FUTURA LA SCUOLA PER L'ITALIA DI DOMANI
Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Istruzione e del Merito
Italiadomani
ISTITUTO STATALE ISTRUZIONE SUPERIORE
VALCERESIO
Liceo Scientifico - Scienze Applicate
Liceo delle Scienze Umane
Istituto Tecnico Turismo
Istituto Tecnico Amministrazione, Finanza e *Marketing* - Relazioni Internazionali
Istituto Professionale per la Sanità e l'Assistenza sociale
Istituto Professionale per i Servizi Commerciali e Turistici
Via Roma, 57 - 21050 Bisuschio (VA) - ☎ Tel. 0332856760 - Fax 0332474918 - vais00400r@istruzione.it

Valutazione d'impatto sulla protezione dei dati Gestione sistema di videosorveglianza

Informazioni sulla PIA

Nome della PIA: Videosorveglianza
Nome autore: Maria Carmela Sferlazza DS
Nome valutatore: Antonio Vargiu DPO
Nome responsabile tratt.dati: Gabriella Angela Vita Lentini
Data di creazione: 10.02.2025

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Questa DPIA è atta alla valutazione dell'impatto connesso all'uso della videosorveglianza negli edifici pubblici scolastici.
Il circuito di videosorveglianza, infatti, permetterebbe alle scuole di prevenire o quanto meno ridurre, gli atti di vandalismo a danno di edifici pubblici.
Facendo riferimento al punto 2 del provvedimento 2010 del Garante privacy, è infatti possibile far ricorso alla videosorveglianza nei casi in cui sia richiesta:

1. Protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e sicurezza pubblica
2. protezione della proprietà;
3. rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge.

L'utilizzo della videosorveglianza, come si legge nel provvedimento di cui sopra, è tuttavia sottoposto ad alcuni vincoli e comunque associabile ad un rischio connesso al trattamento dei dati personali degli individui. Si rende perciò necessaria l'identificazione di piattaforme e policy di utilizzo volte a minimizzare la possibilità di rischi connessi alla protezione dei dati personali.

Quali sono le responsabilità connesse al trattamento?

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

- **Il titolare del trattamento** è "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". Ove l’impianto fosse realizzato e gestito dall’istituzione scolastica sarà il dirigente scolastico a svolgere la funzione di titolare. La scuola sarà titolare del trattamento anche se l’impianto fosse realizzato da altro ente (ad esempio comune o provincia) che ne affida alla scuola la gestione. In questo caso per valutare il ruolo dell’ente proprietario bisogna verificare se questo ha possibilità di accedere alle registrazioni.

- **Il Responsabile della Protezione dei Dati (RPD)** ha il compito di fornire supporto a titolare, docenti e interessati, per tutte quelle questioni concernenti la protezione dei dati personali all'interno dell'ambito di applicazione del trattamento.
- **I responsabili esterni del trattamento:** ove presenti, possono essere individuati nella società esterna all'amministrazione scolastica che gestisce l'acquisizione la conservazione delle immagini. Sarà necessario procedere alla nomina formale dei precedenti quali responsabili del trattamento ai sensi dell'Art. 28, comma 3 del GDPR.
- **Autorizzati al trattamento:** personale scolastico che è autorizzato dal titolare a trattare dati personali e registrazioni acquisite dall'impianto.

Nel caso in cui la proprietà dell'impianto fosse di ente esterno (comune o provincia, ad esempio) bisognerà considerare se questo delega completamente il trattamento dei dati personali e la gestione delle registrazioni alla scuola che mantiene quindi il ruolo di titolare del trattamento. In caso contrario bisognerà valutare se l'ente esterno agisce come titolare o come responsabile del trattamento.

Ci sono standard applicabili al trattamento?

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

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati trattati sono immagini in formato digitale, che si articolano principalmente in due categorie.

1. immagini generiche dei soggetti che non ne permettono l'identificazione (ad esempio nel caso in cui il soggetto si trovasse di spalle rispetto alla telecamera)
2. immagini di soggetti identificabili.

La prima tipologia di dati non necessita di alcun accorgimento nel trattamento la seconda tipologia di dato è ascrivibile alla categoria "dati personali" ai sensi dell'Art. 4 comma 1 del GDPR e come tali devono essere trattati e tutelati secondo quanto previsto dal GDPR.

Quali sono le zone sottoposte a controllo?

L'impianto di videosorveglianza copre le seguenti aree dell'istituto:

1. Zone perimetrali esterne:
    - Aree di accesso all'edificio scolastico
    - Perimetro esterno della struttura
    - Punti strategici di passaggio
    - Aree di parcheggio e transito veicolare di pertinenza dell'istituto
2. Eventuali aree tecniche o locali sensibili:
    - Zone di particolare rilevanza per la sicurezza dell'edificio

Le telecamere sono state posizionate in modo da:

- Riprendere esclusivamente le aree di pertinenza scolastica
- Non inquadrare spazi pubblici esterni, proprietà confinanti o aree private di terzi
- Limitare l'angolo visuale alle sole zone che necessitano effettivamente di controllo
- Non riprendere luoghi dove si svolgono attività didattiche

L'attivazione del sistema avviene esclusivamente:

- In orari di chiusura dell'istituto
- In assenza di attività didattiche
- Quando non sono in corso attività extrascolastiche autorizzate

Sono disposti specifici divieti per garantire la sicurezza?

È assolutamente vietata:

- L'attivazione durante l'orario scolastico
- La ripresa di aule, laboratori o altri spazi dedicati alla didattica
- La ripresa di uffici o luoghi di lavoro del personale scolastico
- Qualsiasi forma di controllo a distanza dell'attività lavorativa"

Qual è il ciclo di vita del trattamento dei dati?

Il ciclo di vita del trattamento si articola nelle seguenti fasi:

1. **Raccolta**
    - Le immagini sono acquisite attraverso le telecamere installate nelle aree individuate
    - La registrazione avviene nelle pertinenze esterne dell'edificio e non internamente.
    - Il sistema non è attivo durante lo svolgimento di attività scolastiche o extrascolastiche
2. **Trasmissione**
    - Il trasferimento dei dati dalle telecamere ai dispositivi di archiviazione avviene tramite rete protetta
    - La trasmissione è cifrata per garantire la sicurezza dei dati
3. **Conservazione**
    - Le registrazioni sono conservate per un massimo di 48ore
    - Il termine può essere esteso solo in caso di:
        - Chiusura dell'istituto per festività o periodi prolungati
        - Specifiche richieste dell'autorità giudiziaria o di polizia giudiziaria
    - La cancellazione avviene automaticamente allo scadere del termine
4. **Accesso e consultazione**
    - L'accesso alle registrazioni è consentito solo a personale espressamente autorizzato
    - Ogni accesso è tracciato con registrazione di:
        - Identità dell'operatore
        - Data e ora
        - Motivazione dell'accesso
    - Le immagini possono essere estratte solo in caso di:
        - Richiesta dell'autorità giudiziaria
        - Denuncia di atti criminosi
        - Esercizio del diritto di accesso da parte degli interessati
5. **Cancellazione**
    - Al termine del periodo di conservazione, i dati sono cancellati in modo automatico
    - La cancellazione deve essere irreversibile e completa
    - Il sistema deve garantire che non sia possibile il recupero dei dati cancellati

L'intero ciclo di vita è sottoposto a misure di sicurezza tecniche e organizzative adeguate a garantire la riservatezza, l'integrità e la disponibilità dei dati trattati.

Quali sono le risorse di supporto ai dati?

Le immagini vengono caricate su dei server, locali e Cloud, che devono garantire le adeguate misure di sicurezza informatica per la protezione dei dati personali contenuti. L'azienda che si occupa della manutenzione e gestione dell'infrastruttura di sorveglianza, se presente, deve essere nominata responsabile del trattamento ai sensi dell'Art. 28 del GDPR.

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il sistema di videosorveglianza è finalizzato alla tutela del patrimonio scolastico attraverso il controllo degli accessi e la prevenzione di intrusioni e atti vandalici, con particolare riferimento alla protezione del locale tecnico e del perimetro dell'istituto. Il trattamento è altresì volto a garantire la sicurezza delle persone che accedono all'area scolastica, senza alcuna finalità di controllo dell'attività lavorativa del personale o di monitoraggio dell'attività didattica.

Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica può essere individuata nell'art. 6, par. 1, lett. e) del GDPR: "il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento".

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

I dati trattati devono rispettare il diritto alla riservatezza. A tal fine, come riportato nel provvedimento dell'8 aprile 2010 del Garante per la Protezione dei Dati Personali, il circuito di sorveglianza potrà essere utilizzato solo ai fini della tutela dell'edificio e dei beni scolastici. Per questo motivo, i circuiti potranno essere utilizzati nelle sole aree interessate e negli orari di chiusura delle amministrazioni scolastiche. In caso di riprese esterne, si dovranno escludere dalla visuale le aree non pertinenti all'edificio. Infine, non si potrà ricorrere alla videosorveglianza nelle ore di attività extrascolastiche che si svolgono all'interno della scuola.

Qual è il periodo di conservazione dei dati?

Come riportato nel provvedimento generale dell'8 aprile 2010 del Garante per la protezione dei dati personali, il periodo di conservazione delle immagini ottenute dai circuiti di videosorveglianza posti presso gli edifici scolastici ha una durata massima di ventiquattro ore. Fanno eccezione le chiusure straordinarie dell'edificio, come ad esempio le festività.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Come riportato nel provvedimento generale dell'8 aprile 2010 del Garante per la protezione dei dati personali, gli interessati al trattamento in questione saranno informati precedentemente al trattamento stesso e tramite la cosiddetta “doppia informativa”. Questa include un’informativa minima, unitamente al cartello contenente la dicitura “Area videosorvegliata”, che viene posta all’accesso della zona videosorvegliata e contiene le informazioni più utili e immediate per l’interessato, quali le finalità del trattamento e l’indicazione del titolare dello stesso, In particolare, in accordo con il punto 3.1 del provvedimento del 2010, l’informativa minima è collocata prima del raggio di azione del circuito di sorveglianza e deve essere chiaramente visibile in ogni condizione ambientale diurna e notturna e può contenere un simbolo che chiarisca se le immagini siano solo visionate o anche registrate. Qualora l’interessato voglia poi approfondire il trattamento dei suoi dati personali, egli potrà accedere senza oneri all’informativa completa, resa ai sensi dell’art. 13 del GDPR. Questa deve innanzitutto contenere l’identità e i dati di contatto del titolare del trattamento e

del Responsabile Protezione Dati (RPD). Andranno poi indicate sia le finalità del trattamento che la base giuridica dello stesso oltre che i destinatari del trattamento, ovvero la società esterna responsabile del circuito di sorveglianza e in caso di furti o atti vandalici, anche le forze dell'ordine, specificando la categoria di riferimento di ogni destinatario. Qualora i dati fossero trasferiti verso paesi terzi o organizzazioni internazionali, bisognerà specificarlo nell'informativa completa. Parte fondamentale dell'informativa completa sono poi i diritti dell'interessato, esercitati senza formalità e in modo gratuito (salvo richieste reiterate, eccessive o infondate) e devono essere ottemperati nella medesima forma della richiesta senza ingiustificato ritardo, nei limiti del periodo di conservazione degli stessi.
Poiché l'informativa dovrà contenere il diritto al reclamo, è necessario inserire Autorità di Controllo e Sito Web (ad esempio, Garante Privacy - https://www.garanteprivacy.it). Infine, l'informativa deve specificare se la comunicazione di dati personali (ai destinatari) è un obbligo di legge o contrattuale, se l'interessato ha l'obbligo di fornire tali dati (e le possibili conseguenze nel caso in cui lo stesso non volesse procedere con la comunicazione) e se è in atto un processo decisionale automatizzato (art. 22 GDPR), con la logica utilizzata, l'importanza e le conseguenze di tale trattamento.

Ove applicabile: come si ottiene il consenso degli interessati?

Non applicabile al presente trattamento.

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

Gli interessati potranno richiedere al titolare l'accesso e la portabilità dei dati personali che li riguardano.

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

Nei casi relativi all'art. 17 GDPR, il titolare del trattamento dovrà procedere alla valutazione della richiesta di cancellazione di tali dati senza ingiustificato ritardo. In caso contrario, i dati seguiranno il ciclo di vita previsto dal trattamento. In ogni caso, sarà sempre necessario considerare i tempi di conservazione scelti dal titolare del trattamento (potrebbe essere impossibile procedere con l'esercizio di tali diritti).

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

Nei casi relativi all'art. 18 GDPR, il titolare del trattamento dovrà procedere alla valutazione della richiesta di limitazione di tali dati senza ingiustificato ritardo. In caso contrario, i dati seguiranno il ciclo di vita previsto dal trattamento. In ogni caso, sarà sempre necessario considerare i tempi di conservazione scelti dal titolare del trattamento (potrebbe essere impossibile procedere con l'esercizio di tale diritto). Per quanto riguarda il diritto all'opposizione, la scuola metterà a disposizione dell'interessato i dati di contatto dell'amministrazione stessa, tramite i quali esprimere la volontà all'esercizio del diritto all'opposizione a tale trattamento. Anche qui, vista la particolare tipologia di trattamento, potrebbe essere impossibile procedere con l'esercizio di tale diritto, poichè sarebbe impossibile definire eventuali regole di gestione dell'opposizione.

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

Il titolare del trattamento ha provveduto a stipulare un contratto di nomina del responsabile, nella persona del DSGA, che ne chiarifichi gli obblighi.
Nel contratto saranno esposti tutti gli aspetti previsti dall'art. 28 del [GDPR]: durata, ambito, finalità, istruzioni di trattamento documentate, autorizzazione preventiva qualora si ricorra a sub-responsabili del trattamento, fornitura di documentazione che dimostri la conformità al [GDPR],

notifica tempestiva di eventuali violazioni dei dati, ecc.

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

Non è previsto il trasferimento di dati personali al di fuori dell'Unione europea.

Valutazione del rischio

Di seguito verranno valutati i seguenti rischi associati all'uso del sistema di videosorveglianza:

- Accesso illegittimo ai dati
- Modifiche indesiderate ai dati
- Perdita di dati

Per ciascuno di questi rischi verranno valutati i seguenti fattori:

- **entità del danno:** 1. Trascurabile, 2. Limitata, 3. Importante, 4. massima
- **probabilità del rischio:** 1. Trascurabile, 2. Limitata, 3. Importante, 4. Massima

A seguito della definizione di **entità del danno** e della **probabilità di rischio** verrà individuata l'**entità del rischio** con un numero compreso fra 1 e 16 ottenuto come prodotto fra i precedenti fattori.

Rischi

Misure esistenti o pianificate

Crittografia

I dispositivi di conservazione devono essere protetti con adeguate tecnologie di crittazione dei dati. Il trasferimento di dati all'interno del sistema di videosorveglianza deve avvenire tramite canali criptati.

Controllo degli accessi logici

L'accesso alle immagini conservate è reso disponibile solamente al personale autorizzato, adeguatamente formato. Devono essere implementate adeguate misure informatiche atte a garantire il controllo e monitoraggio degli accessi ai dati.

Tracciabilità

Le registrazioni devono contenere le informazioni riguardanti la data e l'ora esatta in cui sono avvenute. Gli accessi ai dati, oltre che contenere informazioni riguardanti l'identità dell'accedente, devono contenere informazioni riguardanti la data e l'ora di accesso.

Archiviazione

L'archiviazione deve avvenire esclusivamente su dispositivi criptati e il cui accesso è protetto da adeguate misure di sicurezza informatica. I dispositivi di archiviazione devono essere protetti da intrusioni malevole atte alla copia non autorizzata dei dati in essi contenuti.

Lotta contro il malware
I dispositivi che vengono utilizzati per l'accesso ai dati devono garantire un livello di sicurezza e protezione contro il malware adeguato, atto a minimizzare il rischio di violazioni dei dati personali.

Backup
I sistemi di backup eventualmente implementati non possono detenere le informazioni per un periodo di tempo superiore a quello indicato per la conservazione delle registrazioni.

Manutenzione
Se la manutenzione dei dispositivi fisici è affidata a soggetti esterni, questi dovranno essere nominati Responsabili del trattamento vincolati da una nomina ai sensi dell'Art. 28 del GDPR.

Sicurezza dei canali informatici
Le trasmissioni dei dati devono avvenire tramite canali criptati, che garantiscano alo stesso tempo l'integrità dei dati trasmessi.

Sicurezza dell'hardware
I dispositivi preposti alla gestione dei dati trattati devono garantire adeguati meccanismi di protezione anti-intrusione, sia fisici che software, e di controllo degli accessi virtuali.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali
La scuola deve essere dotata di un regolamento interno per la gestione delle violazioni di dati personali. Il responsabile del trattamento, ove presente, è obbligato a riferire al titolare qualunque violazione riconducibile ai dati trattati.

Accesso illegittimo ai dati

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

- Compromissione del sistema di sicurezza dell'edificio scolastico
- Utilizzo improprio delle immagini per pianificare attività criminose
- Diffusione non autorizzata di immagini dell'edificio e delle sue vulnerabilità
- Vanificazione delle misure di tutela del patrimonio scolastico

Quali sono le principali minacce che potrebbero concretizzare il rischio?

- Attacchi informatici mirati al sistema di videosorveglianza
- Manomissione fisica dei dispositivi di registrazione
- Intercettazione delle comunicazioni tra telecamere e sistemi di registrazione
- Compromissione delle credenziali di accesso
- Errori nella configurazione dei sistemi di sicurezza

Quali sono le fonti di rischio?

- Soggetti esterni con intenti criminosi (hacker, criminali)
- Personale tecnico interno non adeguatamente formato
- Addetti alla manutenzione non correttamente supervisionati
- Malfunzionamenti dei sistemi di protezione
- Carenze nelle procedure di gestione degli accessi

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?
- Cifratura delle registrazioni e delle trasmissioni
- Sistema di controllo accessi con autenticazione forte
- Tracciamento di ogni operazione sui dati
- Aggiornamento costante dei sistemi di protezione
- Formazione specifica del personale autorizzato
- Procedure documentate di gestione degli incidenti
- Piano di ripristino in caso di compromissione
- Verifica periodica dell'efficacia delle misure di sicurezza

Come stimereste la gravità del rischio? LIMITATA (2) - Un accesso illegittimo potrebbe compromettere l'efficacia del sistema di sicurezza dell'edificio e potrebbe esporre a rischi il patrimonio scolastico. Gli impatti sono tuttavia limitati dalla circostanza che il sistema opera solo in orari di chiusura dell'istituto.

Come stimereste la probabilità del rischio? LIMITATA (2) - Nonostante le misure di sicurezza implementate, la possibilità di accessi illegittimi non può essere considerata trascurabile, considerando sia i possibili attacchi esterni sia i potenziali errori interni nella gestione del sistema."

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?
- Alterazione o cancellazione delle registrazioni che potrebbero servire come prova di reati
- Manipolazione delle immagini tale da compromettere la loro validità come elementi probatori
- Perdita dell'integrità del sistema di videosorveglianza come strumento di sicurezza

Quali sono le principali minacce?
- Alterazione volontaria o involontaria delle registrazioni
- Cancellazione accidentale prima del termine previsto
- Manomissione dei sistemi di registrazione
- Modifiche alla configurazione del sistema che ne compromettano il corretto funzionamento

Quali sono le fonti di rischio?
- Personale tecnico autorizzato che opera erroneamente sul sistema
- Attacchi informatici mirati
- Malfunzionamenti del sistema di registrazione
- Errori nella procedura di backup e conservazione

Quali misure contribuiscono a mitigare il rischio?

- Sistema di logging che traccia ogni operazione sui dati
- Limitazione degli accessi ai soli soggetti autorizzati
- Formazione specifica del personale tecnico
- Misure di sicurezza contro accessi non autorizzati

Come stimereste la gravità del rischio? LIMITATA (2) - La modifica o perdita delle registrazioni potrebbe compromettere le finalità di sicurezza del sistema e la sua efficacia come strumento di tutela del patrimonio scolastico.

Come stimereste la probabilità del rischio? TRASCURABILE (1) - Le misure tecniche e organizzative implementate rendono difficile la modifica non autorizzata dei dati. La maggior parte delle operazioni è automatizzata e tracciata."

Perdita di dati

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

- Impossibilità di utilizzare le registrazioni per documentare eventuali intrusioni o atti vandalici
- Compromissione dell'efficacia del sistema di sicurezza dell'edificio scolastico
- Impossibilità di fornire elementi probatori in caso di richiesta dell'autorità giudiziaria

Quali sono le principali minacce?

- Guasti hardware dei sistemi di registrazione
- Malfunzionamenti del software di gestione
- Danneggiamento fisico dei dispositivi
- Eventi accidentali (incendi, allagamenti, sbalzi di tensione)

Quali sono le fonti di rischio?

- Eventi naturali o accidentali
- Malfunzionamenti tecnici
- Errori umani nella gestione del sistema
- Atti vandalici diretti ai dispositivi di registrazione
- Attacchi informatici distruttivi

Quali misure contribuiscono a mitigare il rischio?

- Sistema di backup automatico delle registrazioni (considerare tuttavia il limite delle 24 ore per la detenzione delle registrazioni)
- Monitoraggio costante del funzionamento del sistema
- Manutenzione preventiva periodica
- Procedure di disaster recovery
- Controllo degli accessi fisici ai dispositivi
- Protezione dei locali tecnici
- UPS e sistemi di protezione elettrica

Come stimereste la gravità del rischio? LIMITATA (2) - La perdita dei dati comprometterebbe le finalità di sicurezza del sistema, ma il danno sarebbe limitato nel tempo data la breve durata della conservazione (24 ore).

Come stimereste la probabilità del rischio? LIMITATA (2) - Le misure tecniche implementate e le procedure di gestione rendono improbabile una perdita totale dei dati. Gli eventi che potrebbero causarla sono rari e comunque mitigati dalle contromisure adottate.

Valutazione gravità del rischio

A seguito dell'analisi condotta abbiamo quindi ricavato le seguenti valutazioni:

Rischio	Entità del danno	probabilità	Gravità del rischio
Accesso illegittimo ai dati	2	2	4
Modifiche indesiderate ai dati	2	1	2
Perdita di dati	2	2	4

L'analisi condotta evidenzia come i rischi, valutati in relazione alla probabilità ed alla entità del danno, sono al di sotto di una soglia accettabile considerate le misure di contenimento del rischio già adottate. Non si ritiene quindi di dover fare analisi più approfondite sui rischi volte a stimare questi in modo più puntuale e alla ulteriore riduzione del rischio residuo.

Conclusioni

L'analisi condotta evidenzia come l'insieme delle misure tecniche e organizzative implementate consenta di mantenere i rischi al di sotto di una soglia accettabile per le seguenti ragioni:

1. **Limitazione temporale del trattamento**
   - Il sistema opera esclusivamente in orari di chiusura dell'istituto
   - Le registrazioni vengono conservate solo per 24 ore
   - La cancellazione avviene in modo automatico
2. **Misure di sicurezza implementate**
   - La cifratura delle trasmissioni e delle registrazioni
   - Il controllo degli accessi
   - Il tracciamento di ogni operazione
3. **Procedure organizzative**
   - La formazione specifica del personale
   - La presenza di istruzioni operative dettagliate
   - Il sistema di gestione degli incidenti
   - Le verifiche periodiche

Considerando che:

- Il trattamento ha finalità limitate e legittime
- Le misure adottate sono proporzionate ai rischi
- I controlli sono regolari e documentati
- Il personale è adeguatamente formato

Si può concludere che il trattamento presenta un livello di rischio residuo accettabile e può essere effettuato nel rispetto dei diritti e delle libertà degli interessati.