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 Mergozzo		
Responsabile della Protezione dei Dati personali (DPO/RPD):	Labor Service S.r.l.		
Data di emissione	08/08/2023	**Versione**	00

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 proseguo 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

I punti a), c), d) sono approfonditi specificatamente nella valutazione dei rischi, la cui procedura comprende fra l'altro la descrizione dei trattamenti, delle loro finalità, del legittimo interesse, nonché delle misure adottate per affrontare i rischi.
Il punto d) sarà oggetto di ulteriore specifica analisi, a seguito della valutazione dei rischi.
Il punto b) verrà analizzato al termine di suddetta valutazione.

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;
2) la gravità del **danno** che verrebbe cagionato dall'eventuale incidente sui diritti e sulle libertà dei soggetti interessati; tale analisi prescinde dal risultato ottenuto
3) 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;
4) 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
Descrizione del trattamento	**Valutazione della probabilità di incidente**	**Valutazione della gravità del danno**
Tale descrizione si ottiene rispondendo alle seguenti domande: ✓ Qual è l'attività di trattamento? ✓ Qual è lo scopo del trattamento? ✓ Quali dati personali sono trattati? ✓ Quali sono gli interessati coinvolti? ✓ Qual è la base giuridica del trattamento? ✓ Dove avviene il trattamento? ✓ Quali sono gli strumenti utilizzati? ✓ Chi sono i destinatari del trattamento? Ci sono responsabili del trattamento e/o contitolari? ✓ Quali misure di sicurezza sono già state adottate?	Tale valutazione si ottiene rispondendo a 20 domande riconducibili ai seguenti settori: a. Rete e risorse tecniche; b. Processi e procedure del trattamento; c. Persone coinvolte nel trattamento; d. Settore commerciale e portata del trattamento;	Tale valutazione si ottiene esaminando le conseguenze che possono verificarsi sui diritti e le libertà degli interessati, tenendo in considerazione i seguenti parametri: ✓ Riservatezza; ✓ Integrità; ✓ Disponibilità;

RISULTATI	MISURE DI SICUREZZA
Illustrazione del risultato derivante dall'incrocio degli esiti emersi dalle fasi 2 e 3	Illustrazione degli adempimenti da svolgere a fronte dei risultati emersi dalla valutazione dei rischi

Le fasi 1, 2, 3, il calcolo dei risultati e l'elaborazione delle misure di sicurezza si ispirano al modello di valutazione dei rischi denominato *"Handbook on Security of Personal Data Processing"* del dicembre 2017, elaborato dalla "European Union Agency for Network and Information Security" (ENISA).

Fase 1: Descrizione del trattamento

FASE 1: Descrizione del trattamento e del contesto	
DOMANDA 1 - Qual è l'attività del trattamento?	
L'attività di trattamento consiste nella sorveglianza sistematica di una zona accessibile al pubblico (videosorveglianza comunale).	
DOMANDA 2 - Qual è lo scopo del trattamento?	
Il trattamento dei dati personali, svolto mediante l'utilizzo dei sistemi di videosorveglianza, è finalizzato a: a. prevenire e reprimere reati sul territorio comunale b. tutelare il patrimonio comunale, prevenire atti di vandalismo ed il danneggiamento a beni mobili ed immobili; c. controllare il traffico in ingresso ed in uscita dal territorio comunale ed in particolare, le targhe delle autovetture per abbandono rifiuti; d. controllare e reprimere l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose.	
DOMANDA 3 - Quali dati personali tratta?	
Immagini (persone e targhe) e relativi dati personali; dati giudiziari ex art. 10 GDPR (eventuale commissione di reato registrato dalle immagini)	
DOMANDA 4 - Quali sono gli interessati coinvolti?	
Tutti coloro che transitano sul territorio del Comune nelle aree videosorvegliate	
DOMANDA 5 – Qual è la base giuridica del trattamento dei dati?	
Il trattamento è lecito, in quanto si fonda sulle seguenti basi giuridiche: È connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, par. 1, lett. e); le norme di legge di riferimento sono il D. Lgs. 18 agosto 2000, n. 267, la Legge 7 marzo 1986, n. 65 sull'ordinamento della Polizia Municipale, il D.P.R. 24 luglio 1977 n. 616, il D.lgs. 31 marzo 1998 n. 112, la Legge 24 luglio 2008 n. 125 recante misure urgenti in materia di sicurezza pubblica, nonché dallo Statuto e dai Regolamenti Comunali e secondo i limiti sanciti dalla normativa in materia di privacy e dal D.lgs. 18 maggio 2018 n. 51, l'art. 6, commi 7 e 8 del D.L. 23 febbraio 2009, n. 11 convertito nella L. 23 aprile 2009, n. 38 in materia di sicurezza pubblica e di contrasto alla violenza sessuale.	
DOMANDA 5 - Dove avviene il trattamento?	
Territorio comunale oggetto di videosorveglianza - Ufficio della Polizia Locale, dove sono posizionati monitor e server.	
DOMANDA 6 - Quali sono gli strumenti utilizzati?	
Videocamere, server e monitor	
DOMANDA 7- Chi sono i destinatari del trattamento?	
• Forze dell'Ordine • Autorità Giudiziarie • La società a cui è stato affidato il servizio di installazione e manutenzione appositamente nominata come responsabile del trattamento ex art. 28 GDPR; • I soggetti interessati tramite richiesta di accesso agli atti.	
DOMANDA 8- Quali misure di sicurezza sono già state implementate?	
☐ Crittografia Indicare i mezzi implementati per assicurare la confidenzialità dei dati archiviati (in database, file, backup	

ecc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di sospetta compromissione ecc.). Specificare i mezzi crittografici impiegati per i flussi di dati (VPN, TLS, ecc.) implementati nel trattamento.	
☐ Anonimizzazione Indicare qui i meccanismi di anonimizzazione implementati, le garanzie da essi introdotte contro l'eventuale reidentificazione e per quali finalità sono implementati.	
☐ Pseudonimizzazione Indicare i metodi utilizzati per il pseudonimizzazione del trattamento.	
☒ Controllo degli accessi logici Descrivere in che modo sono definiti e attribuiti i profili degli utenti. Specificare i mezzi di autenticazione implementati precisando, ove applicabile, le regole per le password (lunghezza minima, caratteri richiesti, durata della validità, numero di tentativi prima del blocco dell'account, ecc.).	**I PROFILI DI ACCESSO DELLE IMMAGINI SONO GESTITI ATTRAVERSO PASSWORD GERARCHICHE, SARA' CURA DELLA COMMITTENZA ASSEGNARLE IN FUNZIONE DI UNA GERARCHIA DA LUI SCELTA.** **LA RESPONSABILITA' DI RESETTARE E/O CREARE UNA NUOVA UTENZA È IN CAPO SOLO ALL'AMMINISTRATORE DI SISTEMA.** **LE PASSWORD RISPONDONO ALLE ADEGUATE CARATTERISTICHE DI SICUREZZA. I TENATIVI CHE PRECEDONO AL BLOCCO SONO N. 4**
☒ Tracciabilità Descrivere le politiche che definiscono la tracciabilità degli eventi e la gestione dei relativi log.	**LO STRUMENTO IDONEO PER TRACCIARE I LOG PER GLI ACCESSI EFFETTUATI DAL COMUNE E DA NOI È LO STORICO EVENTI REGISTRATO DALLA MACCHINA. GLI ACCESSI SONO SEMPRE TRACCIABILI.**
☐ Archiviazione Descrivere le politiche di conservazione e gestione di archivi elettronici contenenti dati personali, finalizzate a tutelarne, in particolare, la validità giuridica per tutto il periodo necessario (versamento, conservazione, migrazione, accessibilità, eliminazione, politiche di archiviazione, protezione della confidenzialità, ecc.).	
☐Sicurezza dei documenti cartacei Descrivere le politiche relative ai documenti cartacei contenenti dati personali utilizzati nell'ambito del trattamento. Tali politiche descrivono come i documenti sono stampati, archiviati, distrutti e condivisi.	

☐Minimizzazione dei dati Descrivere i metodi utilizzati, come: filtraggio e rimozione, riduzione del potenziale identificativo attraverso trasformazione, riduzione della natura identificativa del dato, riduzione dell'accumulazione dei dati, limitazione dell'accesso ai dati	
☐ Vulnerabilità Descrivere le politiche volte a limitare la probabilità e la gravità dei rischi per le risorse utilizzate durante l'operatività (documentare le procedure operative, inventariazione e aggiornamento di software e hardware, correzione di vulnerabilità, duplicazione dei dati, limitazioni all'accesso fisico al materiale, ecc.).	
☐ Lotta contro il malware Descrivere le misure volte a proteggere l'accesso a reti pubbliche (Internet) o non controllate (di partner) nonché postazioni e server contro malware che potrebbe compromettere la sicurezza dei dati personali.	
☐Gestione postazioni Descrivere le misure adottate per ridurre la possibilità che le caratteristiche del software (sistemi operativi, applicazioni aziendali, software per ufficio, impostazioni ecc.) vengano sfruttate per danneggiare i dati personali (aggiornamenti, protezione fisica e accessi, lavoro su uno spazio di rete protetto, controlli di integrità, logging, ecc.).	
☐ Sicurezza dei siti web Descrivere i metodi e gli strumenti implementati per ridurre il rischio che le caratteristiche di un sito web siano sfruttate al fine di pregiudicare dati personali (disciplinare generale di sicurezza, cifratura TLS dei flussi di dati, politica di rilascio dei cookie, audit di sicurezza, ecc.) .	
☒Backup Descrivere le politiche di backup tali da assicurare la disponibilità e/o l'integrità dei dati personali, tutelandone la confidenzialità (periodicità dei backup, cifratura del canale di trasmissione dati, test di integrità, ecc.).	**LE IMMAGINI SONO SOTTOPOSTE A BACKUP** **NEL CASO DI INCEDENTE, I DATI PERSONALI POTREBBERO ESSERE RECUPERATI TEMPESTIVAMENTE.**
☒ Manutenzione Descrivere la politica di manutenzione fisica dei dispositivi, specificando l'eventuale ricorso	**L'IMPIANTO ESEGUE UNA DIAGNOSI AUTOMATICA ED È PREVISTO UN INTERVENTO DEI TECNICI.**

all'outsourcing. Dovrà comprendere la manutenzione remota, ove autorizzata, e specificare i metodi di gestione dei materiali difettosi.	
☒Contratto con il responsabile del trattamento I dati personali comunicati a o gestiti da responsabili del trattamento devono beneficiare di garanzie sufficienti.	**IL TITOLARE HA FORNITO AL RESPONSABILE DEL TRATTAMENTO FORMALI INDICAZIONI CIRCA IL TRATTAMENTO DEI DATI PERSONALI, COME PREVISTO DALL'ART. 28 GDPR.**
☒ Sicurezza dei canali informatici A seconda del tipo di rete sulla quale il trattamento è effettuato (isolata, privata o Internet), il titolare del trattamento deve implementare sistemi di protezione adeguati: firewall, sonde antintrusione o altri dispositivi (attivi o passivi) volti a garantire la sicurezza della rete.	**LA TRASMISSIONE DELLE IMMAGINI AVVENGONO ATTRAVERSO CANALI SICURI, PROTETTI DA VIRUS ATTRAVERSO ANTIVIRUS STANDARD.**
☐ Controllo degli accessi fisici Descrivere l'esistenza di un controllo degli accessi fisici ai locali che ospitano il trattamento (zonizzazione, accompagnamento di visitatori, assegnazione di badge, porte chiuse, e così via). Indicare se sono in atto procedure di allarme in caso di irruzione.	
☐ Tracciabilità di incidenti Descrivere l'esistenza di misure messe in atto per rilevare tempestivamente incidenti relativi a dati personali e disporre di elementi utilizzabili per studiarli o per fornire prove nel contesto di indagini (politica di registrazione eventi, rispetto degli obblighi di protezione dei dati ecc.)	
☒Sicurezza dell'hardware Descrivere l'esistenza di misure adottate per ridurre il rischio che le caratteristiche delle apparecchiature (server, postazioni fisse, portatili, periferiche, dispositivi di comunicazione, supporti rimovibili ecc.) siano utilizzate per danneggiare i dati personali (inventario, compartimentalizzazione, ridondanza, limiti per l'accesso ecc.)	**LA WORKSTATION È PROTETTA DA ANTIVISRUS E FIREWALL CON AGGIORNAMENTI AUTOMATICI PERIODICI.**
☐Prevenzione delle fonti di rischio Descrivere l'esistenza di misure per evitare che fonti di rischio, umane o	

non umane, anche se scarsamente probabili, arrechino pregiudizio ai dati personali (merci pericolose, aree geografiche pericolose, trasferimento dati al di fuori dell'UE, ecc.)	
☐ Protezione contro fonti di rischio non umane Descrivere l'esistenza di misure per ridurre o evitare i rischi connessi a fonti non umane (fenomeni climatici, incendi, danni provocati dall'acqua, incidenti interni o esterni, animali, ecc.) che potrebbero influire sulla sicurezza dei dati personali (misure preventive, di rilevamento, protezione, ecc.)	
☐Politica di tutela della privacy Descrivere l'esistenza di un'organizzazione idonea a guidare e verificare la protezione dei dati personali all'interno della struttura (designazione di un DPO/RPD, creazione di un organo di monitoraggio, ecc.)	
☐Gestione delle politiche di tutela della privacy Il titolare del trattamento deve disporre di una base documentale che formalizzi gli obiettivi e le regole da applicare nel campo della protezione dei dati (piano d'azione, revisione periodica delle politiche in materia di protezione dati, ecc.)	
☐Gestione dei rischi Descrivere l'esistenza di una politica che definisce i processi volti a controllare i rischi che i trattamenti comportano per i diritti e le libertà degli interessati (censimento dei trattamenti di dati personali, dei dati trattati, dei supporti utilizzati, valutazione del rischio, definizione di misure esistenti o previste ecc.)	
☐Integrare la protezione della privacy nei progetti Descrivere l'esistenza di procedure che descrivono i metodi volti a tenere conto della protezione dei dati personali in ogni nuovo trattamento (certificazioni, specifiche di riferimento, gestione del rischio per la persona interessata secondo una metodologia interna o indicata dall'autorità di controllo, ecc.)	

☐Gestire gli incidenti di sicurezza e le violazioni dei dati personali Descrivere l'esistenza di un'organizzazione operativa per rilevare e gestire eventi che possono influire sulle libertà e sulla riservatezza degli interessati (definizione delle responsabilità, piano di reazione, caratterizzazione delle violazioni ecc.)	
☐Gestione del personale Esistenza di un piano che preveda le misure di sensibilizzazione adottate al momento della presa in carico di un dipendente, e di una procedura che descriva le misure adottate una volta cessato il rapporto di lavoro con i soggetti che accedono ai dati.	
☐Gestione dei terzi che accedono ai dati Esistenza di una procedura volta a ridurre i rischi per le libertà e la vita privata degli interessati potenzialmente conseguenti all'accesso legittimo ai dati da parte di terzi (identificazione dei soggetti terzi, contratto di outsourcing, convenzione, BCR, ecc.)	
☐Vigilanza sulla protezione dei dati Descrivere l'esistenza di misure che consentano una visione globale e aggiornata dello stato di protezione dei dati e della conformità con il GDPR (verifica della conformità dei trattamenti, obiettivi e indicatori, responsabilità, ecc.).	

Fase 2: Valutazione della probabilità di incidente

FASE 2: Probabilità che si verifichi l'evento			
RETI E RISORSE TECNICHE			
D1	Il trattamento dei dati personali viene eseguito (parzialmente o totalmente) tramite Internet?	Quando il trattamento dei dati personali viene eseguito in tutto o in parte tramite Internet, aumentano le possibili minacce da parte di aggressori esterni online (ad esempio Denial of Service, SQL injection, attacchi Man-in-the-Middle), soprattutto quando il servizio è disponibile (e quindi, rintracciabile/noto) a tutti gli utenti di Internet.	SI
D2	Il trattamento dei dati personali può essere fatto da remoto?	Quando l'accesso a un sistema di elaborazione interna dei dati viene fornito tramite Internet, la probabilità di minacce esterne aumenta (ad esempio a causa di aggressori esterni online). Allo stesso tempo aumenta anche la probabilità di abuso (accidentale o intenzionale) dei dati da parte degli utenti (ad esempio divulgazione accidentale di dati personali quando si lavora in spazi pubblici).	SI

		Un'attenzione particolare dovrebbe essere prestata ai casi in cui è consentita la gestione/amministrazione remota del sistema IT.	
D3	Il trattamento dei dati personali è in condivisione con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	La connessione a sistemi IT esterni può introdurre ulteriori rischi legati alle minacce (e ai potenziali difetti di sicurezza) inerenti a tali sistemi. Lo stesso vale per i sistemi interni, tenendo conto che, se non opportunamente configurati, tali connessioni possono consentire l'accesso (ai dati personali) a più persone all'interno dell'organizzazione (che in linea di principio non sono autorizzate per tale accesso).	SI
D4	Esistono persone non autorizzate che possono accedere al trattamento dei dati personali?	Sebbene l'attenzione sia stata posta su sistemi e servizi elettronici, l'ambiente fisico (rilevante per questi sistemi e servizi) è un aspetto importante che, se non adeguatamente salvaguardato, può seriamente compromettere la sicurezza (ad esempio consentendo alle parti non autorizzate di accedere fisicamente alle apparecchiature IT e componenti di rete o non fornire protezione della sala computer in caso di disastro fisico).	NO
D5	Il sistema sottostante al trattamento dei dati personali non è aggiornato alle ultime tecnologie presenti sul mercato?	Componenti hardware e software mal progettate, implementate e/o mantenute possono comportare gravi rischi per la sicurezza delle informazioni. A tal fine, le buone o le migliori pratiche accumulano l'esperienza di eventi precedenti e possono essere considerate come linee guida pratiche su come evitare l'esposizione e raggiungere determinati livelli di resilienza.	NO
PROCESSI / PROCEDURE RELATIVI AL TRATTAMENTO DEI DATI			
D1	I ruoli e le responsabilità dei soggetti che si occupano del trattamento sono generici o non chiaramente definiti e circoscritti?	Quando i ruoli e le responsabilità non sono chiaramente definiti, l'accesso (e l'ulteriore elaborazione) dei dati personali può essere incontrollato, con conseguente uso non autorizzato delle risorse e compromissione della sicurezza complessiva del sistema.	NO
D2	Le regole di condotta inerenti alle procedure organizzative aziendali sono ambigue o non chiaramente definite?	Quando un uso appropriato delle risorse non è chiaramente definito, potrebbero sorgere minacce alla sicurezza a causa di incomprensioni o di un uso improprio intenzionale del sistema. La chiara definizione delle politiche per le risorse di rete, di sistema e fisiche può ridurre i potenziali rischi.	NO
D3	I dipendenti sono autorizzati a portare e a utilizzare fuori dal luogo di lavoro gli strumenti di lavoro necessari per connettersi al sistema di elaborazione dei dati personali?	I dipendenti che utilizzano i loro dispositivi personali all'interno dell'organizzazione potrebbero aumentare il rischio di perdita di dati o accesso non autorizzato al sistema informativo. Inoltre, poiché i dispositivi non sono controllati a livello centrale, possono introdurre nel sistema bug o virus aggiuntivi.	NO

D4	I dipendenti sono autorizzati a trasferire, archiviare o altrimenti elaborare dati personali al di fuori dei locali di lavoro?	L'elaborazione di dati personali al di fuori dei locali dell'organizzazione può offrire molta flessibilità, ma allo stesso tempo introduce rischi aggiuntivi, sia legati alla trasmissione di informazioni attraverso canali di rete potenzialmente insicuri (es. Reti Wi-Fi aperte), sia uso non autorizzato di queste informazioni.	NO
D5	Le attività di elaborazione e trattamento dei dati personali possono essere eseguite senza la creazione di log file (step di passaggio)?	La mancanza di adeguati meccanismi di registrazione (log) e monitoraggio può aumentare l'abuso intenzionale o accidentale di processi/procedure e risorse, con conseguente abuso di dati personali.	SI
PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI			
D1	Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	Quando l'accesso (e l'ulteriore elaborazione) dei dati personali è aperto a un gran numero di dipendenti, le possibilità di abuso a causa del fattore umano aumentano. Definire chiaramente chi ha realmente necessità di accedere ai dati e limitare l'accesso solo a quelle persone può contribuire alla sicurezza dei dati personali.	NO
D2	Qualche parte dell'operazione di trattamento dei dati è eseguita da soggetti terzi?	Quando l'elaborazione viene eseguita da soggetti esterni, l'organizzazione può perdere parzialmente il controllo su questi dati. Inoltre, possono essere introdotte ulteriori minacce alla sicurezza a causa delle minacce intrinseche a questi appaltatori. È importante che l'organizzazione selezioni gli appaltatori che possono offrire un elevato livello di sicurezza e definire chiaramente quale parte del processo è loro assegnata, mantenendo il più possibile un alto livello di controllo.	SI
D3	Gli obblighi delle parti/persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	Quando i dipendenti non sono chiaramente informati sui loro obblighi, le minacce derivanti da un uso improprio accidentale (ad es. Divulgazione o distruzione) di dati, aumentano in modo significativo.	NO
D4	Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	Quando i dipendenti non sono consapevoli della necessità di applicare le misure di sicurezza, possono causare accidentalmente ulteriori minacce al sistema. La formazione può contribuire notevolmente a sensibilizzare i dipendenti sia sui loro obblighi di protezione dei dati, sia sull'applicazione di specifiche misure di sicurezza.	NO
D5	Le persone/le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e/o distruggere in modo sicuro i dati personali?	Molte violazioni dei dati personali si verificano a causa della mancanza di misure di protezione fisica, come serrature e sistemi di distruzione sicura. I file cartacei sono solitamente parte dell'input o dell'output di un sistema informativo, possono contenere dati personali e devono anche essere protetti da divulgazione e riutilizzi non autorizzati.	NO
SETTORE COMMERCIALE E PORTATA DEL TRATTAMENTO			

D1	Ritieni che il tuo settore aziendale sia incline agli attacchi informatici?	Quando gli attacchi alla sicurezza si sono già verificati in uno specifico settore aziendale, indica che l'organizzazione probabilmente dovrà prendere ulteriori misure per evitare un evento simile.	SI
D2	La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	Se l'organizzazione è già stata attaccata o ci sono indizi che possa essere successo, è necessario prendere ulteriori misure per prevenire eventi simili in futuro.	NO
D3	Hai ricevuto notifiche e/o reclami riguardo alla sicurezza del sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	Bug di sicurezza/vulnerabilità possono essere sfruttati per eseguire attacchi (cyber o fisici) a sistemi e servizi. Si dovrebbero prendere in considerazione dei bollettini sulla sicurezza contenenti informazioni importanti relative alle vulnerabilità della sicurezza che potrebbero influire sui sistemi e sui servizi menzionati sopra.	NO
D4	Un'operazione di elaborazione riguarda un grande volume di interessati e/o dati personali?	Il tipo e il volume dei dati personali (circa >50 persone/dati personali) possono rendere l'operazione di elaborazione appetibile per gli aggressori (a causa del valore intrinseco di questi dati).	SI
D5	Esistono “buone prassi” di sicurezza specifiche per il tuo settore aziendale che non sono state adeguatamente seguite?	Le misure di sicurezza specifiche del settore sono solitamente adattate ai bisogni (e ai rischi) del particolare settore. La mancanza di conformità con le migliori pratiche pertinenti potrebbe essere un indicatore di scarsa gestione della sicurezza.	NO

In base al numero di risposte affermative ottenute, viene indicato, per ogni area di valutazione, il relativo punteggio.

AREA DI VALUTAZIONE	**PROBABILITÀ**	
	NUMERO DI SI	**PUNTEGGIO**
RETE E RISORSE TECNICHE	0 - 1	1
	2 - 3	2
	4 - 5	3
PROCESSI / PROCEDURE RELATIVI AL TRATTAMENTO DEI DATI PERSONALI	0 - 1	1
	2 - 3	2
	4 - 5	3
PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	0 - 1	1
	2 - 3	2
	4 - 5	3
SETTORE COMMERCIALE E PORTATA DEL TRATTAMENTO	0 - 1	1
	2 - 3	2
	4 - 5	3

Sommando i punteggi ottenuti dalle tabelle precedenti, si ottiene il livello di probabilità di accadimento della minaccia:

SOMMA COMPLESSIVA DEI PUNTEGGI	LIVELLO DI PROBABILITÀ DI ACCADIMENTO DELLA MINACCIA
4 - 5	Basso
6 - 8	Medio
9 - 12	Alto

Risultati della valutazione della probabilità di incidente

AREA DI VALUTAZIONE	NUM SI	PUNTEGGIO
RETI E RISORSE TECNICHE	3	1
PROCESSI / PROCEDURE RELATIVI AL TRATTAMENTO DEI DATI	1	1
PARTI / PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	1	1
SETTORE COMMERCIALE E PORTATA DEL TRATTAMENTO	2	2
	TOTALE	5
	LIVELLO	BASSO

Fase 3: Valutazione del danno sui diritti e libertà delle persone interessate

FASE 3: Valutazione del danno del trattamento		
		LIVELLO DI DANNO
Riservatezza/Confidenzialità	☒ Danno per la reputazione ☒ Discriminazione ☒ Furto d'identità ☐ Perdite finanziarie ☐ Danni fisici o psicologici ☒ Perdita di controllo dei dati ☐ Altri svantaggi economici e sociali ☐ Impossibilità di esercitare diritti, servizi o opportunità	**ALTO**
Integrità	☐ Danno per la reputazione ☐ Discriminazione ☐ Furto d'identità ☐ Perdite finanziarie ☐ Danni fisici o psicologici ☐ Perdita di controllo dei dati ☒ Altri svantaggi economici e sociali ☒ Impossibilità di esercitare diritti, servizi o opportunità	**ALTO**
Disponibilità	☐ Danno per la reputazione ☐ Discriminazione ☐ Furto d'identità ☐ Perdite finanziarie ☐ Danni fisici o psicologici	**ALTO**

	☐ Perdita di controllo dei dati ☒ Altri svantaggi economici e sociali ☒ Impossibilità di esercitare diritti, servizi o opportunità	
Valutazione Complessiva		**ALTO**

Tabelle riassuntive del rischio calcolato

TABELLA RIASSUNTIVA FASE 2 E 3	
Probabilità che si verifichi l'evento	BASSO
Livello di intensità del danno	ALTO

Livello di intensità del danno

Probabilità che si verifichi l'evento	BASSO	MEDIO	ALTO
ALTO			
MEDIO			
BASSO			**X**

3.2 Misure migliorative pianificate

☐ Crittografia Indicare i mezzi implementati per assicurare la confidenzialità dei dati archiviati (in database, file, backup ecc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di sospetta compromissione ecc.). Specificare i mezzi crittografici impiegati per i flussi di dati (VPN, TLS, ecc.) implementati nel trattamento.	
☐ Anonimizzazione Indicare qui i meccanismi di anonimizzazione implementati, le garanzie da essi introdotte contro l'eventuale reidentificazione e per quali finalità sono implementati.	
☐ Pseudonimizzazione Indicare i metodi utilizzati per il pseudonimizzazione del trattamento.	
☒ Controllo degli accessi logici Descrivere in che modo sono definiti e attribuiti i profili degli utenti. Specificare i mezzi di autenticazione implementati precisando, ove applicabile, le regole per le password (lunghezza minima, caratteri richiesti, durata	**I PROFILI DI ACCESSO DELLE IMMAGINI SONO GESTITI ATTRAVERSO PASSWORD GERARCHICHE, SARA' CURA DELLA COMMITTENZA ASSEGNARLE IN FUNZIONE DI UNA GERARCHIA DA LUI SCELTA.** **LA RESPONSABILITA' DI RESETTARE E/O CREARE UNA NUOVA UTENZA È IN CAPO SOLO ALL'AMMINISTRATORE DI SITEMA.**

della validità, numero di tentativi prima del blocco dell'account, ecc.).	**LE PASSWORD RISPONDONO ALLE ADEGUATE CARATTERISTICHE DI SICUREZZA. I TENATIVI CHE PRECEDONO AL BLOCCO SONO N. 4**
☒ Tracciabilità Descrivere le politiche che definiscono la tracciabilità degli eventi e la gestione dei relativi log.	**LO STRUMENTO IDONEO PER TRACCIARE I LOG PER GLI ACCESSI EFFETTUATI DAL COMUNE E DA NOI È LO STORICO EVENTI REGISTRATO DALLA MACCHINA. GLI ACCESSI SONO SEMPRE TRACCIABILI.**
☐ Archiviazione Descrivere le politiche di conservazione e gestione di archivi elettronici contenenti dati personali, finalizzate a tutelarne, in particolare, la validità giuridica per tutto il periodo necessario (versamento, conservazione, migrazione, accessibilità, eliminazione, politiche di archiviazione, protezione della confidenzialità, ecc.).	
☐Sicurezza dei documenti cartacei Descrivere le politiche relative ai documenti cartacei contenenti dati personali utilizzati nell'ambito del trattamento. Tali politiche descrivono come i documenti sono stampati, archiviati, distrutti e condivisi.	
☐Minimizzazione dei dati Descrivere i metodi utilizzati, come: filtraggio e rimozione, riduzione del potenziale identificativo attraverso trasformazione, riduzione della natura identificativa del dato, riduzione dell'accumulazione dei dati, limitazione dell'accesso ai dati	
☐ Vulnerabilità Descrivere le politiche volte a limitare la probabilità e la gravità dei rischi per le risorse utilizzate durante l'operatività (documentare le procedure operative, inventariazione e aggiornamento di software e hardware, correzione di vulnerabilità, duplicazione dei dati, limitazioni all'accesso fisico al materiale, ecc.).	
☐ Lotta contro il malware Descrivere le misure volte a proteggere l'accesso a reti pubbliche (Internet) o non controllate (di partner) nonché postazioni e server contro malware che potrebbe compromettere la sicurezza dei dati personali.	
☐Gestione postazioni	

Descrivere le misure adottate per ridurre la possibilità che le caratteristiche del software (sistemi operativi, applicazioni aziendali, software per ufficio, impostazioni ecc.) vengano sfruttate per danneggiare i dati personali (aggiornamenti, protezione fisica e accessi, lavoro su uno spazio di rete protetto, controlli di integrità, logging, ecc.).	
☐ Sicurezza dei siti web Descrivere i metodi e gli strumenti implementati per ridurre il rischio che le caratteristiche di un sito web siano sfruttate al fine di pregiudicare dati personali (disciplinare generale di sicurezza, cifratura TLS dei flussi di dati, politica di rilascio dei cookie, audit di sicurezza, ecc.) .	
☒Backup Descrivere le politiche di backup tali da assicurare la disponibilità e/o l'integrità dei dati personali, tutelandone la confidenzialità (periodicità dei backup, cifratura del canale di trasmissione dati, test di integrità, ecc.).	**LE IMMAGINI SONO SOTTOPOSTE A BACKUP** **NEL CASO DI INCEDENTE, I DATI PERSONALI POTREBBERO ESSERE RECUPERATI TEMPESTIVAMENTE.**
☒ Manutenzione Descrivere la politica di manutenzione fisica dei dispositivi, specificando l'eventuale ricorso all'outsourcing. Dovrà comprendere la manutenzione remota, ove autorizzata, e specificare i metodi di gestione dei materiali difettosi.	**L'IMPIANTO ESEGUE UNA DIAGNOSI AUTOMATICA ED E' PREVISTO UN INTERVENTO DEI TECNICI.**
☒Contratto con il responsabile del trattamento I dati personali comunicati a o gestiti da responsabili del trattamento devono beneficiare di garanzie sufficienti.	**IL TITOLARE HA FORNITO AL RESPONSABILE DEL TRATTAMENTO FORMALI INDICAZIONI CIRCA IL TRATTAMENTO DEI DATI PERSONALI, COME PREVISTO DALL'ART. 28 GDPR.**
☒ Sicurezza dei canali informatici A seconda del tipo di rete sulla quale il trattamento è effettuato (isolata, privata o Internet), il titolare del trattamento deve implementare sistemi di protezione adeguati: firewall, sonde antintrusione o altri dispositivi (attivi o passivi) volti a garantire la sicurezza della rete.	**LA TRASMISSIONE DELLE IMMAGINI AVVENGONO ATTRAVERSO CANALI SICURI, PROTETTI DA VIRUS ATTRAVERSO ANTIVIRUS STANDARD.**
☐ Controllo degli accessi fisici Descrivere l'esistenza di un controllo degli accessi fisici ai locali che ospitano il trattamento (zonizzazione, accompagnamento	

di visitatori, assegnazione di badge, porte chiuse, e così via). Indicare se sono in atto procedure di allarme in caso di irruzione.	
☐ Tracciabilità di incidenti Descrivere l'esistenza di misure messe in atto per rilevare tempestivamente incidenti relativi a dati personali e disporre di elementi utilizzabili per studiarli o per fornire prove nel contesto di indagini (politica di registrazione eventi, rispetto degli obblighi di protezione dei dati ecc.)	
☒Sicurezza dell'hardware Descrivere l'esistenza di misure adottate per ridurre il rischio che le caratteristiche delle apparecchiature (server, postazioni fisse, portatili, periferiche, dispositivi di comunicazione, supporti rimovibili ecc.) siano utilizzate per danneggiare i dati personali (inventario, compartimentalizzazione, ridondanza, limiti per l'accesso ecc.)	**LA WORKSTATION È PROTETTA DA ANTIVISRUS E FIREWALL CON AGGIORNAMENTI AUTOMATICI PERIODICI.**
☐Prevenzione delle fonti di rischio Descrivere l'esistenza di misure per evitare che fonti di rischio, umane o non umane, anche se scarsamente probabili, arrechino pregiudizio ai dati personali (merci pericolose, aree geografiche pericolose, trasferimento dati al di fuori dell'UE, ecc.)	
☐ Protezione contro fonti di rischio non umane Descrivere l'esistenza di misure per ridurre o evitare i rischi connessi a fonti non umane (fenomeni climatici, incendi, danni provocati dall'acqua, incidenti interni o esterni, animali, ecc.) che potrebbero influire sulla sicurezza dei dati personali (misure preventive, di rilevamento, protezione, ecc.)	
☐Politica di tutela della privacy Descrivere l'esistenza di un'organizzazione idonea a guidare e verificare la protezione dei dati personali all'interno della struttura (designazione di un DPO/RPD, creazione di un organo di monitoraggio, ecc.)	

☐Gestione delle politiche di tutela della privacy Il titolare del trattamento deve disporre di una base documentale che formalizzi gli obiettivi e le regole da applicare nel campo della protezione dei dati (piano d'azione, revisione periodica delle politiche in materia di protezione dati, ecc.)	
☐Gestione dei rischi Descrivere l'esistenza di una politica che definisce i processi volti a controllare i rischi che i trattamenti comportano per i diritti e le libertà degli interessati (censimento dei trattamenti di dati personali, dei dati trattati, dei supporti utilizzati, valutazione del rischio, definizione di misure esistenti o previste ecc.)	
☐Integrare la protezione della privacy nei progetti Descrivere l'esistenza di procedure che descrivono i metodi volti a tenere conto della protezione dei dati personali in ogni nuovo trattamento (certificazioni, specifiche di riferimento, gestione del rischio per la persona interessata secondo una metodologia interna o indicata dall'autorità di controllo, ecc.)	
☐Gestire gli incidenti di sicurezza e le violazioni dei dati personali Descrivere l'esistenza di un'organizzazione operativa per rilevare e gestire eventi che possono influire sulle libertà e sulla riservatezza degli interessati (definizione delle responsabilità, piano di reazione, caratterizzazione delle violazioni ecc.)	
☐Gestione del personale Esistenza di un piano che preveda le misure di sensibilizzazione adottate al momento della presa in carico di un dipendente, e di una procedura che descriva le misure adottate una volta cessato il rapporto di lavoro con i soggetti che accedono ai dati.	
☐Gestione dei terzi che accedono ai dati Esistenza di una procedura volta a ridurre i rischi per le libertà e la vita privata degli interessati potenzialmente conseguenti all'accesso legittimo ai dati da parte di terzi (identificazione dei soggetti terzi, contratto di outsourcing, convenzione, BCR, ecc.)	

☐Vigilanza sulla protezione dei dati Descrivere l'esistenza di misure che consentano una visione globale e aggiornata dello stato di protezione dei dati e della conformità con il GDPR (verifica della conformità dei trattamenti, obiettivi e indicatori, responsabilità, ecc.).	

3.3 Valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità

3.3.1. Valutazione della necessità del trattamento

Le finalità del trattamento sono state definite nell'apposito Regolamento approvato dal Consiglio Comunale.

I dati raccolti per determinati fini (ad esempio ragioni di sicurezza, tutela del patrimonio) non possono essere utilizzati per scopi diversi e/o ulteriori (ad esempio pubblicità, analisi dei comportamenti di consumo), salvo esigenze di polizia e di giustizia.

Infatti, è vietato utilizzare le immagini che, anche accidentalmente, dovessero essere assunte per finalità di controllo anche indiretto sull'attività professionale dei dipendenti, del rispetto dell'art. 4 della Legge 20 maggio 1970 n. 300 (Statuto dei Lavoratori).

Inoltre, le telecamere sono state installate in modo tale da limitare l'angolo visuale delle riprese quando non necessario, evitando immagini dettagliate, ingrandite o dettagli non rilevanti. L'iniziativa di adottare un sistema di videocontrollo è nata dall'esigenza di prevenire e reprimere efficacemente la commissione di atti criminosi all'interno del territorio del Comune, di dare un supporto al servizio di protezione civile, di aumentare la percezione e migliorare l'attuazione della sicurezza pubblica, nonché di controllare il traffico e di accertare eventuali infrazioni del Codice della Strada.

Il sistema informativo e i programmi informatici sono configurati riducendo al minimo l'utilizzazione dei dati personali e di dati identificativi. L'obiettivo è quello di procedere all'identificazione dell'interessato solo nei casi in cui siano rilevati degli illeciti anche attraverso il sistema automatico di lettura targhe.

I dati raccolti dalle videocamere sono conservati per un periodo non superiore a 7 giorni successivi alla rilevazione, fatte salve speciali e motivate esigenze di ulteriore conservazione, ed in modo particolare, in relazione ad illeciti che si siano verificati o ad indagini dell'Autorità Giudiziaria o di quella di Pubblica Sicurezza.

Si segnala, in particolare, che, da un punto di vista del traffico, il territorio comunale è attraversato da un'arteria stradale di notevole importanza livello nazionale ed internazionale: la Strada Statale n. 33 del Sempione E-62, che collega la rete autostradale italiana con quella svizzera.

Il Comune di Mergozzo, inoltre, è un territorio molto turistico, soprattutto nella stagione primaverile ed estiva.

È quindi un territorio di confine e turistico, con notevole ed importante traffico veicolare e transito di persone. Ne discende, pertanto, la necessità di effettuare un maggiore controllo.

La presenza di videocamere e dei cartelli segnalanti sarebbe, anzitutto, un valido deterrente alla commissione di illeciti e di reati. In un secondo momento, la registrazione delle immagini costituirebbe un valido ed efficace strumento di prova e di verifica del transito di veicoli e persone.

Il Comune di Mergozzo non avrebbe strumenti alternativi, in quanto sarebbe inattuabile l'impiego di personale di sorveglianza e di sicurezza h 24 su tutto il territorio comunale che si vuole controllare.

3.3.2. Valutazione della proporzionalità del trattamento

È necessario che l'attività di trattamento oggetto di valutazione sia proporzionata, in relazione alle finalità che si perseguono, rispetto ai diritti ed alle libertà degli interessati. A tal fine, il Comune si è premurato di informarli nella maniera più efficace del sistema di videosorveglianza, ponendolo nella condizione di conoscere ed esercitare i diritti privacy. Si indicano qui di seguito le misure adottate dal Titolare.

- ✓ La presenza delle videocamere è segnalata con apposita **cartellonistica**. Essa è stata posizionata all'accesso delle aree in cui sono concretamente posizionate le telecamere e comunque prima che i soggetti interessati entrino nel raggio di azione del sistema di videosorveglianza.
- ✓ Sul sito è stata pubblicata **l'informativa estesa** ex art. 13 GDPR, all'interno della quale sono esposti i diritti privacy ex art. 13 GDPR, nonché gli strumenti per esercitarli.
- ✓ All'interno della sezione privacy, è stato pubblicato il **modulo per esercitare i diritti privacy**.

Con riferimento alla richiesta per esercitare il diritto di accesso ai dati personali raccolti mediante un impianto di videosorveglianza, previsto dall'art. 15 del GDPR, essa 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.

La richiesta dev'essere inviata, entro il termine previsto per la cancellazione delle immagini, all'Ufficio responsabile della gestione dell'impianto di videosorveglianza Ufficio Polizia Locale che la valuterà al fine di procedere con la consegna del materiale. L'accoglimento della richiesta è vincolato alla condizione che non venga violato il diritto alla riservatezza di soggetti terzi.
Tutti i diritti previsti dagli artt. 15 e ss del GDPR 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 individua e rende note le modalità di trasmissione della richiesta all'interno di un'apposita sezione del sito web istituzionale.

Pertanto, il trattamento in esame può essere valutato adeguatamente necessario e proporzionato in relazione alle finalità che il titolare persegue legittimamente.

3.4 Parere del DPO e degli interessati

Parere del DPO:
Il sistema può essere implementato nella parte relativa alle misure di sicurezza poste a protezione dei dati personali, al fine di conformare il trattamento alle *Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*, emanate dall'EDPB.

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) È **necessario**, in quanto tale finalità non potrebbe essere raggiunta diversamente ed altrettanto efficacemente.

Storico revisioni

Rev. nr.	Oggetto	DATA	Pag. sostituite	Pag. aggiunte
0	**Prima emissione**			

Firme

NOME e COGNOME	RUOLO	FIRMA
Paolo Tognetti	**Il Titolare del trattamento - Sindaco del Comune di Mergozzo**	 Firmato digitalmente da: TOGNETTI PAOLO Firmato il 24/08/2023 16:51 Seriale Certificato: 1925939 Valido dal 17/11/2022 al 17/11/2025 InfoCamere Qualified Electronic Signature CA
Labor Service Srl	**Il Responsabile della Protezione dei dati personali**	Chiara Rittini