Valutazione d'impatto (DPIA) in relazione al sistema di videosorveglianza sul territorio comunale

Ai sensi dell'art. 35 REGOLAMENTO (UE) 2016/679

Titolare del trattamento	Comune di Arizzano		
Responsabile della Protezione dei Dati personali (DPO/RPD):	Labor Service S.r.l. Dott.ssa Angela Emanuele		
Autori	• **Arch. Enrico Calderoni** Responsabile della gestione dell'impianto di videosorveglianza • **Dott.ssa Angela Emanuele** Responsabile della Protezione dei Dati personali		
Data di emissione	26/11/2024	**Versione**	0

Sommario

1. Riferimenti normativi

La valutazione d'impatto (o, altrimenti detta, DPIA – *Data Protection Impact Assessment*) è una procedura prevista dall'articolo 35 del Regolamento (UE) 2016/679 (GDPR) che il titolare deve svolgere allorquando intraprenda un'attività di trattamento particolarmente delicata. Lo scopo è quello di verificare l'impatto del trattamento sui diritti e le libertà degli interessati, valutandone, da una parte, la necessità e la proporzionalità rispetto al fine da perseguire, dall'altra, l'idoneità delle misure di sicurezza approntate per annullare o almeno limitare i rischi di incidenti. Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

Si riporta qui di seguito il testo integrale della citata norma, dove sono specificatamente indicate le condizioni al ricorrere delle quali è doverosa la valutazione d'impatto.

1. Quando un tipo di trattamento, allorché prevede in particolare l'**uso di nuove tecnologie**, **considerati la natura, l'oggetto, il contesto e le finalità** del trattamento, può presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:
a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un **trattamento automatizzato**, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il **trattamento, su larga scala, di categorie particolari di dati personali** di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
c) la **sorveglianza sistematica su larga scala di una zona accessibile al pubblico**.

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.

5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

7. **La valutazione contiene** almeno:
a) una **descrizione sistematica dei trattamenti previsti e delle finalità del trattamento**, compreso, ove applicabile, **l'interesse legittimo** perseguito dal titolare del trattamento;

b) una valutazione della **necessità e proporzionalità** dei trattamenti in relazione alle finalità;
c) una **valutazione dei rischi per i diritti e le libertà** degli interessati di cui al paragrafo 1; e
d) le **misure previste per affrontare i rischi**, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento

11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

2. Doverosità di svolgere la DPIA

Il Comune tramite l'installazione di un impianto di videosorveglianza pone in essere un trattamento che può rappresentare un rischio elevato per i diritti e le libertà delle persone fisiche, tenendo conto della natura, dell'oggetto, del contesto, delle finalità e delle eventuali nuove tecnologie utilizzate.
Pertanto, risulta obbligatoria la redazione del presente documento anche ai sensi dell'art. 35, par. 3, lett. c) GDPR.

3. Svolgimento della valutazione di impatto

Ritenuta, quindi, doverosa una valutazione d'impatto, il Comune, nel prosieguo del documento, rappresenta nel dettaglio quanto richiesto dal paragrafo 7 dell'art. 35 GDPR:

a) una **descrizione sistematica dei trattamenti previsti e delle finalità del trattamento**, compreso, ove applicabile, **l'interesse legittimo** perseguito dal titolare del trattamento;
b) una valutazione della **necessità e proporzionalità** dei trattamenti in relazione alle finalità;
c) una **valutazione dei rischi per i diritti e le libertà** degli interessati di cui al paragrafo 1;
d) le **misure previste per affrontare i rischi**, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione

3.1 La valutazione dei rischi

La valutazione dei rischi connessi al trattamento dei dati personali è una procedura che dev'essere adottata in relazione a ciascuna attività compiuta dal Titolare, la quale implichi un trattamento di dati personali.
Tale valutazione ha lo scopo di individuare:

1. le **peculiarità** di ciascuna attività di trattamento;
2. la **probabilità** che si verifichi un incidente idoneo ad intaccare la sicurezza del trattamento stesso;
3. la gravità del **danno** che verrebbe cagionato dall'eventuale incidente sui diritti e sulle libertà dei soggetti interessati; tale analisi prescinde dal risultato ottenuto;
4. il **rischio** connesso a ciascuna attività di trattamento svolta dal Titolare, quale risultato derivante dall'incrocio dell'esito emerso dall'analisi della probabilità e del danno;
5. le **misure necessarie** per la riduzione del rischio.

Essa si compone delle diverse fasi, qui di seguito schematicamente illustrate.

FASE 1	FASE 2	FASE 3
Contesto del trattamento	**Principi fondamentali del trattamento**	**Rischi**
✓ Panoramica del trattamento ✓ Dati, processi e risorse di supporto	✓ Proporzionalità e necessità ✓ Misure a tutela dei diritti degli interessati	✓ Misure esistenti o pianificate ✓ Accesso illegittimo ai dati ✓ Modifiche indesiderate dei dati ✓ Perdita di dati ✓ Panoramica dei rischi

Fase 1: Contesto del trattamento

Panoramica del trattamento

Quale è il trattamento in considerazione?
Il trattamento in considerazione, svolto dal Comune di Arizzano, riguarda il sistema di videosorveglianza di aree accessibili al pubblico (videosorveglianza comunale).
In particolare, il trattamento dei dati personali, svolto mediante l'utilizzo dei sistemi di videosorveglianza è finalizzato a:

a) utilizzare, quando possibile, le immagini registrate nella ricostruzione della dinamica degli incidenti stradali;
b) tutelare il patrimonio comunale da atti vandalici, danneggiamenti e furti;
c) tutelare la sicurezza urbana, ai sensi dell'art. 6 del dl 11/2009 convertito dalla L. 38/2009;
d) controllare le aree considerate a maggiore rischio per la sicurezza, l'incolumità e l'ordine pubblico;
e) rilevare infrazioni al Codice della Strada, da attuarsi nel rispetto delle norme specifiche che regolano la materia;
f) rilevare e controllare le targhe dei veicoli in transito attraverso telecamere per la lettura targhe, al fine di poter disporre di utili elementi per l'avvio di eventuali accertamenti connessi con la sicurezza urbana e per prevenire e sanzionare irregolarità di tipo amministrativo;
g) rilevare infrazioni a norme di legge o regolamento di competenza specifica della polizia municipale, con particolare riferimento alla tutela dell'ambiente;
h) prevenire, indagare, accertare e perseguire reati.

Commento [I1]:

Quali sono le responsabilità connesse al trattamento?
Il Titolare del trattamento è il Comune di Arizzano che autorizza al trattamento i soggetti che accedono alle immagini.
Inoltre, per l'attività di installazione viene coinvolta una ditta esterna specializzata appositamente nominata Responsabile del trattamento dei dati ai sensi dell'art. 28 GDPR.

Ci sono standard applicabili al trattamento?
Linee guida 03/2019 sul trattamento dei dati personali attraverso dispositivi video dell'EDPB.

Dati, processi e risorse di supporto

Quali sono i dati trattati?
Attraverso il sistema di videosorveglianza è possibile registrare le immagini di persone e le targhe di veicoli.
Le immagini sono archiviate per sette giorni e successivamente cancellate, se non utilizzate ai fini procedimentali.
I dati possono essere comunicati a: soggetti privati che ne fanno motivata richiesta, limitatamente ai dati a loro riferiti o in applicazione del diritto di accesso ai sensi della L. 241/1990 qualora vi sia un legittimo interesse del richiedente; Forze di Polizia o Autorità Giudiziarie per il perseguimento degli illeciti commessi sul territorio comunale.

Alle immagini possono accedere: la ditta di installazione e manutenzione appositamente nominata come Responsabile del trattamento; i soggetti autorizzati al trattamento dei dati.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?
Le registrazioni delle immagini catturate dalle telecamere di contesto vengono salvate su apposito server collocato presso la sede comunale.
L'impianto prevede l'utilizzo di videocamere con funzione Giorno e Notte, e di apparati radio wireless per il trasporto dei flussi video.
Le immagini sono archiviate per 7 giorni e successivamente cancellate automaticamente se non utilizzate ai fini procedimentali.

FASE 2. Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?
Nella richiamata cornice normativa ed all'interno del nuovo sistema di lotta alla criminalità che attribuisce ai Comuni un ruolo strategico nel perseguire finalità di tutela della sicurezza pubblica, l'impianto di videosorveglianza del Comune di Arizzano, è precipuamente rivolto a garantire la sicurezza urbana che, l'art. 1 del Decreto del Ministero dell'Interno del 5 agosto del 2008, testualmente definisce come il "bene pubblico da tutelare attraverso attività poste a difesa, nell'ambito delle comunità locali, del rispetto delle norme che regolano la vita civile, per migliorare le condizioni di vivibilità nei centri urbani, la convivenza civile e la coesione sociale."
Inoltre, il Comune ha adottato specifico Regolamento comunale in cui esplicita le finalità del trattamento che hanno quale base giuridica di legittimità l'art. 6, lett. e), GDPR ossia "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". Le finalità sono anche riportate nell'informativa privacy specifica per la videosorveglianza che sarà pubblicata sul sito internet del Comune.

Quali sono le basi legali che rendono lecito il trattamento?
Il trattamento è lecito in quanto si fonda sull'esercizio di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Comune di Arizzano (art. 6, par. 1, lett. e), GDPR) in forza delle seguenti normative:

· Legge 7 marzo 1986, n. 65 sull'ordinamento della polizia municipale
· Legge n. 38/2009 "Conversione in legge, con modificazioni, del decreto-legge 23 febbraio 2009, n. 11, recante misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori";
· 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 Linee Guida approvate il 26 luglio 2018 dalla Conferenza Stato – Città ed autonomie locali.
Statuto e Regolamenti comunali.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?
Il sistema informativo e i programmi informatici sono configurati riducendo al minimo l'utilizzazione dei dati personali e dei dati identificativi; l'obiettivo è quello di procedere all'identificazione dell'interessato solo nei casi in cui siano rilevati degli illeciti.

I dati sono esatti e aggiornati?
Le immagini registrate sono costantemente riaggiornate tramite sistema di sovrascrittura delle stesse, una volta decorso il periodo di tempo impostato per la loro conservazione

Qual è il periodo di conservazione dei dati?
I dati raccolti dalle videocamere sono conservati per un periodo non superiore a 7 giorni successivi alla rilevazione, fatte salve motivate esigenze di ulteriore conservazione, ed in modo particolare, in relazione ad illeciti che si siano verificati che determinando un procedimento anche di tipo amministrativo o ad indagini dell'Autorità Giudiziaria o di quella di Pubblica Sicurezza. In relazione alle capacità di immagazzinamento delle immagini sui server, le immagini riprese in tempo reale sovrascrivono quelle registrate trascorsi 7 giorni.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?
Il Comune di Arizzano provvederà ad affiggere un'adeguata segnaletica verticale che illustra l'informativa breve ex art. 13 GDPR. Essa sarà posizionata all'accesso delle aree in cui saranno concretamente ubicate le telecamere e comunque prima che i soggetti interessati entrino nel raggio di azione del sistema di videosorveglianza.
L'Informativa estesa, contenente tutte le informazioni di cui all'art. 13 GDPR, sarà resa disponibile sul sito internet istituzionale e presso gli uffici comunali.

Ove applicabile: come si ottiene il consenso degli interessati?
Il trattamento delle immagini tramite videosorveglianza effettuato per motivi di interesse pubblico è lecito in quanto connesso all'esecuzione di un compito di interesse pubblico ed all'esercizio di pubblici poteri di cui è investito il titolare (art. 6, lett. e), GDPR ed art. 2-ter D. Lgs. 196/2003 ss. mm.). Pertanto, non è necessario che il titolare richieda agli interessati di manifestare il loro consenso.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?
Con riferimento al diritto di accesso ai dati personali raccolti mediante un impianto di videosorveglianza previsto dall'art. 15 del GDPR la richiesta di accesso deve contenere:

- dati del richiedente;
- indicazione del luogo o dei luoghi in cui è stata effettuata la possibile ripresa;

- data e fascia oraria in cui è avvenuta la possibile ripresa (la fascia oraria deve essere indicata con un'approssimazione di trenta minuti);
- abbigliamento ed eventuali accessori;
- eventuale presenza di accompagnatori.

Nella sezione privacy del sito internet istituzionale è disponibile un modulo per esercitare un diritto in materia di privacy.
Fermo restando che le richieste pervenute con una modulistica difforme saranno ugualmente istruite, purché contenenti tutti gli elementi suindicati che, tuttavia, potranno formare oggetto di successiva integrazione.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?
Tutti i diritti sono esercitabili gratuitamente e senza particolari formalità mediante la presentazione, a mezzo posta elettronica o altro canale, di una richiesta di esercizio dei diritti indirizzata al Titolare del trattamento, responsabile dei sistemi di videosorveglianza. In ogni caso, al fine di consentire l'esercizio di tali diritti, il Comune di Arizzano individua e rende note le modalità di trasmissione della richiesta all'interno di un'apposita sezione privacy del sito internet istituzionale.

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?
Tutti i diritti sono esercitabili gratuitamente e senza particolari formalità mediante la presentazione, a mezzo posta elettronica o altro canale, di una richiesta di esercizio dei diritti indirizzata al Titolare del trattamento, responsabile dei sistemi di videosorveglianza. In ogni caso, al fine di consentire l'esercizio di tali diritti, il Comune di Arizzano individua e rende note le modalità di trasmissione della richiesta all'interno di un'apposita sezione privacy del sito internet istituzionale.

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?
Ai fini dell'installazione, del corretto funzionamento e della manutenzione degli impianti, il Comune si avvale della collaborazione esterna di ditta specializzata, che svolge prestazioni strumentali e subordinate alle scelte del Titolare del trattamento. Tale fornitore è stato nominato Responsabile del trattamento ai sensi dell'art. 28 GDPR con specifico atto formale in cui sono dettagliati gli obblighi a lui riferiti.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?
Il Titolare del trattamento non ha intenzione di trasferire i dati personali dell'interessato verso un Paese terzo all'Unione Europea o verso un'organizzazione internazionale. Ove si rendesse necessario, il trasferimento avverrà nel rispetto del Capo V del Regolamento (UE) 2016/679.

FASE 3. Rischi

Misure esistenti o pianificate

Crittografia
I dati presenti su Hard Disk oppure su eventuali Micro Sd presenti direttamente sulle telecamere tutti i dati sono criptati perciò non sono accessibili da persone terze se venissero sottratti eventuali dischi.

Controllo degli accessi logici
Per l'accesso all'impianto di videosorveglianza vengono utilizzate password con una lunghezza minima di 10 caratteri e almeno un carattere speciale.

Tracciabilità degli accessi
Da parte della società che gestisce l'impianto di videosorveglianza, le politiche che definiscono la tracciabilità degli eventi e la gestione dei relativi log sono ben strutturate per garantire la sicurezza e l'integrità dei dati.

Le telecamere e gli switch mantengono i log degli accessi, registrando dettagliatamente ogni evento rilevante. Questi log includono informazioni come timestamp, identificativi degli utenti e le attività eseguite. L'accesso a questi log è rigorosamente limitato ai membri del reparto specifico, garantendo che solo il personale autorizzato possa visualizzare e gestire tali informazioni.
I log sono conservati per un periodo di tempo adeguato a consentire un'analisi approfondita in caso di incidenti di sicurezza o di necessità di audit.

Sicurezza dei documenti cartacei
Tutti i dati personali sono digitali, comprese le password, e vengono archiviati in modo sicuro tramite gestori di password dedicati. Tuttavia, nel caso in cui fosse necessario trattare documenti cartacei contenenti dati personali, le politiche relative a questi documenti sono attentamente delineate. I documenti cartacei vengono stampati solo quando strettamente necessario e con apposita autorizzazione. Una volta stampati, sono archiviati in armadi chiusi a chiave, accessibili solo al personale autorizzato. Quando i documenti non sono più necessari, vengono distrutti in modo sicuro tramite trituratori di documenti certificati, garantendo che i dati personali non possano essere recuperati.

Limitazione della vulnerabilità
Vengono eseguiti aggiornamenti di sicurezza periodici su tutte le apparecchiature, telecamere e switch, per ridurre la probabilità che si verifichino vulnerabilità note. Le vulnerabilità identificate vengono prontamente corrette attraverso patch e aggiornamenti software, garantendo che i sistemi siano sempre protetti contro le minacce più recenti.

Backup
Per quanto riguarda i dati di registrazione delle telecamere, questi vengono mantenuti per un periodo compreso tra 8 e 20 giorni, a seconda delle specifiche esigenze operative e di sicurezza. Questa gestione temporale delle registrazioni consente di avere un archivio sufficiente per individuare e analizzare eventuali incidenti, pur rispettando le normative sulla protezione dei dati personali e garantendo la privacy degli individui

Manutenzione dell'impianto
La politica di manutenzione fisica dei dispositivi prevede un approccio strutturato e metodico, con l'eventuale ricorso all'outsourcing per interventi specializzati. La manutenzione di primo livello viene effettuata da remoto, gestendo l'alimentazione delle telecamere e altri dispositivi dove possibile. Questo permette di risolvere rapidamente problemi minori senza necessità di interventi fisici sul posto. Tuttavia, per interventi più complessi che non possono essere risolti da remoto, si procede con un intervento diretto sul posto, eseguito da tecnici specializzati. Per quanto riguarda i materiali difettosi, questi rimangono in mano al Comune. Questo consente di mantenere un controllo diretto sulla gestione dei dispositivi guasti, assicurando che siano riparati o sostituiti in modo tempestivo e sicuro, evitando potenziali rischi di sicurezza derivanti dalla gestione esterna dei materiali difettosi.

Sicurezza dell'hardware
Per ridurre il rischio che le apparecchiature possano essere utilizzate per danneggiare i dati personali, vengono adottate diverse misure di sicurezza. Innanzitutto, viene mantenuto un inventario dettagliato e aggiornato di tutte le apparecchiature, e queste sono organizzate in compartimenti fisici e logici per limitare l'accesso ai dati sensibili solo al personale autorizzato. Viene implementata la ridondanza delle apparecchiature critiche per garantire continuità operativa in caso di guasto. L'accesso sia fisico che logico alle apparecchiature è rigorosamente controllato, con l'uso di password complesse e autenticazione a più fattori. A livello hardware, tutti gli armadi che contengono apparecchiature condivise sono sottochiave, così come gli armadi delle telecamere di sicurezza, garantendo che solo il personale autorizzato possa accedervi. Queste misure integrate assicurano un ambiente sicuro per le apparecchiature e i dati personali gestiti.

Accesso illegittimo ai dati

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

- Discriminazione
- Danno per la reputazione
- Perdita di controllo dei dati
- Conoscenza da parte di terzi non autorizzati.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

- Furto dei supporti fisici di archiviazione e registrazione
- Attacchi informatici alla rete
- Errore umano.

Quali sono le fonti di rischio?

- Virus informatici
- Persona interna o esterna all'ente o al fornitore.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

- Crittografia
- Controllo degli accessi logici
- Tracciabilità degli accessi
- Sicurezza dei documenti cartacei
- Limitazione della vulnerabilità
- Sicurezza dell'hardware.

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

Limitata, la gravità del rischio è ritenuta limitata.

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

Limitata, la probabilità del rischio è ritenuta limitata in quanto le misure di sicurezza adottate del Titolare sono idonee a mitigare il rischio di accesso illegittimo ai dati.

Modifiche indesiderate dei dati

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

- Danno per la reputazione
- Discriminazione
- Impossibilità di esercitare diritti, servizi o opportunità.

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

Attacchi informatici alla rete.

Quali sono le fonti di rischio?

Virus informatici.

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

- Crittografia
- Limitazione della vulnerabilità
- Sicurezza dell'hardware.

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

Limitata, la gravità del rischio è ritenuta importante perché è previsto altresì un backup.

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

Limitata, la probabilità del rischio è ritenuta limitata in quanto le misure di sicurezza adottate del Titolare sono idonee a mitigare il rischio di modifiche indesiderate dei dati.

Perdita di dati

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

- Perdita di controllo dei dati
- Limitazione dei diritti.

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

- Attacchi informatici alla rete
- Errore umano
- Furto dei supporti fisici di archiviazione e registrazione
- Danni fisici ai supporti di archiviazione e registrazione anche a seguito di eventi esterni quali incendi, calamità naturali ecc…

Quali sono le fonti di rischio?

- Virus informatici
- Persona interna o esterna all'ente o al fornitore
- Usura o malfunzionamento dei supporti di archiviazione e registrazione
- Incendio
- Calamità naturali.

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

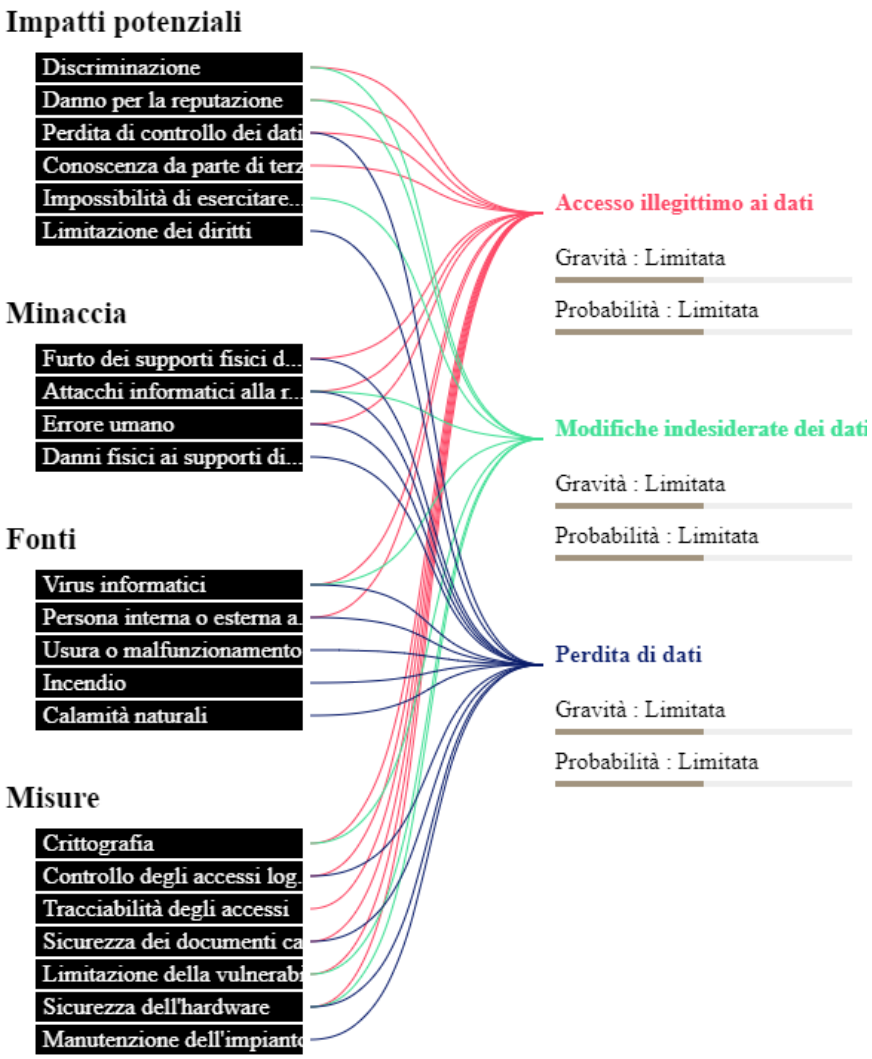
- Manutenzione dell'impianto
- Sicurezza dei documenti cartacei
- Sicurezza dell'hardware
- Controllo degli accessi logici.

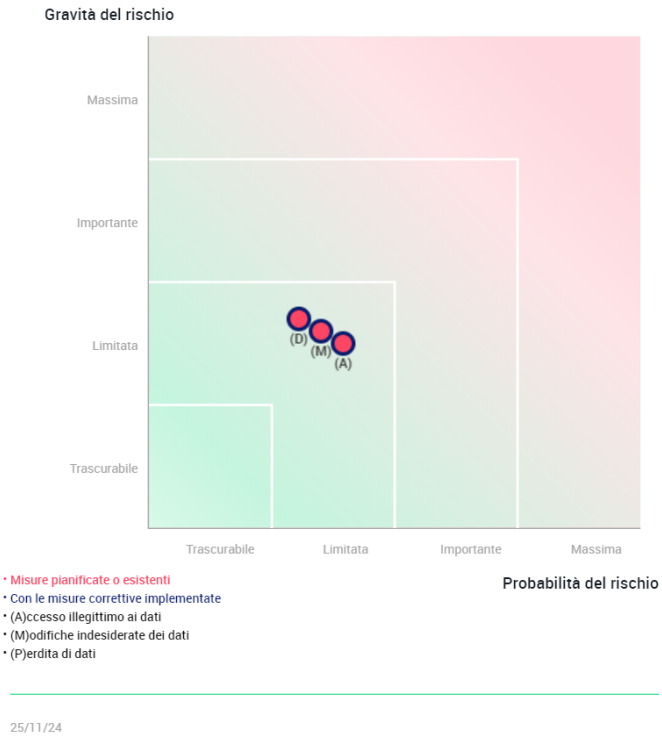
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata, la gravità del rischio è ritenuta limitata perché è previsto un backup dei dati.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?
Limitata, la probabilità del rischio è ritenuta limitata in quanto le misure di sicurezza adottate del Titolare sono idonee a mitigare il rischio di perdita dei dati.

3.2 Panoramica dei rischi





3.3 Misure migliorative pianificate

TIPOLOGIA DI MISURA	MISURA MIGLIORATIVA SPECIFICA E SCOPO
☒**Gestione del personale**	Formazione del personale specifica sul tema della videosorveglianza.

3.4 Parere del DPO e degli interessati

Parere del DPO:
Dall'analisi delle misure di sicurezza in essere, si ritiene che il sistema possa essere implementato nella parte relativa alla formazione specifica del personale operante sul sistema di videosorveglianza, al fine di conformare il trattamento alle *Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, emanate dall'EDPB.
Ciò premesso, si ritiene che il rischio stimato sia attenuato dalle misure di sicurezza già adottate e che si propone di adottare.
In ogni caso, il Comune di Arizzano si impegna a riesaminare periodicamente la DPIA, specialmente qualora si registrasse una variazione del trattamento, della natura, del contesto, delle modalità e della tipologia di dati, nonché delle misure di sicurezza adottate.
Alla luce della DPIA effettuata, non si ritiene necessario condividere il presente documento con l'Autorità Garante (obbligo sussistente solo in caso di un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio – art. 36, par. 1).

Richiesta del parere degli interessati
Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati
Il sistema di videosorveglianza delle aree accessibile al pubblico coinvolge potenzialmente un numero non definito e una tipologia di interessati vari e, pertanto, è impossibile richiederne un parere.

4. Conclusioni

Dopo aver valutato nel dettaglio quanto richiesto dal par. 7 dell'art. 35 GDPR, il Comune può concludere che il trattamento di videosorveglianza analizzato risulta:

1) **Proporzionato** alla finalità che legittimamente si vuole perseguire: nel contemperamento degli interessi, prevale quello della prevenzione e repressione di illeciti e di reati, nonché di migliorare la sicurezza della cittadinanza.
2) **Necessario**, in quanto tale finalità non potrebbe essere raggiunta diversamente ed altrettanto efficacemente.