COMUNE DI LOIRI PORTO SAN PAOLO

Provincia Gallura Nord Est Sardegna

DATA PROTECTION IMPACT ASSESSMENT

Valutazione Impatto Privacy – Impianto Videosorveglianza

Nome della DPIA

IMPIANTO VIDEOSORVEGLIANZA COMUNALE

DATA CREAZIONE	Maggio 2026
DATA AGGIORNAMENTO	

Premessa

Scopo del documento

La DPIA si rende necessaria, a norma dell'art. 35, ogniqualvolta dal trattamento possa conseguire un rischio elevato per i diritti e le libertà delle persone interessate, anche durante un trattamento già in corso di esecuzione, qualora si verifichi un mutamento nelle finalità di quest'ultimo o una modifica dei dati stessi che comporti **una maggiore percentuale di rischio**.

La valutazione di impatto privacy è necessaria nel caso di sistemi integrati – sia pubblici, sia privati – che collegano telecamere tra soggetti diversi, o nel caso di sistemi intelligenti, capaci di analizzare le immagini ed elaborarle, per rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli. È il caso, soprattutto della videosorveglianza pubblica, che consente la visione delle immagini a soggetti diversi e che si avvalgono di appositi software per l'analisi delle immagini e per il lancio degli allarmi in caso di riscontrate anomalie.

La valutazione d'impatto sulla protezione dei dati è sempre richiesta, in particolare, in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico (articolo 35, paragrafo 3, lettera c) del GDPR) e negli altri casi indicati dal Garante con il provvedimento 467 dell'11 ottobre 2018. In quest'ultima deliberazione, l'Autorità Garante per la Privacy ha individuato un elenco delle tipologie di trattamenti, comunque non esaustivo, da sottoporre a valutazione d'impatto.

Il modello della presente DPIA è stato estratto, senza rielaborazioni sostanziali, dallo strumento PIA (valutazione di impatto sulla protezione dei dati) progettato dalla Commission Nationale de l'Informatique et des Libertés (CNIL v. 2.3.0), autorità di controllo francese, esplicitamente validato e suggerito anche dal Garante per la protezione dei dati personali italiano.

Definizioni, acronimi e abbreviazioni

Espressione/Acronimo	*Definizione/Significato*
Servizio	Utilizzo degli impianti di videosorveglianza attivati nel territorio del Comune di LOIRI PORTO SAN PAOLO

Espressione/Acronimo	*Definizione/Significato*
Titolare del trattamento	Ovvero anche solo "Titolare" è secondo l'art. 4 GDPR "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali". Nel contesto di questo documento, il titolare è il **Comune di Loiri Porto San Paolo**, cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali
Responsabile del trattamento	Soggetto/Azienda Fornitrice del servizio/ manutenzione, nominata Responsabile del trattamento ai sensi dell'art. 28 del Reg. UE 2016/679
Interessato	La persona fisica cui si riferiscono i dati personali oggetto di trattamento. Trattasi di una persona fisica identificata ovvero identificabile in modo diretto o indiretto

Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come ad esempio la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (GDPR, Articolo 4, Comma 2).
Rischio	Nel contesto del presente documento, il prodotto tra la probabilità di ledere i diritti e le libertà delle persone fisiche a cui i dati personali trattati si riferiscono e l'impatto su tali diritti e libertà che si verrebbe a produrre per l'interessato ove l'evento temuto (c.d. "minaccia") si dovesse verificare.
DPIA/PIA	Data Protection Impact Assessment (Valutazione d'Impatto sulla protezione dei dati)
GDPR/Reg. UE 2016/679	General Data Protection Regulation. REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

Gli elementi oggetto della presente DPIA sono:

A. **CONTESTO:** (PANORAMICA DEL TRATTAMENTO – DATI, PROCESSI e RISORSE di SUPPORTO
B. **PRINCIPI FONDAMENTALI:** (PROPORZIONALITÀ e NECESSITÀ)
C. **MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI**
D. **MISURE SICUREZZA ESISTENTI**
E. **RISCHI** (ACCESSO ILLEGITIMO AI DATI - MODIFICHE INDESIDERATE DEI DATI - PERDITE DEI DATI

CONTESTO

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza (VDS) attivati nel territorio del Comune di Loiri Porto San Paolo avviene da parte del Titolare e dei soggetti specificatamente designati-autorizzati.

Le finalità di utilizzo degli impianti di videosorveglianza sono conformi alle funzioni istituzionali attribuite al Comune dalla legge 7 marzo 1986, n. 65 sull'ordinamento della Polizia Municipale, dallo statuto e dai regolamenti comunali, dalla direttiva Polizia 2016/680 attuata con decreto lgs. 18 maggio 2018, n. 51 nonché dal decreto-legge n. 14 del 20

febbraio 2017 convertito in legge n. 48 del 13 aprile 2017 “disposizioni urgenti in materia di sicurezza delle città” e successive modificazioni ed integrazioni e dalle altre disposizioni normative applicabili al Comune, e recepito nella delibera del Consiglio Comunale n°12 del 01.04.2026 di approvazione del Regolamento comunale per la disciplina e l’utilizzo di impianti di videosorveglianza.

Il trattamento dei dati personali mediante sistemi di videosorveglianza è effettuato allo scopo di:

a) incrementare la sicurezza urbana e la sicurezza pubblica nonché la percezione delle stesse rilevando situazioni di pericolo e consentendo l’intervento degli operatori;
b) prevenire, accertare e reprimere gli atti delittuosi, le attività illecite e gli episodi di microcriminalità commessi sul territorio comunale e quindi ad assicurare maggiore sicurezza ai cittadini nell’ambito del più ampio concetto di “sicurezza urbana” già richiamato; le informazioni potranno essere condivise con altre forze di Polizia competenti a procedere nei casi di commissione di reati;
c) tutelare gli immobili di proprietà o in gestione dell’Amministrazione Comunale e gli edifici pubblici e a prevenire eventuali atti di vandalismo o danneggiamento;
d) controllare le aree considerate a maggiore rischio per la sicurezza, l’incolumità e l’ordine pubblico;
e) al monitoraggio del traffico;
f) attivare uno strumento operativo di protezione civile sul territorio comunale;
g) ad acquisire elementi probatori in fattispecie di violazioni amministrative o penali;
h) 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;
i) monitorare il rispetto delle disposizioni concernenti, modalità, tipologia ed orario di deposito dei rifiuti;
j) verificare l’osservanza di ordinanze e/o regolamenti comunali al fine di consentire l'adozione degli opportuni provvedimenti;

Quali sono le responsabilità connesse al trattamento?

La presente analisi garantisce che il trattamento dei dati personali, effettuato mediante l’attivazione di un sistema VDS operante nel territorio del Comune di Liori Porto San Paolo, si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all’identità personale; garantisce, altresì, i diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento, avuto riguardo anche alla libertà di circolazione nei luoghi pubblici o aperti al pubblico. La presente valutazione di impatto viene svolta in quanto si intende valutare i rischi associati al trattamento, le misure identificate per attenuarli al fine di evitare che il trattamento effettuato mediante l'utilizzo dello strumento tecnologico messo a disposizione possa, potenzialmente, ledere i diritti e le libertà degli interessati ai quali i dati si riferiscono.

Le responsabilità del trattamento sono connesse alle funzioni e ruoli come specificate nel regolamento comunale VDS (artt. 6-7-8-9):

- ✓ il Titolare del trattamento è il Sindaco pro tempore;
- ✓ Il Designato al trattamento è nominato dal Titolare nella figura del Responsabile dell’Area Vigilanza;
- ✓ Gli Autorizzati al trattamento dei dati sono previsti e incaricati dal Designato;
- ✓ Se formalmente nominato, possono essere nominati come responsabili esterni del trattamento 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 dell’impianto di videosorveglianza nel caso in esame.

Ci sono standard applicabili al trattamento?

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

- Provvedimento generale in materia di videosorveglianza in ambito pubblico e privato del 08 aprile 2010 del Garante della protezione dei dati personali (G.U. n. 99 del 29/04/2010);
- Linee guida sulla Videosorveglianza negli enti locali dell'ANCI del 09 novembre 2010;
- Circolare del Ministero dell'Interno inerente i Sistemi di videosorveglianza e relative specifiche tecniche per i Comuni del 02 marzo 2012 e successive indicazioni;
- Regolamento UE Generale sulla Protezione dei Dati 2016/679 relativo "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" (anche "RGPD/GDPR");
- Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali" some modificato ed integrato dal D. Lgs 101/2018;
- Allegato 1 al provvedimento n. 467 dell'11 ottobre 2018, pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018, inerente all'elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto del Garante della protezione dei dati personali;
- Direttiva UE 2016/680 relativa "alla protezione delle persone fisiche con riguardo al trattamento dei dati
- personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio", recepita con il D.lgs. 51/2018;
- riferimento agli articoli 7 del D.lgs. 51/2018 (sul trattamento di categorie particolari di dati personali), 6 c. 7 del D.L. 11/2009 (sule Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori") e 54 del D.lgs. 267/2000 (Testo Unico Enti Locali);
- DPR del 15 gennaio 2018, n. 15, recante "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia";
- Decreto-legge 20 febbraio 2017, n. 14, convertito, con modificazioni, dalla legge 18 aprile 2017, n. 48, recante "Disposizioni urgenti in materia di sicurezza delle città" e successive modificazioni ed integrazioni del D.L. 14.06.19 n. 53 convertito con modifiche con L. 8 agosto 2019 n. 77.
- Linee guida 03/2019 v.2 del 29 gennaio 2020 pubblicate dall'EDPB, inerenti al trattamento di dati personali attraverso dispositivi video;
- Le regole per installare telecamere del 05 dicembre 2020, il vademecum e le FAQ in materia di videosorveglianza del 03 dicembre 2020 del Garante della protezione dei dati personali.;
- Regolamento Comunale sulla Videosorveglianza approvato con delibera Consiglio Comunale n°12/2026

Dati, processi e risorse di supporto

Quali sono i dati trattati?

L'impianto di VDS consente riprese video, diurne e notturne, in condizioni sufficienti di illuminazione naturale ed artificiale, riprende e registra immagini che permettono di identificare in modo diretto o indiretto le persone e sono installati nel territorio dell'Ente. Le videocamere possono essere sia fisse che mobili. I dati che vengono trattati fanno

riferimento a persone fisiche; al possesso di beni e proprietà; alle caratteristiche fisiche; abitudini; al comportamento, alla posizione geografica. Inoltre, sono trattati i dati degli autoveicoli (n. targa). L'impianto è sempre in funzione ed è configurato per la registrazione continuativa.
Le informazioni inerenti al numero delle telecamere, luogo di installazione, alle caratteristiche tecniche dell'impianto, si rimanda alle tabelle inserite nella presente DPIA.
Le videocamere consentono riprese video e sono collegate a 3 stanze server dislocate in Loiri, Porto San Palo e Porto Taverna, dove vengono trasmesse ponte radio anche le riprese effettuate in località Stagno e Porto Faro. Le immagini sono visualizzate in tempo reale su monitor da personale designato/autorizzato. Il sistema è a circuito chiuso, senza possibilità di accesso da remoto. Il salvataggio avviene su server dedicati senza possibilità di accesso da remoto.

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

Il ciclo di vita dei dati prevede i seguenti trattamenti:

a) acquisizione, b) registrazione, c) organizzazione, d) conservazione, e) consultazione, f) raffronto, g) interconnessione, h) limitazione, i) pseudonimizzazione, l) estrazione

Le immagini videoregistrate sono conservate: per il periodo ordinariamente **non superiore a 7 giorni successivi alla rilevazione**, che possono essere estesi, tenuto conto delle esigenze specifiche e documentate di indagine e di prevenzione dei reati, in particolare su esplicita richiesta dell'Autorità. L'estensione dei tempi di conservazione, devono essere sostenute da specifiche ed evidenti esigenze investigative e di polizia giudiziaria nonché specifiche richieste da parte dell'Autorità prefettizia e giudiziaria, tenuto conto di eventuali ulteriori necessità di conservazione in caso di ricorsi;

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

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

Quali sono le risorse di supporto ai dati?

Persone:

1) Sindaco/Titolare;
2) Personale interno Designato ed Autorizzato ed adeguatamente formato.
3) Responsabile "esterno" nominato ex art 28 GDPR (manutenzione)
4) Responsabile Protezione dei dati/DPO

Possono essere autorizzati all'accesso alla sala di "controllo" solo il personale designato ed autorizzato espressamente dal Titolare e per scopi connessi alle finalità individuate nel regolamento comunale, nonché il personale addetto alla manutenzione degli impianti nominato ex art 28 GDPR ed alla pulizia dei locali, preventivamente individuato dal titolare o dal designato al trattamento.
L'accesso alla sala, da parte di soggetti diversi da quelli indicati sopra è subordinato al rilascio, da parte del Titolare o del designato, di un'autorizzazione scritta, motivata e

corredata da specifiche indicazioni in ordine ai tempi ed alle modalità dell'accesso. L'accesso avviene in presenza di designati od autorizzati del Comune; dell'avvenuto accesso si dà menzione nel registro degli accessi.
Gli autorizzati al trattamento e i preposti sono gli unici dotati di proprie credenziali di autenticazione di accesso al sistema. Il sistema è fornito di "log" di accesso*. Infatti, l'accesso ai sistemi che gestiscono i dati oggetto dello specifico trattamento, può essere effettuato esclusivamente da operatori muniti di credenziali di accesso valide e strettamente personali, rilasciate su disposizione del designato del trattamento come individuato.

*L'accesso ai sistemi di registrazione prevede l'adozione di sistemi idonei alla registrazione degli accessi logici degli autorizzati/designati e delle operazioni compiute sulle immagini registrate, compresi i relativi riferimenti temporali, con conservazione per un periodo di tempo congruo all'esercizio dei doveri di verifica periodica dell'operato dei designati da parte del titolare, comunque non inferiore a sei mesi.

Le immagini rilevanti ogni sorta di infrazione o reato vengono scaricate in locale attraverso il dispositivo di memoria di massa e messe a disposizione in caso di necessità agli organismi giudiziari.

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento dei dati personali, acquisiti mediante l'impianto di VDS si svolge nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. L'utilizzo dell'impianto comporta esclusivamente il trattamento di dati personali rilevati mediante le riprese video che, in relazione ai luoghi di installazione delle telecamere, interessano i soggetti ed i mezzi di trasporto che transitano nell'area oggetto di sorveglianza.

Quali sono le basi legali che rendono lecito il trattamento?

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

In ossequio al disposto di cui sopra, il trattamento dati è effettuato dal Comune esclusivamente per lo svolgimento delle funzioni istituzionali.

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

Principio di necessità - 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, rispettivamente, 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 rimpiegare solo i dati anonimi, con riprese di insieme e, il software utilizzato deve preventivamente essere impostato per cancellare periodicamente ed autonomamente i dati registrati.

Principio di proporzionalità - La raccolta e l'uso delle immagini devono essere proporzionali agli scopi perseguiti. In applicazione dei principi di proporzionalità e di necessità, nel procedere alla commisurazione tra la necessità del sistema di videosorveglianza ed il grado di rischio concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra un'effettiva esigenza di deterrenza. Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi. La proporzionalità va valutata in ogni fase o modalità del trattamento.

Nell'uso delle apparecchiature volte a riprendere, per i legittimi interessi indicati, aree esterne ed edifici, il trattamento deve essere effettuato con modalità tali da limitare l'angolo di visuale all'area effettivamente da proteggere.

Principio di finalità - Ai sensi dell'art. 5, Paragrafo 1, lett. b), RGPD, i dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che ciò non sia incompatibile con tali finalità. E' consentita pertanto la videosorveglianza come misura complementare volta a migliorare e garantire la sicurezza urbana che il DM Interno 05/08/2008 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."

I dati sono esatti e aggiornati?

I dati, essendo fotografia del reale, sono esatti e aggiornati per loro natura e non manomissibili.

Qual è il periodo di conservazione dei dati?

I dati personali registrati mediante l'utilizzo dell'impianto di VDS di cui alla presente analisi sono conservate per il periodo ordinariamente non superiore a 7 giorni successivi alla rilevazione, che possono essere estesi tenuto conto delle esigenze specifiche e documentate di indagine e di prevenzione dei reati. L'estensione dei tempi di conservazione devono essere sostenute da specifiche ed evidenti esigenze investigative e di polizia giudiziaria nonché specifiche

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati sono informati mediante:

a) pubblicazione del regolamento comunale elaborato e adottato dall'Ente;

b) installazione di apposita segnaletica permanente, contenente l'informativa breve, nelle aree in cui sono concretamente posizionate le telecamere;

c) informativa completa, contenente gli elementi di cui agli articoli 13-22 del GDPR, disponibile agevolmente e senza oneri per gli interessati, sul sito web e nei locali dell'Ente.

La segnaletica viene collocata prima del raggio di azione di ogni telecamera, o nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; la stessa è predisposta in modo da avere un posizionamento chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di VDS sia eventualmente attivo in orario notturno.

L'informativa di cui sopra non è dovuta nel caso di utilizzo di telecamere a scopo investigativo a tutela dell'ordine e sicurezza pubblica, prevenzione, accertamento o repressione di reati.

Ove applicabile: come si ottiene il consenso degli interessati?

Considerato che il Titolare del trattamento è una pubblica amministrazione che eroga servizi pubblici legalmente attribuiti, non è tenuto all'acquisizione del consenso al trattamento dei dati.

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

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

- di ottenere dal Titolare del trattamento, la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi;
- ad essere informato sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali;
- di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 del GDPR, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21 del GDPR.

L'istanza per l'esercizio dei diritti, da parte dell'interessato, è presentata al Titolare o al Designato dell'Ente e può essere presentata mediante lettera raccomandata inoltrata all'indirizzo del Titolare ovvero mediante PEC al seguente indirizzo:

- protocollo.loiriportosanpaolo@legalmail.it

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

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

Il Designato/Autorizzato, avrà cura di accertare l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; in caso di accertamento positivo, fisserà il giorno, l'ora ed il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano.

Qualora l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, ai sensi dell'art. 15 par. 3 del GDPR, si procederà al rilascio dei files contenenti le immagini, in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della ripresa (art. 15 par. 4 del GDPR).
I diritti come sopra esplicitati, riferiti ai dati personali concernenti persone decedute, possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato per ragioni familiari meritevoli di protezione.
Nell'esercizio dei diritti, l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti associazioni od organismi. L'interessato potrà altresì farsi assistere da persona di fiducia.

Qualora non sia possibile identificare l'interessato (o in caso di richieste eccessive o manifestamente infondate) il designato – previa adeguata motivazione ed entro i termini di 7 giorni dalla richiesta – informerà l'interessato dell'impossibilità di dare seguito alla richiesta.

In caso di esito negativo all'istanza dell'interessato, quest'ultimo potrà rivolgersi al Garante della protezione dei dati personali per il reclamo, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Al fine di:
−non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;
−non compromettere l'attività di prevenzione, indagine, accertamento e perseguimento di reati o l'esecuzione di sanzioni penali;
−proteggere la sicurezza pubblica;
−proteggere la sicurezza nazionale;
potranno essere adottate misure amministrative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato e per il tempo in cui ciò costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessai della persona fisica interessata.

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

In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo.

Per esercitare il diritto alla cancellazione, se possibile in ragione dell'obbligo dell'Ente di conservazione delle informazioni, gli interessati possono contattare direttamente il Titolare del trattamento/il Designato, recandosi direttamente presso l'Ente, mediante invio di raccomandata ovvero di posta certificata, ai canali di contatto indicati dal Titolare all'interno dell'informativa.

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

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

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

Il rapporto di responsabilità tra il Titolare ed il responsabile della manutenzione/gestione tecnica è definito e disciplinato da un contratto di appalto dei relativi servizi e regolamentato con apposito atto di nomina. Gli obblighi derivanti dal trattamento incidentale dei dati trattati mediante l'utilizzo dell'impianto, sono disciplinati in apposito allegato per la nomina conforme alle disposizioni previste dall'art. 28 Reg. UE 2016/679.

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

I dati non vengono trasferiti al di fuori dello spazio
SEE

MISURE ESISTENTI O PIANIFICATE

Anonimizzazione

I dati c.d. "particolari" ex art 9 GDPR, eventualmente rilevati, vengono trattati in maniera riservata unicamente dal personale strettamente necessario e a questo autorizzato. I dati oggetto di trattamento vengono resi sempre anonimi.

Controllo degli accessi logici e tracciabilità

- Individuazione di postazione informatica dedicata dotata di username e password personale di accesso per ogni operatore (unico e tracciabile);
- il software prevede la registrazione e conseguente tracciabilità degli accessi logici e delle operazioni effettuate dagli autorizzati al trattamento dei dati.
- Assegnazione, ad uso esclusivo, di una credenziale di autenticazione agli operatori;
- Aggiornamento periodico delle credenziali di autenticazione;
- Attivazione di uno screensaver automatico, dopo pochi minuti di non utilizzo, con inserimento password per la prosecuzione del lavoro;
- Disattivazione delle credenziali di autenticazione nel caso di inutilizzo perdurato ovvero in caso di perdita di qualità di autorizzato/designato.

Sicurezza dei documenti cartacei

I documenti cartacei vengono conservati dal Designato/autorizzato in appositi armadi chiusi a chiave ed in conformità a quanto previsto dalle procedure aziendali di riferimento, in maniera tale da garantire la riservatezza e la non visibilità a terzi non autorizzati.

Protezione di sicurezza informatiche (malware e vulnerabilità)

- Installazione e aggiornamento periodico di sistemi antivirus e antimalware;
- Aggiornamento costante dei software utilizzati;
- Utilizzo di un sistema Firewall sugli elaboratori ed aggiornamento periodico;
- Utilizzo di filtro anti-spam ed aggiornamento periodico;
- Divieto di scaricare software e di installare programmi da siti poco attendibili o non ufficiali;
- Reinstallazione dei programmi danneggiati o distrutti.

La memorizzazione delle immagini avviene su server dislocati in locali comunali (Municipio di Loiri – Locali Comunali Porto San Paolo e Porto Taverna) dedicati e protetto da rack dotati di serrature di sicurezza.

Minimizzazione dei dati

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

Archiviazione e Backup

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

Controllo degli accessi fisici

- Gli accessi fisici agli uffici sono limitati e controllati;
- Chiavi dei locali custodite dal solo personale Designato ed autorizzato (Polizia Municipale;
- Server custodito in armadio dedicato dotato di serratura.

Sicurezza dell'hardware e prevenzione delle fonti di rischio - Manutenzione

- Manutenzione programmata degli strumenti;
- Distruzione di tutti i supporti removibili non utilizzati;
- Misure antincendio ed estintori e loro revisione periodica;
- Accordo di assistenza continuativa con ditta di sicurezza;
- Manutenzione costante impianti e apparecchiature elettriche ed elettroniche;
- Monitoraggio e impegno della direzione nel controllo delle regole in materia di salute e sicurezza sui luoghi di lavoro.

Politica di tutela della privacy

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

- Formazione sugli aspetti principali della GDPR;
- Istruzioni ai designati ed agli autorizzati, finalizzate al controllo e alla custodia dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento senza l'ausilio di strumenti elettronici;
- Istruzioni in merito alla protezione dello strumento elettronico in caso di assenza temporanea durate le sessioni di lavoro;
- Istruzioni in merito alla segretezza e alla custodia delle credenziali di autenticazione;
- Istruzioni in merito all'accesso agli archivi digitali;
- Istruzioni organizzative e tecniche per la custodia dei supporti removibili su cui sono memorizzati i dati;
- Aggiornamento periodico o al verificarsi di eventuali modifiche della lista degli incaricati e dei profili di autorizzazione;
- Definizione di responsabilità e sanzioni disciplinari;
- Controllo degli accessi ai dati e programmi;
- Controllo sull'operato degli addetti alla manutenzione;

- Definizione di procedure per le copie di sicurezza, la loro custodia e il ripristino dei dati;
- Monitoraggio continuo delle sessioni di lavoro;
- Nomina Responsabile Protezione Dati/DPO

Misure di sicurezza specifiche videosorveglianza

Ai sensi di quanto previsto dall'art. 24 del GDPR, i dati personali acquisiti mediante l'impiego dell'impianto VDS sono protetti da misure di sicurezza tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato e trattamento non consentito o non conforme alle finalità del presente documento. Il Titolare del trattamento, previa valutazione dei rischi mette in atto misure volte a:

Il sistema di registrazione supporta tutte le funzionalità previste dalla normativa ed è dimensionato con adeguata capacità per il supporto di tutte le telecamere previste oltre ad una futura espansione sia in termini di funzionalità che di prestazioni e capacità di memorizzazione su supporti ridondati.

Le specifiche tecniche delle telecamere sono conformi alle normative europee cosi come da relazioni allegate

- Il trasporto delle immagini avviene su link protetti. La rete dedicata alla Videosorveglianza è isolata dalle altre reti di comunicazione attraverso apparati dedicati o VLAN dedicate.
- La memorizzazione delle immagini avviene su server dislocati in locali dedicati e protetti da rack dotati di serrature di sicurezza.
- L'accesso alla sala controllo e relativi terminali di visualizzazione è limitato e regolamentato attraverso le politiche dettate dall'Amministrazione al solo personale designato ed autorizzato.
- L'accesso alle funzioni del sistema di videosorveglianza è strutturato per livelli di autorizzazione e protetto da password nominative rilasciate al solo personale designato ed autorizzato.
- Le aree videosorvegliate sono adeguatamente segnalate attraverso i cartelli informativi secondo il modello previsto dal Codice della privacy

Inoltre sono state adottate istruzioni e misure di sicurezza al fine di:

- impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate ("controllo dei supporti di dati");
- impedire che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione ("controllo della conservazione");
- impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati ("controllo dell'Utente") e garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso ("controllo dell'accesso ai dati");
- garantire la possibilità di verificare e accertare gli organismi ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione dei dati ("controllo della trasmissione");
- garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata ("controllo dell'introduzione");

- impedire che i dati personali possano essere letti, copiati o cancellati in modo non autorizzato;
- garantire la sicurezza durante i trasferimenti di dati personali o il trasporto di supporti di dati (“controllo del trasporto”);
- garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati (“recupero”);
- garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati (“affidabilità”) e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema (”integrità”).

RISCHI

Accesso illegittimo ai dati

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

Diffusione non autorizzata, intercettazione di informazioni in rete, pregiudizio alla reputazione.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Abuso di privilegi, accesso non autorizzato ai sistemi aziendali per operazioni non consentite/non autorizzate, furto nei locali aziendali, vulnerabilità degli assets, azione di virus informatici o di programmi suscettibili di recare danno, distruzione totale o parziale e/o diffusione non autorizzata e/o inibizione dell'accesso ai dati, spamming o tecniche di sabotaggio.

Quali sono le fonti di rischio?

Fonti di rischio interne ed esterne anche non umane come attacchi informatici, virus e malware.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici e tracciabilità; Sicurezza dei documenti cartacei; Protezione contro i malware e vulnerabilità; Crittografia; Minimizzazione dei dati; Controllo degli accessi fisici; Manutenzione; Sicurezza dei canali informatici, Politica di tutela della privacy; Misure di sicurezza specifiche.

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

In considerazione dei dati oggetto di trattamento, il rischio individuato è da considerarsi

BASSO

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

LIMITATO

Modifiche indesiderate dei dati

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

Alterazione dei dati, negazione dell’accesso a servizi, pregiudizio alla reputazione.

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

Accesso ai dati da parte di soggetti non autorizzati e/o accesso ai dati per trattamenti non consentiti, sottrazione di credenziali di autenticazione, accesso ai dati da parte di soggetti in orari non consentiti, errore umano, carenza di consapevolezza, disattenzione, incuria o indisponibilità, comportamenti contrari ai principi di sicurezza e protezione dei dati,

comportamenti sleali o fraudolenti, operazioni accidentali non consentite e/o contrarie ai principi di sicurezza e protezione dei dati.

Quali sono le fonti di rischio?

Utenti interni ed esterni all'organizzazione, attacchi informatici.

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

Controllo degli accessi logici e tracciabilità; Protezione contro i malware e vulnerabilità; Crittografia; Minimizzazione dei dati; Archiviazione e back-up; Controllo degli accessi fisici; Sicurezza dei canali informatici, Politica di tutela della privacy; Misure di sicurezza specifiche.

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

In considerazione dei dati oggetto di trattamento, il rischio individuato è da considerarsi

BASSO.

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

LIMITATO

Perdita di dati

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

Indisponibilità dei dati, danno reputazionale.

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

Errori umani nella gestione della sicurezza fisica, eventi distruttivi, naturali o artificiali, nonché dolosi, accidentali o dovuti ad incuria, malfunzionamento, guasti, eventi naturali, alterazioni delle trasmissioni, indisponibilità o degrado degli strumenti, guasto ai sistemi complementari, sottrazione di strumenti contenenti dati, comportamenti sleali o fraudolenti, errore materiale, sottrazione di credenziali di autenticazione, azione di virus informatici o di programmi suscettibili di recare danno.

Quali sono le fonti di rischio?

Utenti e esterni all'organizzazione, attacchi informatici, eventi calamitosi, malfunzionamenti.

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

Controllo degli accessi logici e tracciabilità; Protezione contro i malware e vulnerabilità; Crittografia; Minimizzazione dei dati; Archiviazione e back-up; Controllo degli accessi fisici; Sicurezza dell'hardware e prevenzione delle fonti di rischio; Sicurezza dei canali informatici, Politica di tutela della privacy; Misure di sicurezza specifiche.

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

In considerazione dei dati oggetto di trattamento, il rischio individuato è da considerarsi

BASSO

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

LIMITATO

INFORMAZIONI sul POSIZIONAMENTO del SISTEMA DI VIDEOSORVEGLIANZA – Specifiche d'Impianto e Infrastruttura di Rete di Loiri e Porto San Paolo.

Si fa riferimento alla relazione di ITM Telematica del 26 gennaio 2026, relativamente a Porto Taverna vedi relazione HOME TEACH Domotica del 15.09.2026

LOIRI

NVR	Hikvision DS-7732	Municipio
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Municipio (Viale Dante DX)
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Municipio (Viale Dante SX)
Encoder	Hikvision DS-6704	Municipio
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Cortile Scuola Elementare
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Cortile Palestra
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Retro Palestra
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Ecocentro
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Ingresso Scuola Materna
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Parco Giochi Scuola Materna
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Incrocio SP24
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Incrocio SP24
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Incrocio SP24
Telecamera	Dahua	Ecocentro
Telecamera	Dahua	Municipio (Ing. Manutentori)
Telecamera	Hikvision DS-2CD63C5G0-IVS	Municipio (lato destro)
Telecamera	Hikvision DS-2CD63C5G0-IVS	Cimitero
Telecamera	Hikvision DS-2CD63C5G0-IVS	Municipio (lato sinistro)

PORTO SANPAOLO

nr. 1 Server di Registrazione a 32 canali

NVR	Hikvision DS-7732	Municipio	
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	SS125 Dir. S.Teodoro	
Telecamera	Hikvision DS-2CD63C5G0-IVS	Porto	
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Municipio (V.le Nenni DX)	
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Municipio (V.le Nenni SX)	
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Municipio (Retro DX)	
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Municipio (Retro SX)	
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Ingresso Scuola Media	

Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Ingresso Scuola Elementare	
Telecamera LT	Hikvision DS-2CD 403	Incrocio SS125 Dir. S.Teodoro	
Telecamera	Hikvision DS-2CD4A26FWD-ISZ	Incrocio SS125 Dir. Olbia	
Encoder	Hikvision DS-6704	Municipio	

PORTO TAVERNA (relazione Home Teach del 15.09.2026)

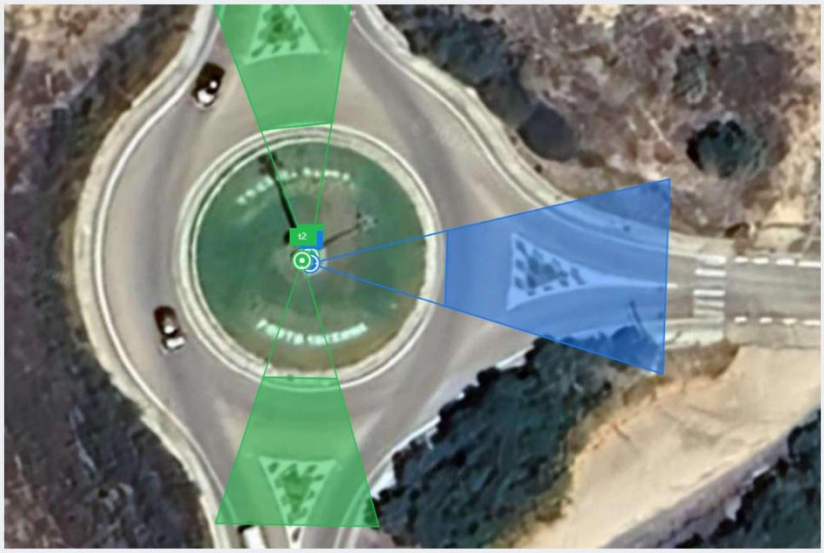
N° 1 server di registrazione NVR DHI-NVR 5432-XI 32 canali

Parcheggio Mare per la collocazione vedi foto in relazione allegata Home Teach

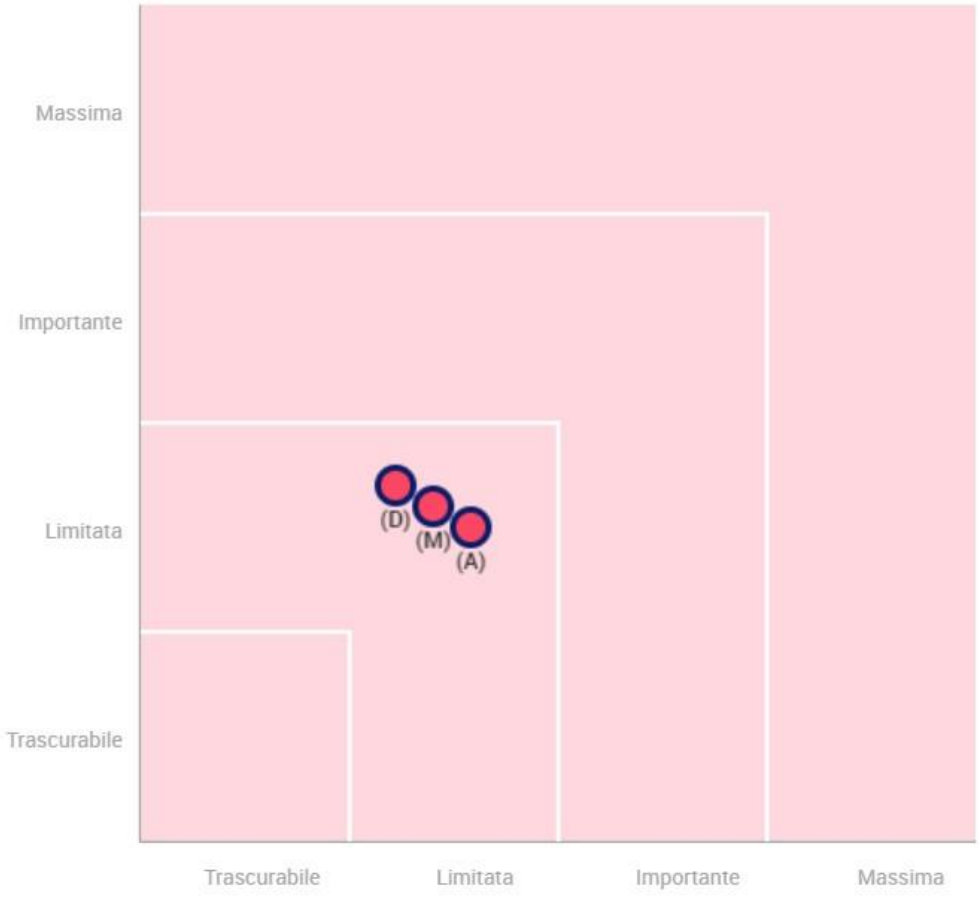
N° 1 telecamera DH IPC HFW244 1S - S
N° 11 telecamere modello DH HFW3841 ZS S2

Parcheggio STAGNO
N° 1 Telecamera modello DH IPC HDW244 T-S
N° 10 telecamere modello HFW3841 ZS S2

TORRE Faro/Rotatoria
N° 1 telecamera modello DH IPC HFW 3841T
N° 2 telecamere DHI ITC 413 PW 43

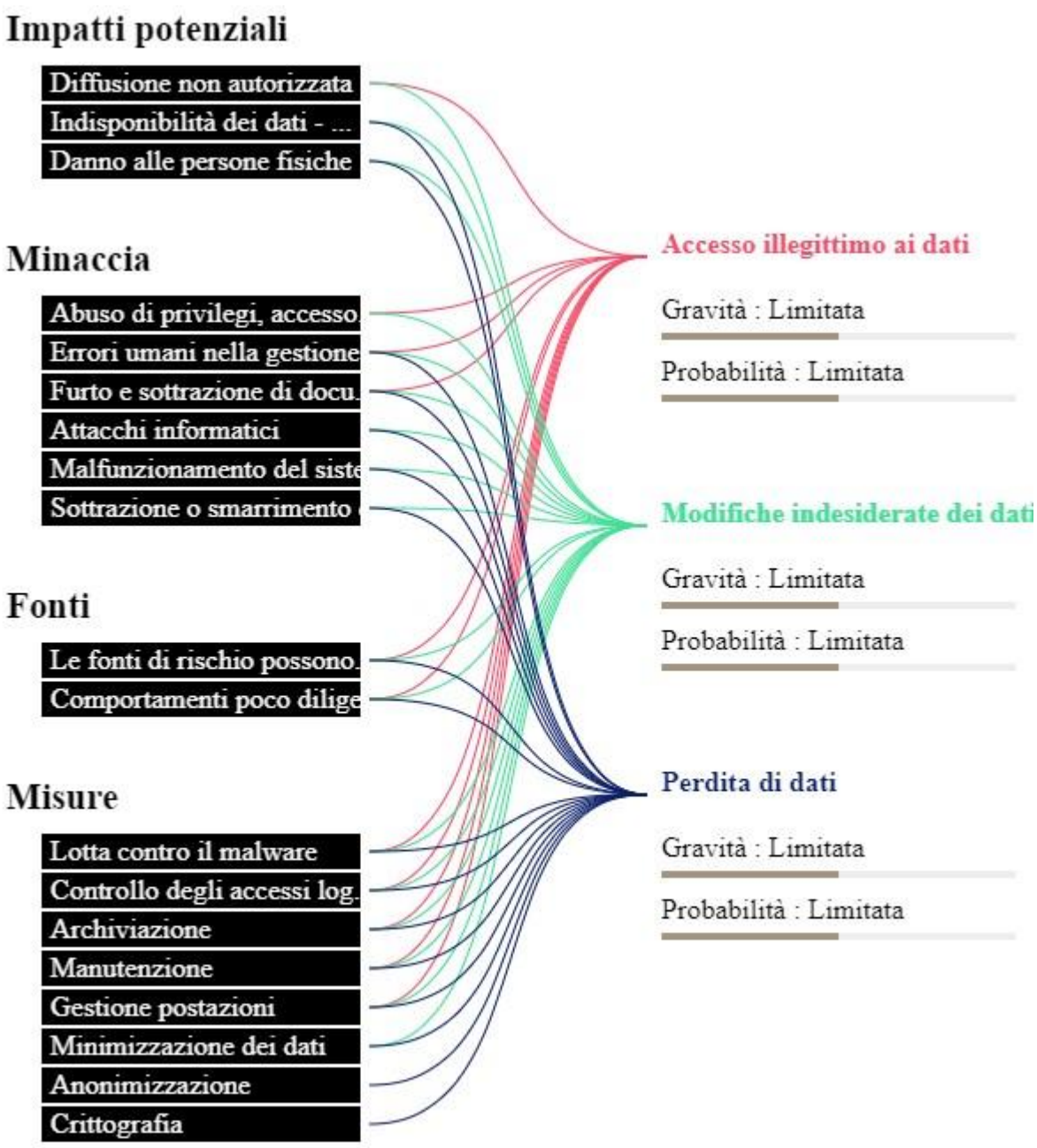


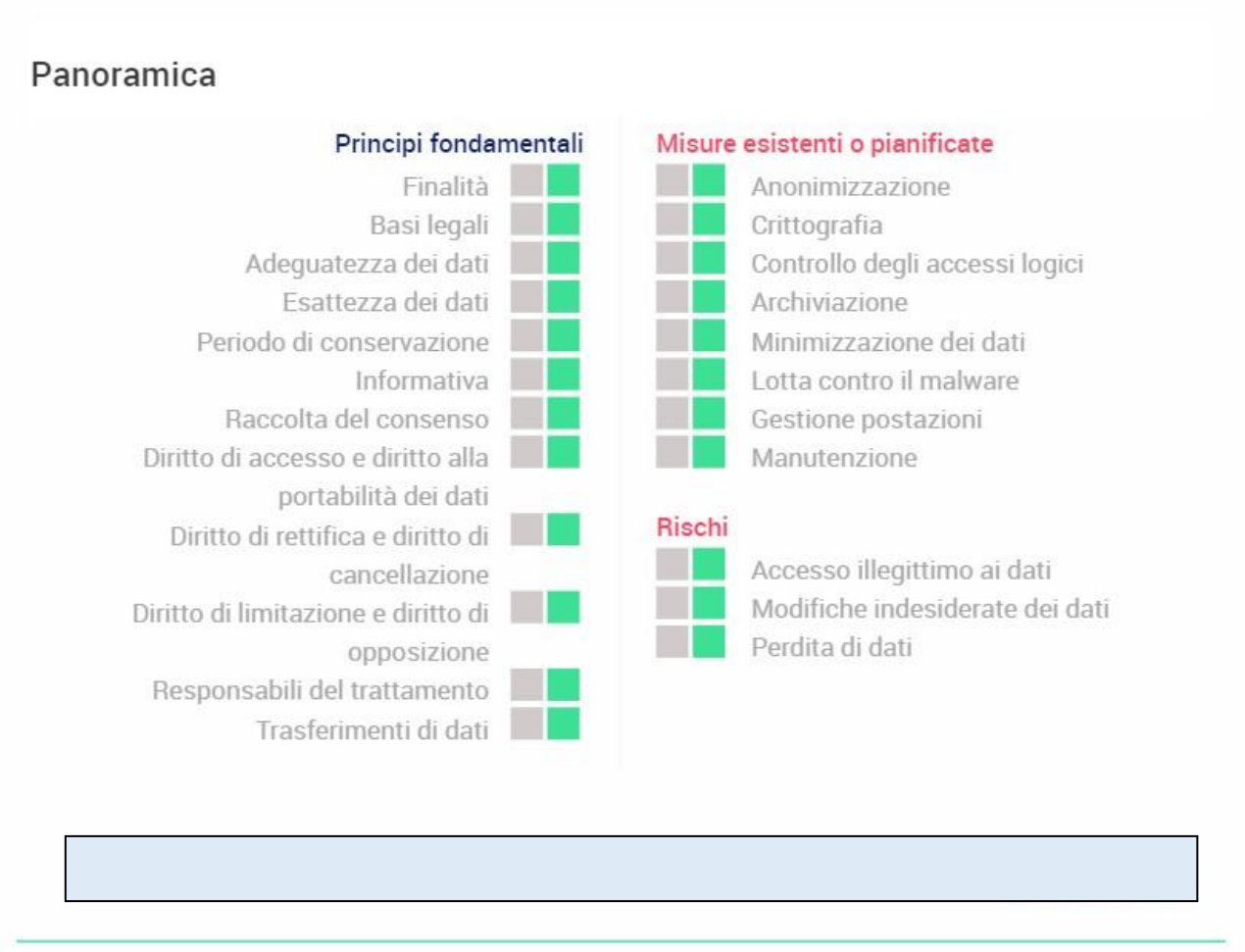
Gravità del rischio



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


Impatti potenziali
Diffusione non autorizzata
Indisponibilità dei dati - ...
Danno alle persone fisiche
Minaccia
Abuso di privilegi, accesso
Errori umani nella gestione
Furto e sottrazione di docu
Attacchi informatici
Malfunzionamento del siste
Sottrazione o smarrimento
Fonti
Le fonti di rischio possono
Comportamenti poco dilige
Misure
Lotta contro il malware
Controllo degli accessi log
Archiviazione
Manutenzione
Gestione postazioni
Minimizzazione dei dati
Anonimizzazione
Crittografia
Accesso illegittimo ai dati
Gravità : Limitata
Probabilità : Limitata
Modifiche indesiderate dei dati
Gravità : Limitata
Probabilità : Limitata
Perdita di dati
Gravità : Limitata
Probabilità : Limitata



CONCLUSIONI

La considerazione del contesto in cui si sviluppa l'azione del sistema di videosorveglianza adottato dal Comune di LOIRI PORTO SAN PAOLO, le sue finalità, le modalità con cui avviene il trattamento dei dati, la tipologia dei medesimi e le misure giuridiche di contenimento dei rischi consentono di poter considerare il rischio per le libertà e di diritti dei cittadini di livello complessivo medio/basso in considerazione della valutazione accettabile.
In particolare dall'analisi delle valutazioni emerse dalla DPIA in relazione all'esame dei processi relativi alla proporzionalità e la necessità dei dati trattati si desume una valutazione accettabile delle procedure messe in campo per la tutela dei dati personali.
Risultano valutate come accettabili anche le misure adottate per informare "gli interessati" dei diritti derivanti dalla presenza di un impianto di videosorveglianza e le misure poste in essere per garantire l'esercizio degli stessi.
Per quanto attiene le misure di sicurezza tecnico/informatiche si ritiene che siano idonee al fine di garantire la sicurezza ed il prevenire la perdita dei dati. I sistemi informatici sono custoditi in specifici locali il cui accesso è consentito al personale designato e/o autorizzato appositamente formato. Allo stato il livello di rischio appare medio/basso in considerazione delle misure adottate che appaiono accettabili.

Prescrizioni

FORMAZIONE - L'obbligo di formazione previsto dalla vigente normativa (art.29 e 32 GDPR) costituisce un dovere generale nell'ambito del principio di accountability e rende necessario e urgente un percorso di aggiornamento per tutti i soggetti coinvolti, per favorire, la conoscenza e le cautele da adottare per la gestione dell'impianto di videosorveglianza e la corretta gestione del trattamento dei dati nel rispetto dei diritti degli interessati.
Durante la DPIA è emersa la necessità che la presente Valutazione di Impatto Privacy dovrà essere sottoposta ad una prima verificata semestrale al fine di accertare se l'uso del sistema di videosorveglianza avviene nel pieno rispetto delle libertà e dei diritti dei cittadini.
Resta intesa la necessità di verificare la congruità ed adeguatezza della presente Valutazione di Impatto Privacy (DPIA) ogni volta che dovesse essere implementato il sistema di videosorveglianza ovvero essere rilevata qualche criticità o l'appalesarsi della necessità di rivalutare l'adeguatezza e la conformità del funzionamento dei sistemi in uso.

Allegati:
Schede Tecnica impianto videosorveglianza e posizionamento videocamere

- Relazione ITM Telematica del 26 gennaio 2026
- Relazione HOME TEACH Domotica del 15.09.2026

Loiri Porto San Paolo, 16/06/2026

Il Titolare **Il RPD/DPO**

Francesco Lai

Firmato digitalmente da:
FRANCESCO LAI
Data: 16/06/2026 11:34:38

STEFANO PAOLI

Signature: Stefano Paoli
Stefano Paoli (Jun 18, 2026 13:20:52 GMT+2)
Email: info@entilocali-learning.it

DPIA (1)

Final Audit Report 2026-06-18

Created:	2026-06-18
By:	mirco rigatti (mirco.rigatti@centrostudientilocali.it)
Status:	Signed
Transaction ID:	CBJCHBCAABAAhHDwEDazIV_Ykc09Cj3lR0mplSi799SQ

"DPIA (1)" History

Document digitally presigned by FRANCESCO LAI
2026-06-16 - 9:34:38 AM GMT- IP address: 31.193.26.46

Document created by mirco rigatti (mirco.rigatti@centrostudientilocali.it)
2026-06-18 - 10:39:45 AM GMT- IP address: 31.193.26.46

Document emailed to info@entilocali-learning.it for signature
2026-06-18 - 10:46:17 AM GMT

Email viewed by info@entilocali-learning.it
2026-06-18 - 11:18:20 AM GMT- IP address: 31.193.26.46

Signer info@entilocali-learning.it entered name at signing as Stefano Paoli
2026-06-18 - 11:20:50 AM GMT- IP address: 31.193.26.46

Document e-signed by Stefano Paoli (info@entilocali-learning.it)
Signature Date: 2026-06-18 - 11:20:52 AM GMT - Time Source: server- IP address: 31.193.26.46 - Signature Appearance Selected: TYPE

Agreement completed.
2026-06-18 - 11:20:52 AM GMT