sono stati nominati autorizzati al trattamento ai sensi dell'Art. 2-quaterdecies del D.Lgs. 196/2003, per l'esercizio delle loro funzioni.

Valutazione : Accettabile

Vigilanza sulla protezione dei dati

L'ente ha nominato un DPO ex art. 37 Reg. UE 679/2016.

Valutazione : Accettabile

Gestione del personale

Tutti gli operatori in forza presso l'ente hanno seguito seminari formativi in ordine all'introduzione del nuovo Reg. UE 679/2016.

Valutazione : Accettabile

Accesso illegittimo ai dati

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

Sistema di videosorveglianza urbana: in caso di sottrazione delle immagini non si correrebbe alcun rischio in quanto le immagini sono soggette a crittografazione.

Sistema di lettura targhe: in caso di sottrazione le immagini non potrebbero essere modificate in quanto crittografate.

Fototrappole: in caso di sottrazione le immagini potrebbero essere modificate in quanto non crittografate.

Dash Cam: in caso di sottrazione le immagini potrebbero essere modificate in quanto non crittografate.

Body Cam: in caso di sottrazione delle immagini le stesse potrebbero essere modificate in quanto le immagini sono soggette a crittografazione.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Sistema di videosorveglianza urbana: il sistema non è connesso ad internet quindi non ci possono essere vulnerabilità “logiche” ma esclusivamente fisiche dovute all’ingresso presso il Comando, all’ingresso presso la Sala Macchine o presso un armadietto stradale.

Sistema di lettura targhe: il sistema non è connesso ad internet quindi non ci possono essere vulnerabilità “logiche” ma esclusivamente fisiche dovute all’ingresso presso il Comando, all’ingresso presso la Sala Macchine o presso un armadietto stradale.

Fototrappole: qualora la fototrappola venisse trafugata verrebbero perse anche le immagini salvate sulla SDCard.

Dash Cam: in caso di sottrazione le immagini potrebbero essere modificate in quanto non crittografate.

Body Cam: in caso di sottrazione le immagini potrebbero essere modificate in quanto non crittografate.

Quali sono le fonti di rischio?

Si veda capo precedente.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Crittografia, Lotta contro il malware, Gestione postazioni, Backup, Controllo degli accessi fisici, Contratto con il responsabile del trattamento, Sicurezza dell'hardware, Manutenzione, Politica di tutela della privacy, Tracciabilità, Archiviazione, Vulnerabilità, Vigilanza sulla protezione dei dati, Gestione del personale.

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

Limitata,

La quantità e la rilevanza dei dati personali trattati potrebbe comportare una gravità di rischio che può essere considerata limitata.

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

Limitata.

L'attivazione di sistemi di vigilanza interna e l'adozione e l'attuazione del regolamento, unito ad attività di sensibilizzazione del personale dipendente, possono essere in grado di limitare violazioni ad alto impatto.

La limitazione a priori del trattamento di dati ex art. 9 e 10, con deroghe in particolari condizioni da parte del titolare, permette di limitare i potenziali rischi connessi ad una loro diffusione illecita.

Valutazione : Accettabile

Modifiche indesiderate dei dati

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

Sistema di videosorveglianza urbana: in caso di sottrazione delle immagini non si correrebbe alcun rischio in quanto le immagini sono soggette a crittografazione.

Sistema di lettura targhe: in caso di sottrazione le immagini non potrebbero essere modificate in quanto crittografate.

Fototrappole: in caso di sottrazione le immagini potrebbero essere modificate in quanto non crittografate.

Dash Cam: in caso di sottrazione le immagini potrebbero essere modificate in quanto non crittografate.

Body Cam: in caso di sottrazione delle immagini le stesse potrebbero essere modificate in quanto le immagini non sono soggette a crittografazione.

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

Sistema di videosorveglianza urbana: il sistema non è connesso ad internet quindi non ci possono essere vulnerabilità "logiche" ma esclusivamente fisiche dovute all'ingresso presso il Comando, all'ingresso presso la Sala Macchine o presso un armadietto stradale.

Sistema di lettura targhe: il sistema non è connesso ad internet quindi non ci possono essere vulnerabilità "logiche" ma esclusivamente fisiche dovute all'ingresso presso il Comando, all'ingresso presso la Sala Macchine o presso un armadietto stradale.

Fototrappole: qualora la fototrappola venisse trafugata verrebbero perse anche le immagini salvate sulla SDCard.

Dash Cam: in caso di sottrazione le immagini potrebbero essere modificate in quanto non crittografate.

Body Cam: in caso di sottrazione le immagini potrebbero essere modificate in quanto non crittografate.

Quali sono le fonti di rischio?

Si veda capo precedente.

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

Controllo degli accessi logici, Crittografia, Tracciabilità, Archiviazione, Vulnerabilità, Lotta contro il malware, Gestione postazioni, Backup, Controllo degli accessi fisici, Sicurezza dell'hardware, Manutenzione, Contratto con il responsabile del

trattamento, Politica di tutela della privacy, Vigilanza sulla protezione dei dati, Gestione del personale.

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

Limitata.

Sebbene la violazione potrebbe portare ad una errata o inefficace prestazione del servizio, le misure di backup e controllo degli accessi logici permetterebbero il recupero delle informazioni e la potenziale identificazione delle fonti di modifica.

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

Trascurabile.

Appare marginale che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti, purché si

proceda alla corretta applicazione e gestione delle misure di sicurezze adottate e pianificate dal comune di Andria.

Valutazione : Accettabile

Perdita di dati

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

Sistema di videosorveglianza urbana: in caso di sottrazione delle immagini non si correrebbe alcun rischio in quanto le immagini sono soggette a crittografazione.

Sistema di lettura targhe: in caso di sottrazione le immagini non potrebbero essere modificate in quanto crittografate.

Fototrappole: in caso di sottrazione le immagini potrebbero essere modificate in quanto non crittografate.

Dash Cam: in caso di sottrazione le immagini potrebbero essere modificate in quanto non crittografate.

Body Cam: in caso di sottrazione delle immagini le stesse potrebbero essere modificate in quanto le immagini non sono soggette a crittografazione.

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

Sistema di videosorveglianza urbana: il sistema non è connesso ad internet quindi non ci possono essere vulnerabilità "logiche" ma esclusivamente fisiche dovute all'ingresso presso il Comando, all'ingresso presso la Sala Macchine o presso un armadietto stradale.

Sistema di lettura targhe: il sistema non è connesso ad internet quindi non ci possono essere vulnerabilità "logiche" ma esclusivamente fisiche dovute all'ingresso presso il Comando, all'ingresso presso la Sala Macchine o presso un armadietto stradale.

Fototrappole: qualora la fototrappola venisse trafugata verrebbero perse anche le immagini salvate sulla SDCard.

Dash Cam: in caso di sottrazione le immagini potrebbero essere modificate in quanto non crittografate.

Body Cam: in caso di sottrazione le immagini potrebbero essere modificate in quanto non crittografate.

Quali sono le fonti di rischio?

Si veda capo precedente.

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

Controllo degli accessi logici, Crittografia, Tracciabilità, Archiviazione, Vulnerabilità, Lotta contro il malware, Gestione postazioni, Backup, Controllo degli accessi fisici, Sicurezza dell'hardware, Manutenzione, Contratto con il responsabile del trattamento, Politica di tutela della privacy, Vigilanza sulla protezione dei dati, Gestione del personale.

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

Limitata.

Possibile errata o rallentata gestione dell'attività amministrativa del comune di Andria a causa dell'incompletezza delle informazioni a disposizione dell'amministrazione.

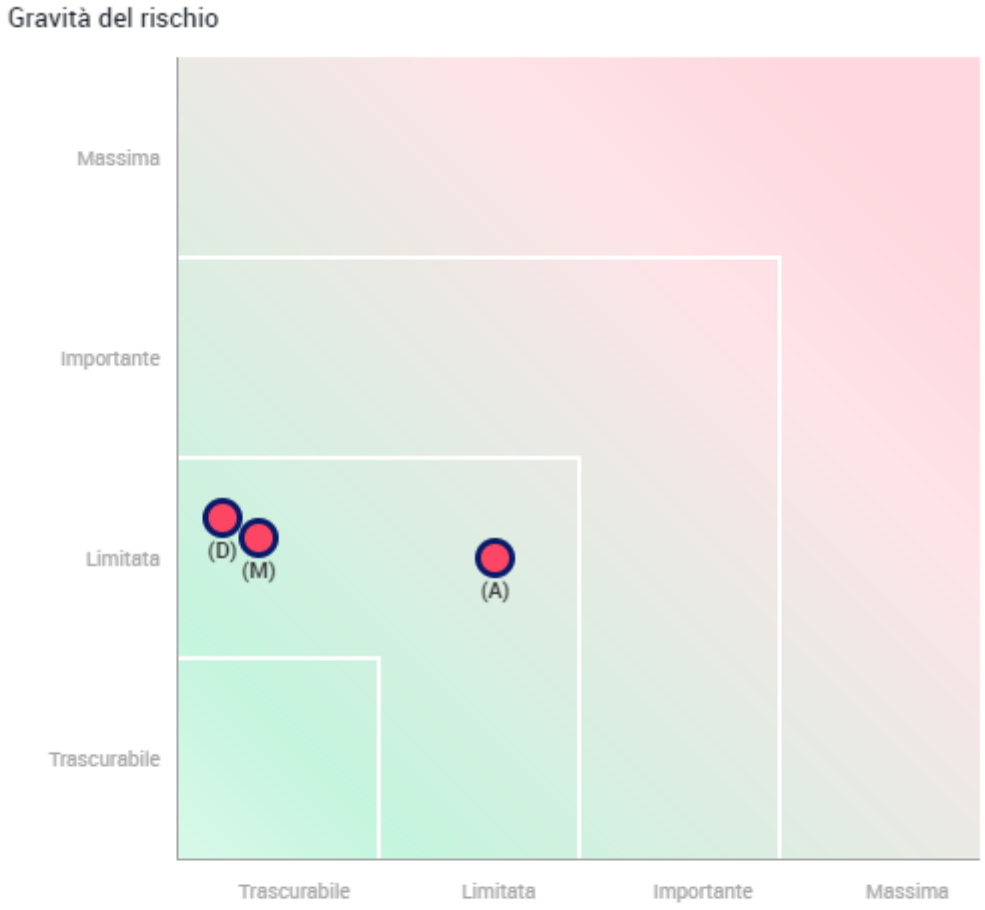
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile.

Appare marginale che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti, purché si proceda alla corretta applicazione e gestione delle misure di sicurezze adottate e pianificate dal comune di Andria.

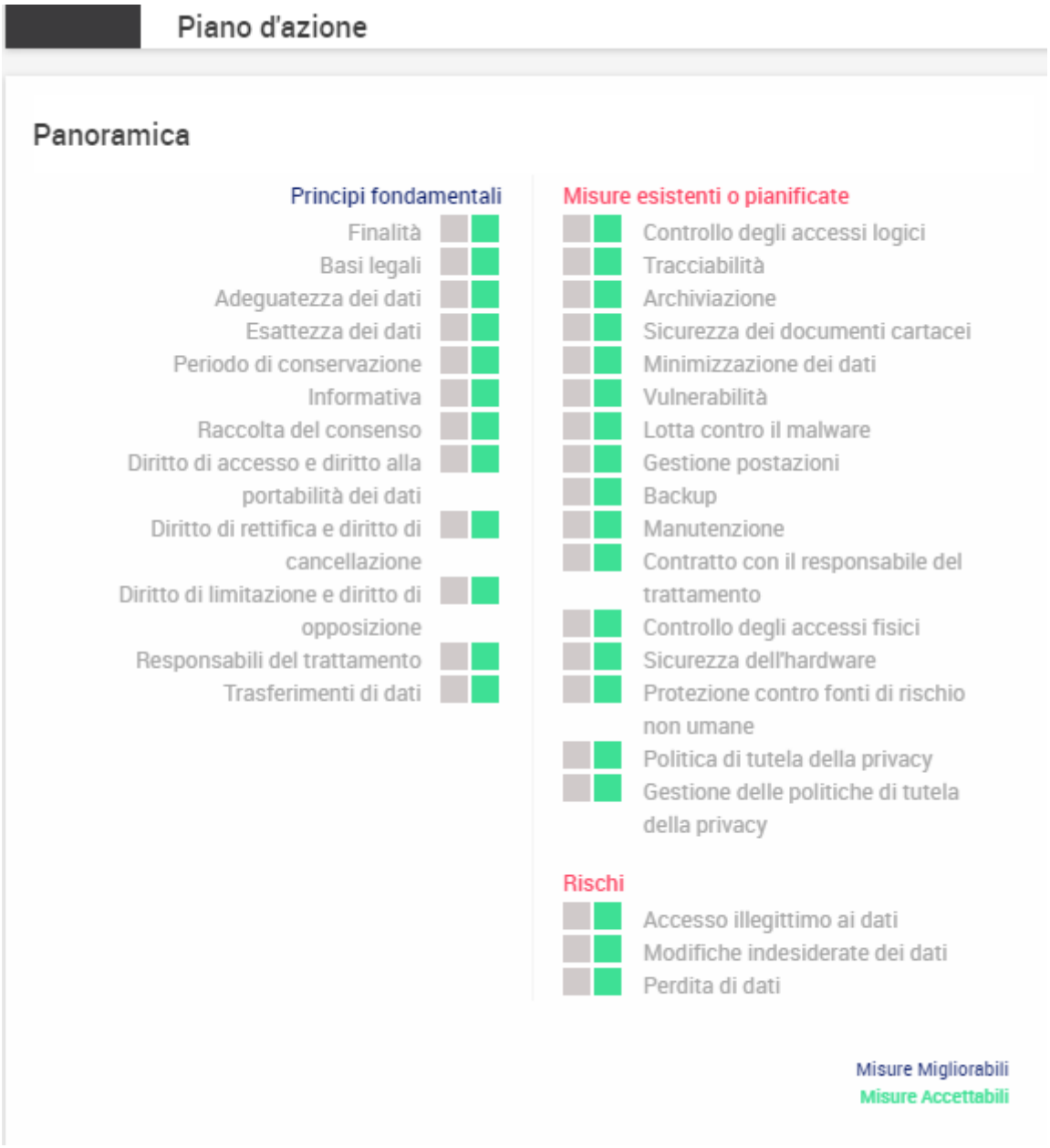
Valutazione : Accettabile

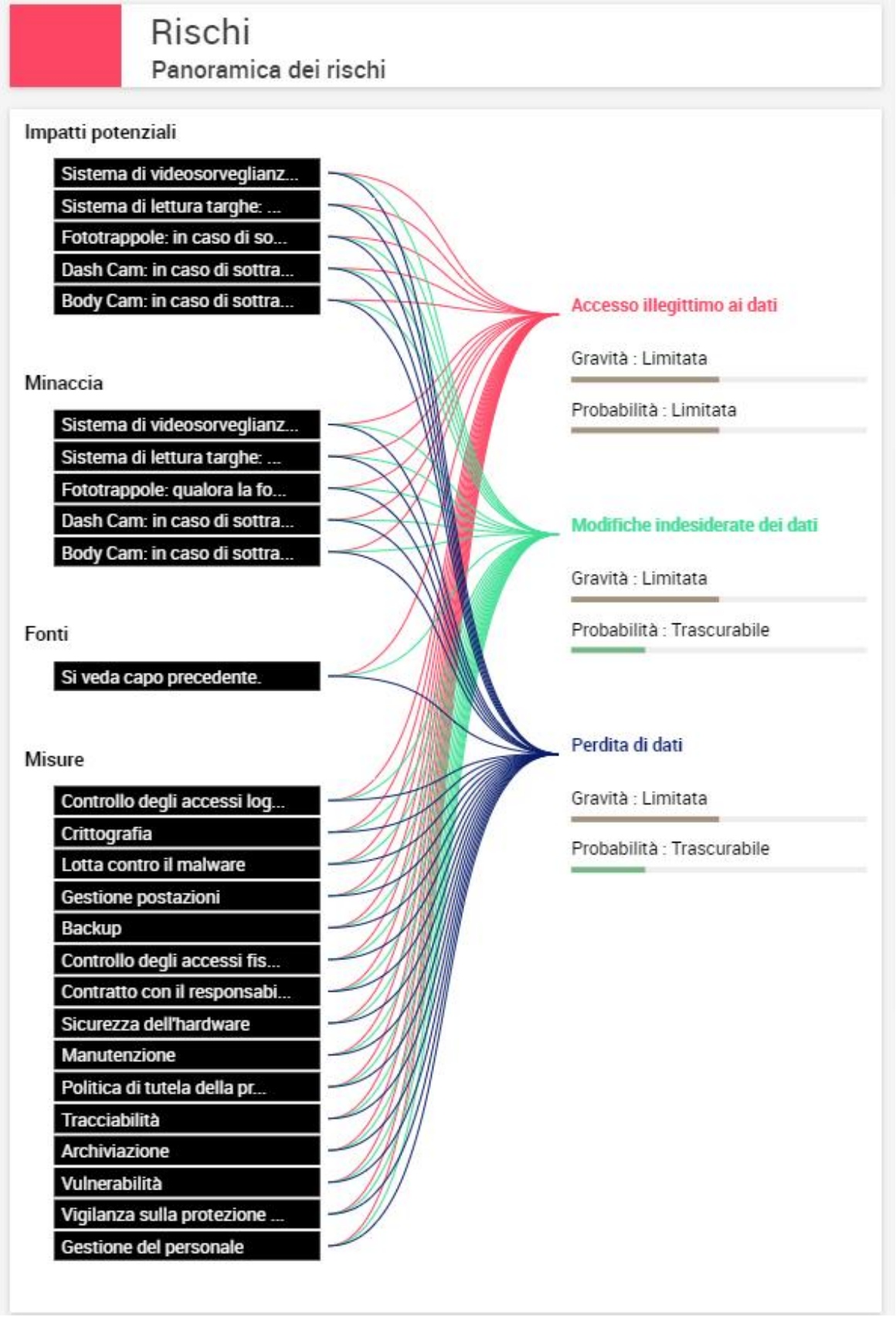
Mappaggio dei rischi



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

Piano d'azione




Rischi
Panoramica dei rischi
Impatti potenziali
Sistema di videosorveglianz...
Sistema di lettura targhe: ...
Fototrappole: in caso di so...
Dash Cam: in caso di sottra...
Body Cam: in caso di sottra...
Minaccia
Sistema di videosorveglianz...
Sistema di lettura targhe: ...
Fototrappole: qualora la fo...
Dash Cam: in caso di sottra...
Body Cam: in caso di sottra...
Fonti
Si veda capo precedente.
Misure
Controllo degli accessi log...
Crittografia
Lotta contro il malware
Gestione postazioni
Backup
Controllo degli accessi fis...
Contratto con il responsabi...
Sicurezza dell'hardware
Manutenzione
Politica di tutela della pr...
Tracciabilità
Archiviazione
Vulnerabilità
Vigilanza sulla protezione ...
Gestione del personale
Accesso illegittimo ai dati
Gravità : Limitata
Probabilità : Limitata
Modifiche indesiderate dei dati
Gravità : Limitata
Probabilità : Trascurabile
Perdita di dati
Gravità : Limitata
Probabilità : Trascurabile

Parere del DPO/RPD

In seguito ad attenta analisi del presente documento, visto l'art. 39 par. 1 lett. C del Reg. 679/2016, il DPO ritiene che i rischi per i diritti e le libertà degli interessati soggetti alle riprese, a seguito dell'adozione delle misure di mitigazione del rischio indicate dall'ente, possano essere qualificati come rischi accettabili in relazione alle finalità perseguite dal trattamento in oggetto. Il sistema nel suo complesso coniuga in un ragionevole equilibrio il diritto alla riservatezza e protezione dei dati personali dei cittadini con le attività di sicurezza urbana e tutela, prevenzione e gestione delle criticità di ordine pubblico in capo alle forze di Polizia Locale, come da competenza normativa. Nello specifico, non sono mai state attivate funzionalità speciali di controllo "intelligente" del sistema di videosorveglianza né di identificazione anche biometrica degli interessati, pertanto nel complesso, alla data odierna, non si ritiene esistente un "rischio elevato" come inteso dall'art. 35 GDPR; per tale ragione, inoltre, non si rende necessario procedere con la Consultazione preventiva ex art. 36 GDPR.

Allegato 1: elenco telecamere installate;
Allegato 2: regolamento per la disciplina della videosorveglianza nel territorio comunale di Andria.

Andria,01.02.2023

Autore
Il dirigente
Dott. Francesco CAPOGNA
Firmato digitalmente

Firmato digitalmente da: Francesco Capogna
Data: 01/02/2023 08:59:03

Sindaco
Sindaco Avv. BRUNO
Firmato digitalmente

Firmato digitalmente da:
Giovanna Bruno
Data: 01/02/2023 11:16:51