



COMUNE DI PUGLIANELLO

Provincia di Benevento

Progetto per la realizzazione di un impianto di videosorveglianza urbana

Valutazione d'impatto sulla protezione dei dati DPIA

Art. 35 Regolamento Generale sulla Protezione dei dati

Il titolare del trattamento: Sindaco on. dott. Francesco Maria Rubano

DPIA effettuata con software del CNIL per la Valutazione di impatto sulla protezione dei dati

INFORMAZIONI SULLA PIA

NOME DELLA PIA

DPIA VIDEOSORVEGLIANZA COMUNE DI PUGLIANELLO

NOME AUTORE

RESPONSABILE POLIZIA MUNICIPALE DOTT.SSA ANTONELLA SCETTA

NOME VALUTATORE

RESPONSABILE POLIZIA MUNICIPALE DOTT.SSA ANTONELLA SCETTA

NOME VALIDATORE

RESPONSABILE PROTEZIONE DATI PERSONALI DOTT. ANTONELLO BOTTE

DATA DI CREAZIONE

29/06/2026

CONTESTO

PANORAMICA DEL TRATTAMENTO

QUALE È IL TRATTAMENTO IN CONSIDERAZIONE?

Il trattamento operato dagli agenti di Polizia Locale, interamente o parzialmente automatizzato, dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza attivati nel territorio dell'Ente, ai sensi e secondo quanto disposto dalla seguente normativa:

- Regolamento UE Generale sulla Protezione dei Dati 2016/679 (di seguito RGPD) 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"*;
- Decreto Legislativo 10 agosto 2018, n. 101 *"Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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)"*;
- Decreto Legislativo 18 maggio 2018, n. 51 – Attuazione della 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"*;
- DPR n. 15 del 15/01/2018 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"*;
- Provvedimento del Garante per la Protezione dei Dati Personali in materia di Videosorveglianza dell'8 aprile 2010 (G.U. n. 99 del 29/04/2010);
- Decreto Ministero dell'Interno 05/08/2008 (GU n. 186 del 09.08.2008);

- Legge n. 38/2009 recante *“misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale nonché in tema di atti persecutori”*.

L'impatto è valutato con particolare attenzione ai diritti e alle libertà degli interessati ed ha come obiettivo di verificare e garantire la protezione dei dati personali di tutti coloro che entrano in contatto o in relazione con le attività di Videosorveglianza.

Le finalità di utilizzo dell'impianto di videosorveglianza sono conformi alle funzioni istituzionali demandate ai Sindaci ed ai Comuni 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”*, dal D.L.vo 18 agosto 2000, n. 267, dal D.P.R. 24 luglio 1977, n. 616, dalla legge sull'ordinamento della Polizia Locale 7 marzo 1986, n. 65 nonché dallo Statuto Comunale e dai Regolamenti Comunali vigenti, ed in particolare:

- a) attivare misure di prevenzione e sicurezza sul territorio Comunale;
- b) la protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, l'ordine e sicurezza pubblica, la prevenzione, accertamento o repressione dei reati o esecuzione di sanzioni penali a norma del D.Lgs. 51/2018
- c) attivazione di uno strumento di Protezione Civile sul territorio comunale;
- d) vigilare sul pubblico traffico;
- e) prevenire eventuali atti di vandalismo o danneggiamento agli immobili ed in particolare al patrimonio comunale e di disturbo alla quiete pubblica;
- f) la protezione della proprietà;
- g) le attività di rilevazione, prevenzione e controllo delle infrazioni, nel quadro delle competenze attribuite dalla legge;
- h) l'acquisizione di fonti di prove in ambito delle attività di polizia amministrativa;
- i) per controllare situazioni di degrado caratterizzate da abbandono di rifiuti su aree pubbliche ed accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose;
- j) monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;
- k) verificare l'osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti;
- l) l'eventuale utilizzo del sistema di videosorveglianza per finalità di prevenzione generale, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, con sistematico accesso da parte di altre forze di polizia, deve essere oggetto di specifici accordi, in cui vengono disciplinati le modalità di accesso, gli ambiti di utilizzo e le correlate responsabilità.

QUALI SONO LE RESPONSABILITÀ CONNESSE AL TRATTAMENTO?

Le responsabilità del trattamento sono connesse ai ruoli ricoperti: il titolare del trattamento è l'Ente è rappresentato dal Sindaco pro tempore; il designato/autorizzato al trattamento (responsabili interni) è il Dirigente/Responsabile di posizione organizzativa del servizio di Polizia Locale, se formalmente nominato; possono essere nominati come Responsabili del trattamento, ai sensi dell'art. 28 del GDPR, tutti i soggetti fisici o giuridici che gestiscono per conto dell'ente dati personali nell'ambito di un appalto di servizi relativo al supporto per la gestione degli impianti.

CI SONO STANDARD APPLICABILI AL TRATTAMENTO?

Al momento non sono contemplati standard da applicare direttamente al trattamento. Tuttavia l'attività di videosorveglianza è disciplinata da uno specifico regolamento adottato dell'ente.

Valutazione: Accettabile

CONTESTO

DATI, PROCESSI E RISORSE DI SUPPORTO

QUALI SONO I DATI TRATTATI?

Gli impianti riprendono e registrano immagini che permettono di identificare in modo diretto o indiretto le persone riprese, consentono riprese unicamente di video o foto, sono installati nel territorio dell'Ente e possono essere sia fissi che mobili.

Vengono trattati i dati degli autoveicoli, targhe e persone fisiche che circolano in prossimità delle telecamere.

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 o interconnessione, limitazione, pseudonimizzazione. Le immagini sono visualizzate in tempo reale direttamente presso il comando della Polizia locale da persone autorizzate. Le immagini rilevanti ogni sorta di infrazione o reato vengono scaricate in locale su dispositivo di memoria di massa, sottoposte a cifratura e messe a disposizione in caso di necessità agli operatori di giustizia. Le immagini e video vengono sovrascritti in maniera automatica dopo sette giorni dalla loro rilevazione.

QUALI SONO LE RISORSE DI SUPPORTO AI DATI?

Gli impianti consentono riprese video e foto a colori, diurne e notturne, in condizioni di sufficiente illuminazione naturale o artificiale. Gli impianti di videosorveglianza sono sempre in funzione e registrano in maniera continuativa. I segnali video e foto delle unità di ripresa sono inviati presso la sede della Polizia locale su data center individuato appositamente, dove sono registrati su appositi server. In queste sedi le immagini sono visualizzate su monitor e hardware client appositamente configurato il cui accesso è protetto, riservato e consentito unicamente al personale formalmente e appositamente incaricato.

Valutazione: Accettabile

PRINCIPI FONDAMENTALI

PROPORZIONALITÀ E NECESSITÀ

GLI SCOPI DEL TRATTAMENTO SONO SPECIFICI, ESPlicitI E LEGITTIMI?

Sì, gli scopi del trattamento sono specifici, espliciti e legittimi. Il trattamento dei dati personali, acquisiti mediante l'utilizzo degli impianti di videosorveglianza gestiti dall'Ente e collegati alle centrali di controllo ubicate 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.

È garantito al contempo il rispetto dei diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento.

L'utilizzo degli impianti 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.

Valutazione: Accettabile

QUALI SONO LE BASI LEGALI CHE RENDONO LECITO IL TRATTAMENTO?

La base giuridica del trattamento è data dunque dalla necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri ai sensi dell'art. 6, paragrafo 1, lettera e) GDPR, nonché dalla necessità di eseguire un compito di un'autorità competente per le finalità di prevenzione, accertamento e perseguimento di reati, salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica ai sensi dell'art. 5 del D.lgs n. 51/2018

Valutazione: Accettabile

I DATI RACCOLTI SONO ADEGUATI, PERTINENTI E LIMITATI A QUANTO È NECESSARIO IN RELAZIONE ALLE FINALITÀ PER CUI SONO TRATTATI (MINIMIZZAZIONE DEI DATI)?

In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. minimizzazione dei dati) di cui all'art. 5, Paragrafo 1, lett. c), RGPD, 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 videosorveglianza. 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.

In attuazione del principio di limitazione e pertinenza, gli impianti di videosorveglianza e i programmi informatici di gestione sono configurati in modo da ridurre al minimo l'uso di dati personali ed identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere raggiunte mediante dati anonimi o con modalità che permettano di identificare l'interessato solo in caso di necessità, 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 visuale delle riprese ed evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti.

L'attività di videosorveglianza raccoglie esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando, quando non indispensabili, immagini dettagliate, ingrandite con dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza. La localizzazione delle telecamere e le modalità di ripresa saranno quindi stabilite in modo conseguente.

Valutazione: Accettabile

I DATI SONO ESATTI E AGGIORNATI?

I dati vengono aggiornati periodicamente, almeno su base annuale, e incrociati con le banche dati nazionali e con quelle degli archivi comunali, in riferimento ai cittadini e alle imprese residenti.

Valutazione: Accettabile

QUAL È IL PERIODO DI CONSERVAZIONE DEI DATI?

I dati personali registrati mediante l'utilizzo degli impianti di videosorveglianza sono conservati per un periodo di tempo non superiore a sette giorni dalla data della rilevazione. Decorso tale periodo, i dati registrati sono cancellati con modalità automatica. Gli strumenti e i supporti elettronici utilizzati sono dotati dei sistemi di protezioni, compreso la cifratura, che garantiscono la tutela dei dati trattati.

Valutazione: Accettabile

PRINCIPI FONDAMENTALI

MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

COME SONO INFORMATI DEL TRATTAMENTO GLI INTERESSATI?

Gli interessati sono informati nei seguenti modi:

- pubblicazione sul sito internet istituzionale di planimetrie e di altra documentazione relative alle zone videosorvegliate e foto-sorvegliate;
- installazione di apposita segnaletica permanente contenente l'informativa minima nelle aree in cui sono concretamente posizionate le telecamere, di cui al già richiamato Provvedimento in materia di videosorveglianza del Garante per la Protezione dei dati Personali del 08/04/2010. Sono fatti salvi i casi di prevenzione, accertamento o repressione dei reati.
- informativa contenente gli elementi di cui all'art. 13 e 14 del Regolamento UE 2016/679 disponibile agevolmente sul sito istituzionale dell'Ente senza oneri per gli interessati con modalità facilmente accessibili anche con strumenti informatici o telematici.
- La segnaletica deve essere collocata prima del raggio di azione della telecamera, o nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; la stessa deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno.
- In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, andranno installati più cartelli informativi,
- L'Ente, nella qualità di Titolare del trattamento dei dati, si obbliga ad informare la comunità cittadina dell'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di videosorveglianza, dell'eventuale incremento dimensionale dell'impianto stesso e dell'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo.

Valutazione: Accettabile

OVE APPLICABILE: COME SI OTTIENE IL CONSENSO DEGLI INTERESSATI?

Essendo l'Ente una Pubblica Amministrazione, che nell'esercizio dei propri pubblici poteri eroga servizi pubblici legittimamente attribuiti, non è tenuto all'acquisizione del consenso al trattamento dei dati. Nei casi in cui questo sia dovuto viene acquisito per iscritto.

Valutazione: Accettabile

COME FANNO GLI INTERESSATI A ESERCITARE I LORO DIRITTI DI ACCESSO E DI PORTABILITÀ DEI DATI?

In relazione al trattamento di dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. da 15 a 22 RGPD, 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 RGPD, 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, RGPD.

L'istanza per l'esercizio dei diritti dell'interessato è presentata al Responsabile della Protezione dei Dati dell'Ente, ai sensi dell'art. 38, paragrafo 4, RGPD ovvero al Responsabile del trattamento dei dati individuato.

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

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

Il responsabile della protezione dei dati dell'Ente ovvero il responsabile del trattamento accerterà l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano.

Qualora, ai sensi dell'art. 15 paragrafo 3 RGPD, l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei files contenenti le immagini in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti ad altre persone fisiche eventualmente presenti al momento della ripresa, in ossequio alla previsione di cui all'art. 15, paragrafo 4 RGPD.

I diritti riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

Nell'esercizio dei propri diritti l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può altresì farsi assistere da persona di fiducia.

Le istanze possono essere trasmesse al titolare o al responsabile anche mediante lettera raccomandata o posta elettronica certificata. Nel caso di esito negativo alla istanza l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Possono 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 interessi della persona fisica interessata, al fine di:

1. Non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;
2. Non compromettere la prevenzione, l'indagine, accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali;
3. Proteggere la sicurezza pubblica;
4. Proteggere la sicurezza nazionale.

Valutazione: Accettabile

COME FANNO GLI INTERESSATI A ESERCITARE I LORO DIRITTI DI RETTIFICA E DI CANCELLAZIONE (DIRITTO ALL'OBLIO)?

Per esercitare il diritto di rettifica e di cancellazione, se possibile, in ragione dell'obbligo dell'Ente di conservazione delle informazioni, gli interessati possono contattare direttamente il titolare o il designato del trattamento dei dati recandosi direttamente presso l'Ente, a mezzo raccomandata o posta elettronica certificata.

Valutazione: Accettabile

COME FANNO GLI INTERESSATI A ESERCITARE I LORO DIRITTI DI LIMITAZIONE E DI OPPOSIZIONE?

Per esercitare il diritto di limitazione o opposizione, se possibile, gli interessati possono contattare direttamente il titolare o il designato del trattamento dei dati recandosi direttamente presso l'Ente, a mezzo raccomandata o posta elettronica certificata.

Valutazione: Accettabile

GLI OBBLIGHI DEI RESPONSABILI DEL TRATTAMENTO SONO DEFINITI CON CHIAREZZA E DISCIPLINATI DA UN CONTRATTO?

Gli obblighi di ogni singolo Responsabile del Trattamento sono definiti nei contratti di appalto dei relativi servizi affidati o negli specifici accordi per il trattamento dei dati personali sottoscritti in uno al contratto.

Valutazione: Accettabile

IN CASO DI TRASFERIMENTO DI DATI AL DI FUORI DELL'UNIONE EUROPEA, I DATI GODONO DI UNA PROTEZIONE EQUIVALENTE?

I dati non vengono trasferiti al di fuori del territorio dell'Unione Europea.

Valutazione: Accettabile

RISCHI

MISURE ESISTENTI O PIANIFICATE

ANONIMIZZAZIONE

I dati particolari ovvero i c.d. dati sensibili, vengono trattati in maniera riservata unicamente dal personale strettamente necessario e a questo autorizzato. Vengono resi sempre completamente anonimi quando pubblicati.

Valutazione: Accettabile

CONTROLLO DEGLI ACCESSI LOGICI

Ad ogni operatore è assegnata una postazione fisica dotata di cassetti chiudibili con chiavi, se previsti, e una postazione di lavoro informatica (PC) dedicata. Ad ogni operatore vengono assegnate credenziali personali, username e password, univoche per l'accesso al sistema informatico.

Valutazione: Accettabile

ARCHIVIAZIONE

Ogni responsabile controlla l'archiviazione dei dati gestiti dall'ufficio in una cartella non condivisa su una postazione informatica protetta da password, mentre gli archivi generali dell'ente sono conservati su un server dedicato il cui accesso è limitato e controllato.

Per quanto riguarda l'archiviazione cartacea questa avviene all'interno degli uffici che trattano i dati e viene garantito l'anonimato delle informazioni contenute. Per quanto riguarda i dati particolari, vengono previste delle misure di protezione ulteriori e specifiche come armadi con chiusure con chiave o casseforti.

Valutazione: Accettabile

SICUREZZA DEI DOCUMENTI CARTACEI

I documenti cartacei vengono conservati dai dipendenti dell'ufficio. Il Responsabile verifica che siano disposti in specifici raccoglitori in modo tale che non vadano dispersi e che non siano visibili a terzi non autorizzati. Gli uffici devono essere chiusi e l'accesso consentito soltanto agli addetti o ai soggetti autorizzati.

Valutazione: Accettabile

MINIMIZZAZIONE DEI DATI

Vengono raccolti e conservati unicamente i dati necessari all'erogazione del servizio.

Valutazione: Accettabile

VULNERABILITÀ

I software in uso vengono aggiornati costantemente e l'accesso ai dati è limitato unicamente agli operatori direttamente interessati ai quali viene assegnato un account univoco e tracciabile.

Valutazione: Accettabile

PROTEZIONE DA MALWARE

Il software di protezione da malware è regolarmente installato e costantemente aggiornato.

Valutazione: Accettabile

BACKUP E COPIE DI SICUREZZA

Vengono effettuate giornalmente copie di sicurezza su unità di backup esterne. I dati di backup vengono cifrati.

Valutazione: Accettabile

SICUREZZA DELLE RETI DI COMUNICAZIONE

Il firewall risulta regolarmente installato, aggiornato e costantemente monitorato il flusso dati.

Valutazione: Accettabile

MANUTENZIONE

Viene effettuata la puntuale manutenzione fisica dei dispositivi sia preventiva che per guasti. Viene tenuto aggiornato l'inventario hw e sw dei dispositivi in uso.

Valutazione: Accettabile

CONTROLLO DEGLI ACCESSI FISICI

Gli accessi fisici agli uffici sono controllati e limitati al solo personale autorizzato, se del caso, dotato di badge.

Valutazione: Accettabile

PREVENZIONE DELLE FONTI DI RISCHIO

Gli Uffici dell'ente risultano rispettare le previsioni normative in materia di salute e protezione sui luoghi di lavoro.

Valutazione: Accettabile

GESTIONE DELLE POLITICHE DI TUTELA DELLA PRIVACY

Le politiche di tutela alla privacy comprendono il regolamento sulla videosorveglianza adottato dall'ente, nonché l'osservanza del Regolamento UE 679/2016 con relativa nomina del Data Protection Officer.

Valutazione: Accettabile

GESTIONE DEL PERSONALE

I dipendenti sono regolarmente invitati a partecipare ad incontri di formazione al fine di essere istruiti e aggiornati sul corretto trattamento dei dati personali.

Valutazione: Accettabile

SPECIFICHE MISURE DI SICUREZZA

Ai sensi di quanto previsto dall'articolo 24 del Reg. UE 2016/679, i dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza sono protetti da misure di sicurezza tali da ridurre al minimo i rischi di distruzione, perdita, modifica, accesso non autorizzato e trattamento non consentito o non conforme alle finalità di cui al Regolamento Comunale adottato dall'Ente.

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

- a. Vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»);
- b. Impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»);
- c. 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»);
- d. 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 cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»);
- f. 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 di dati («controllo della trasmissione»);
- g. Garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);
- h. Impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»);
- i. Garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»);
- j. Garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento stiano segnalati («affidabilità») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).

Valutazione: Accettabile

TRACCIABILITÀ

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

Valutazione: Accettabile

RISCHI

ACCESSO ILLEGITTIMO AI DATI

QUALI POTREBBERO ESSERE I PRINCIPALI IMPATTI SUGLI INTERESSATI SE IL RISCHIO SI DOVESSE CONCRETIZZARE?

Impatto limitato.

QUALI SONO LE PRINCIPALI MINACCE CHE POTREBBERO CONCRETIZZARE IL RISCHIO?

Perdita di dati, uso improprio di dati, diffusione di dati riservati o sensibili.

QUALI SONO LE FONTI DI RISCHIO?

Fonti di rischio interne ed esterne anche non umane.

QUALI MISURE FRA QUELLE INDIVIDUATE CONTRIBUISCONO A MITIGARE IL RISCHIO?

Controllo degli accessi logici, Minimizzazione dei dati, Anonimizzazione, Sicurezza dei documenti cartacei, Gestione delle politiche di tutela della privacy, Prevenzione delle fonti di rischio, Tracciabilità.

COME STIMERESTE LA GRAVITÀ DEL RISCHIO, SPECIALMENTE ALLA LUCE DEGLI IMPATTI POTENZIALI E DELLE MISURE PIANIFICATE?

Limitata, Il rischio è limitato, vengono riprese soprattutto i numeri di targa degli autoveicoli e le immagini sono conservate solo in caso di necessità di tutela della pubblica sicurezza.

COME STIMERESTE LA PROBABILITÀ DEL RISCHIO, SPECIALMENTE CON RIGUARDO ALLE MINACCE, ALLE FONTI DI RISCHIO E ALLE MISURE PIANIFICATE?

Limitata, secondo le misure pianificate il rischio è trascurabile.

Valutazione: Accettabile

RISCHI

MODIFICHE INDESIDERATE DEI DATI

QUALI SAREBBERO I PRINCIPALI IMPATTI SUGLI INTERESSATI SE IL RISCHIO SI DOVESSE CONCRETIZZARE?

Impatto limitato.

QUALI SONO LE PRINCIPALI MINACCE CHE POTREBBERO CONSENTIRE LA CONCRETIZZAZIONE DEL RISCHIO?

Errore materiale, evento doloso o abuso di ufficio da parte degli addetti ai lavori, accesso ai dati da parte di soggetti esterni non competenti e non autorizzati.

QUALI SONO LE FONTI DI RISCHIO?

Fonti di rischio interne ed esterne anche non umane.

QUALI MISURE, FRA QUELLE INDIVIDUATE, CONTRIBUISCONO A MITIGARE IL RISCHIO?

Backup e copie di sicurezza, Sicurezza delle reti di comunicazione, Manutenzione, Vulnerabilità, Controllo degli accessi fisici, Prevenzione delle fonti di rischio, Protezione da malware, Controllo degli accessi logici, Specifiche misure di sicurezza.

COME STIMERESTE LA GRAVITÀ DEL RISCHIO, IN PARTICOLARE ALLA LUCE DEGLI IMPATTI POTENZIALI E DELLE MISURE PIANIFICATE?

Importante, gli interessati potrebbero sperimentare inconvenienti significativi, superabili nonostante alcune difficoltà.

COME STIMERESTE LA PROBABILITÀ DEL RISCHIO, SPECIALMENTE CON RIGUARDO A MINACCE, FONTI DI RISCHIO E MISURE PIANIFICATE?

Limitata, appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: furto di supporti cartacei conservati in un locale dell'organizzazione il cui accesso è controllato).

Valutazione: Accettabile

RISCHI

PERDITA DI DATI

QUALI POTREBBERO ESSERE GLI IMPATTI PRINCIPALI SUGLI INTERESSATI SE IL RISCHIO DOVESSE CONCRETIZZARSI?

Impatto limitato.

QUALI SONO LE PRINCIPALI MINACCE CHE POTREBBERO CONSENTIRE LA MATERIALIZZAZIONE DEL RISCHIO?

Errore materiale, evento doloso o abuso di ufficio da parte degli addetti ai lavori, accesso ai dati da parte di soggetti esterni non competenti e non autorizzati, Attacco hacker.

QUALI SONO LE FONTI DI RISCHIO?

Fonti di rischio interne ed esterne anche non umane.

QUALI MISURE, FRA QUELLE INDIVIDUATE, CONTRIBUISCONO A MITIGARE IL RISCHIO?

Minimizzazione dei dati, Sicurezza delle reti di comunicazione, Protezione da malware, Backup e copie di sicurezza, Manutenzione, Gestione delle politiche di tutela della privacy, Anonimizzazione, Sicurezza dei documenti cartacei, Specifiche misure di sicurezza.

COME STIMERESTE LA GRAVITÀ DEL RISCHIO, SPECIALMENTE ALLA LUCE DEGLI IMPATTI POTENZIALI E DELLE MISURE PIANIFICATE?

Importante.

COME STIMERESTE LA PROBABILITÀ DEL RISCHIO, SPECIALMENTE CON RIGUARDO ALLE MINACCE, ALLE FONTI DI RISCHIO E ALLE MISURE PIANIFICATE?

Limitata.

Valutazione: Accettabile

Impatti potenziali

Impatto limitato

Minaccia

Perdita di dati, uso improp.

Errore materiale, evento do

Attacco hacker

Fonti

Fonti di rischio interne ed.

Misure

Controllo degli accessi log.

Minimizzazione dei dati

Anonimizzazione

Sicurezza dei documenti ca

Gestione della politiche di

Prevenzione delle fonti di

Tracciabilità

Backup e copie di sicurezza

Sicurezza delle reti di com.

Manutenzione

Vulnerabilità

Controllo degli accessi fis.

Protezione da malware

Specifiche misure di sicure

Accesso illegittimo ai dati

Gravità : Importante

Probabilità : Limitata

Modifiche indesiderate dei dati

Gravità : Importante

Probabilità : Limitata

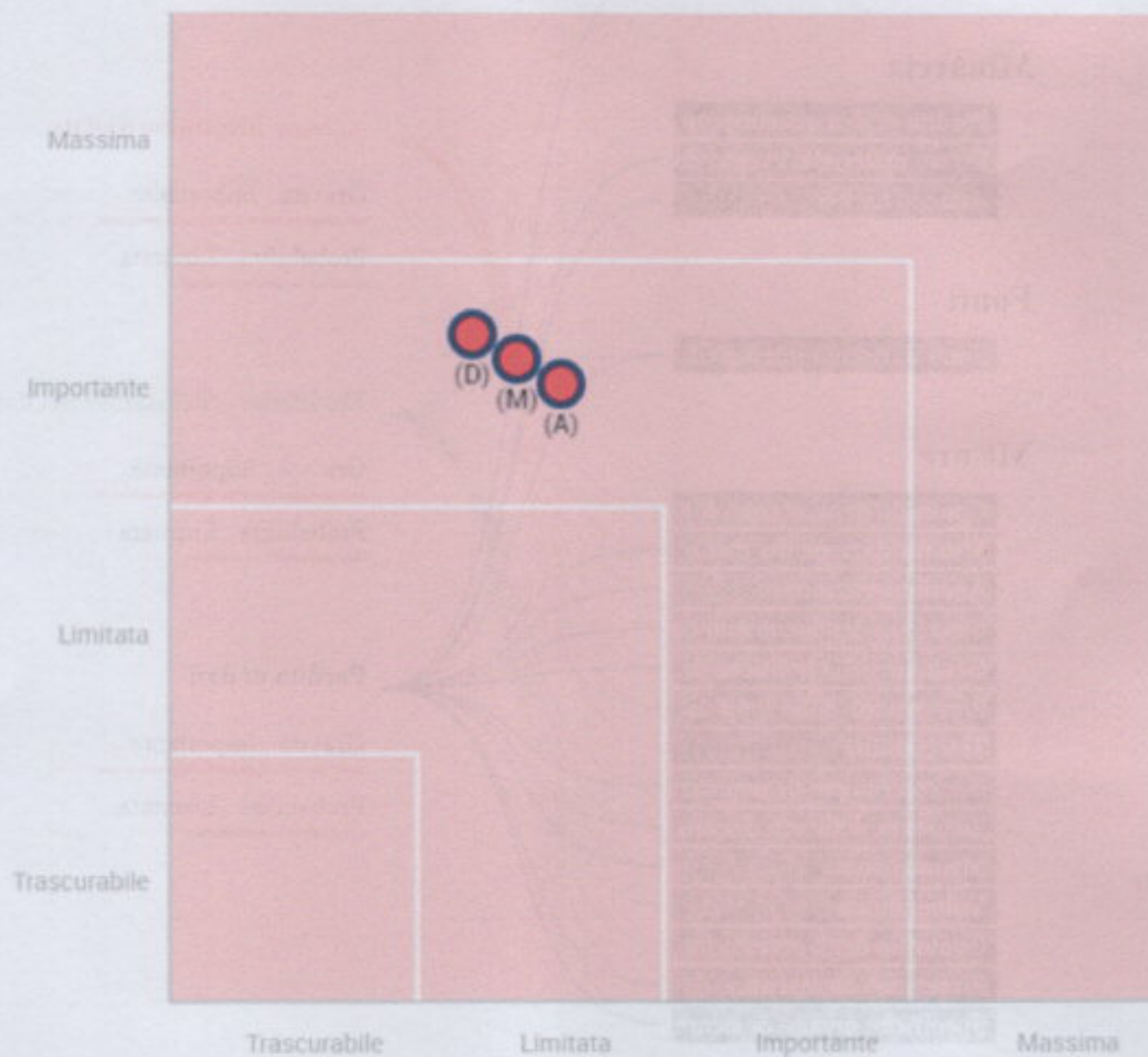
Perdita di dati

Gravità : Importante

Probabilità : Limitata

MAPPATURA DEL RISCHIO

Gravità del rischio

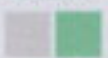
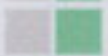
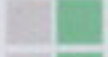


Probabilità del rischio

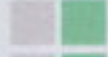
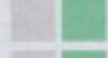
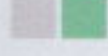
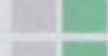
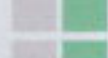
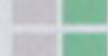
- **Misure pianificate o esistenti**
- **Con le misure correttive implementate**
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

Panoramica

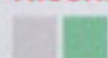
Principi fondamentali

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

Misure esistenti o pianificate

	Anonimizzazione
	Controllo degli accessi logici
	Archiviazione
	Sicurezza dei documenti cartacei
	Minimizzazione dei dati
	Vulnerabilità
	Protezione da malware
	Backup e copie di sicurezza
	Sicurezza delle reti di comunicazione
	Manutenzione
	Controllo degli accessi fisici
	Prevenzione delle fonti di rischio
	Gestione della politiche di tutela della privacy
	Gestione del personale
	Specifiche misure di sicurezza
	Tracciabilità

Rischi

	Accesso illegittimo ai dati
	Modifiche indesiderate dei dati
	Perdita di dati

Misure Migliorabili

Misure Accettabili

Panoramica

Principi fondamentali

Struttura organizzativa