

Regolamento per l'esercizio del sistema di videosorveglianza del Liceo scientifico G.Torelli di Fano e Pergola, aggiornato al Provvedimento del Garante per la protezione dei dati personali del 8-4-2010 e al Reg. UE 2016/679 – GDPR



Titolo documento: Regolamento per l'esercizio del sistema di videosorveglianza

Codice documento: 0018

Data ultimo aggiornamento: Approvato con deliberazione del Consiglio di Istituto del Liceo Scientifico Torelli di Fano del 28-6-2021

Indice

Art. 1 - Definizioni	3
Art. 2 - Obiettivo del presente Regolamento	5
Art. 3 - Ambito di validità e di applicazione del presente regolamento	6
Art. 4 - Identificazione del titolare del trattamento dei dati	6
Art. 5 - Obiettivi e finalità del sistema di videosorveglianza	6
Art. 6 – Verifica del pieno soddisfacimento dei principi di liceità, necessità, non eccedenza e proporzionalità, e finalità.	7
6.1 Premessa	
6.2 Principio di liceità	
6.3 Principio di necessità	
6.4 Principio di non eccedenza e proporzionalità	
6.5 Principio di finalità	
Art. 7 – Utilizzi esplicitamente vietati	8
Art. 8 – Tipi di trattamenti autorizzati	9
Art. 9 – Tipologie di soggetti e di strutture coinvolte nelle operazioni di trattamento dei dati	9
Art. 10 – Accesso telematico da parte di soggetti incaricati di operazioni di assistenza o manutenzione	10
Art. 11 – Modalità di designazione dei soggetti coinvolti nelle operazioni di trattamento	10
Art. 12 – Designazione dei soggetti autorizzati	10
Art. 13 – Tempi di conservazione delle immagini	11
Art. 14 – Luogo e modalità di memorizzazione delle immagini	11
Art. 15 – Cifratura dei dati trasmessi mediante apparati e tecnologie wireless	11
Art. 16 – Ottemperanza al Provvedimento del 27-11-2008 del Garante per la protezione dei dati personali relativo al controllo dell’operato degli amministratori di sistema.	11
Art. 17 – Installazione di nuove telecamere	12
Art. 18 – Informativa	12
Art. 19 – Riscontro all’interessato	12
Art. 20 – Requisiti minimi sul luogo di collocazione del server	13
Art. 21 – Iniziale deroga ai requisiti minimi sul luogo di collocazione del server	13
Art. 22 – Requisiti minimi sugli strumenti elettronici, informatici e telematici.	13
Art. 23 – Cessazione del trattamento	14
Art. 24 – Danni cagionati per effetto del trattamento dei dati personali	14
Art. 25 – Modifiche e integrazioni regolamentari	14

Art. 1 - Definizioni

Di seguito si riportano alcune definizioni rilevanti ai fini del presente regolamento; per le altre definizioni si rimanda all'art. 4 del Reg. UE 2016/679 – GDPR.

Ai sensi del 1° comma dell'art. 4 del GDPR si intende per:

- 1)«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- 2)«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 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;
- 3)«limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- 4)«profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- 5)«pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- 6)«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- 7)«titolare del trattamento»: 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- 8)«responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- 9)«destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.
Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- 10)«terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- 11)«consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12)«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13)«dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14)«dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

15)«dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16)«stabilimento principale»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17)«rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi di divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13)«dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14)«dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

15)«dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16)«stabilimento principale»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del

trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

c) un reclamo è stato proposto a tale autorità di controllo;

23) «trattamento transfrontaliero»:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

26) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Art. 2 - Obiettivo del presente Regolamento

Obiettivo del presente regolamento è assicurare che i trattamenti di dati personali effettuati dal Liceo scientifico Torelli mediante il sistema di videosorveglianza, avvengano correttamente, lecitamente, e conformemente a quanto previsto dalla disciplina rilevante in materia di sicurezza e

protezione dei dati personali; in particolare, il rispetto del presente regolamento garantirà la conformità:

- ai provvedimenti del Garante per la protezione dei dati personali, con particolare riferimento al provvedimento generale del 8 aprile 2010 del Garante per la protezione dei dati personali, dedicato alla videosorveglianza;
- al Reg. UE 2016/679, detto anche GDPR;
- alle prescrizioni del D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali), così come modificato dal D.Lgs. 101/2018;
- al D.Lgs. 51/2018, relativamente all'utilizzo delle immagini e delle riprese filmiche in eventuali attività di Polizia Giudiziaria da parte delle Forze dell'Ordine, nello svolgimento di attività di prevenzione, repressione ed accertamento di reati od illeciti;
- alle prescrizioni di cui all'art. 6 del GDPR relative alle basi giuridiche del trattamento;
- ai principi di:
 - o trasparenza;
 - o liceità;
 - o necessità;
 - o non eccedenza e proporzionalità rispetto alle finalità;
 - o finalità;
 - o minimizzazione dei dati di cui all'art. 5 del GDPR.

Art. 3 - Ambito di validità e di applicazione del presente regolamento

Le prescrizioni del presente regolamento si applicano obbligatoriamente ai trattamenti di dati personali e sensibili effettuati mediante sistema di videosorveglianza: sotto la **diretta titolarità** del Liceo scientifico Torelli, all'interno dei locali e delle pertinenze (es. giardini, campi da gioco etc.) e nelle immediate vicinanze.

Art. 4 - Identificazione del titolare del trattamento dei dati

Il titolare dei trattamenti di dati personali effettuati mediante il sistema di videosorveglianza del Liceo scientifico Torelli è il Liceo scientifico Torelli stesso: pertanto, competono esclusivamente al Liceo scientifico Torelli le decisioni in ordine alle finalità e alle modalità del trattamento, compreso anche il profilo della sicurezza.

A titolo esemplificativo e non esaustivo, si riportano di seguito alcune decisioni che spettano esclusivamente al Liceo scientifico Torelli:

- il numero, la tipologia e i luoghi di installazione attuale e futura delle telecamere;
- i tempi massimi e minimi di memorizzazione delle immagini;
- gli strumenti elettronici, informatici e telematici da utilizzare per la gestione delle immagini, compresa la ripresa e la memorizzazione delle immagini stesse;
- l'individuazione dei soggetti che possono essere a vario titolo coinvolti (in qualità di incaricati, oppure di responsabili interni od esterni oppure di autonomi titolari) nelle operazioni di trattamento dai dati e nelle operazioni di amministrazione di gestione di sistema informatico e telematico;
- l'individuazione di compiti e responsabilità da assegnare ai soggetti individuati in precedenza.

Art. 5 - Obiettivi e finalità del sistema di videosorveglianza

Il sistema di videosorveglianza, in quanto sistema che comporta il trattamento di dati personali, può venire utilizzato (ai sensi dell'art. 6 comma 1 lettera e) del GDPR) esclusivamente per il perseguimento delle funzioni istituzionali del titolare del trattamento dei dati, vale a dire del Liceo Scientifico Torelli.

In via esemplificativa e non esaustiva le finalità sono:

- sicurezza e tutela del patrimonio dell'Istituto, di beni e persone;

- contrasto al fenomeno del vandalismo;
- attivazione di misure di prevenzione e sicurezza;
- raccolta e costituzione di materiale probatorio di natura fotografica e filmica a supporto delle attività di accertamento, contestazione e notificazione di infrazioni, ai sensi degli artt. 13 e 14 della Legge 24 novembre 1981, n. 689;
- prevenzione e rilevazione di reati;
- prevenzione e rilevazione di atti vandalici;
- rilevazione situazioni di pericolo, consentendo l'eventuale l'intervento degli operatori;

Art. 6 – Verifica del pieno soddisfacimento dei principi di liceità, necessità, non eccedenza e proporzionalità, e finalità.

6.1 Premessa

La verifica del rispetto dei principi di liceità, necessità, non eccedenza e proporzionalità e finalità dovrà venire effettuata periodicamente sia nei confronti del sistema di videosorveglianza nel suo complesso, sia nei confronti di ciascuna telecamera installata.

6.2 Principio di liceità

Affinché sia soddisfatto il principio di liceità, si dovrà periodicamente verificare che:

- le finalità perseguite mediante il sistema di videosorveglianza siano coerenti e compatibili con le funzioni istituzionali di competenza del Liceo scientifico Torelli
 - la videosorveglianza non avvenga in violazione delle vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata (es. art. 615bis del Codice Penale), di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela;
 - la videosorveglianza non abbia luogo in violazione delle tutele riconosciute ai lavoratori, con particolare riferimento a quanto previsto dalla Legge 300/1970 (Statuto dei Lavoratori);
 - le riprese o le registrazioni non vengano effettuate in violazione di quanto previsto da disposizioni di legge da osservare in caso di installazione di apparecchi audiovisivi;
- la videosorveglianza avvenga nel rispetto delle norme del codice penale che vietano le intercettazioni di comunicazioni e conversazioni;
- siano osservati specifici limiti derivanti da disposizioni di legge o di regolamento che prevedono o ipotizzano la possibilità di installare apparecchiature di ripresa locale, aerea o satellitare (d.l. 24 febbraio 2003, n.28, convertito, con modificazioni, dalla legge 24 aprile 2003, n. 88), disposizioni che, quando sono trattati dati relativi a persone identificate o identificabili, vanno applicate nel rispetto dei principi affermati dal Codice, in tema per esempio di sicurezza presso stadi e impianti sportivi.

6.3 Principio di necessità

Affinché sia rispettato il principio di necessità deve essere escluso qualsiasi utilizzo superfluo ed evitati eccessi e ridondanze. Inoltre il sistema informatico e ciascuna telecamera deve essere configurata ed utilizzata in maniera tale da non utilizzare dati relativi a soggetti identificabili quando le finalità del trattamento possono essere perseguite raccogliendo solamente dati anonimi; inoltre il software deve essere configurato in modo da cancellare automaticamente e periodicamente i dati eventualmente registrati.

Ulteriori considerazioni da tenere presenti per il rispetto del principio di necessità sono le seguenti:

- l'esigenza di perseguire le finalità deve essere concreta, reale e comprovabile;
- il personale dipendente dell'Istituto, non potendo avere una presenza costante, non è in grado di assicurare il monitoraggio e la registrazione continua dei fatti, che solo un sistema di videosorveglianza può assicurare;

- da un punto di vista economico, l'utilizzo di un sistema elettronico di videosorveglianza presenta dei costi sensibilmente inferiori rispetto ai costi derivanti dall'utilizzo di personale dedicato al perseguimento delle finalità indicate in precedenza;
- il sistema di videosorveglianza deve essere configurato per l'utilizzazione al minimo di dati personali e di dati 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.

6.4 Principio di non eccedenza e proporzionalità

Il rispetto dei principi di non eccedenza e proporzionalità si dovrà valutare periodicamente con riferimento ai criteri di seguito elencati:

- il numero e la collocazione delle telecamere devono essere effettivamente commisurate al reale livello di rischio, evitando la rilevazione o la registrazione in aree che non siano soggette a concreti pericoli o che non siano meritevoli di particolare tutela;
- il posizionamento, la tipologia di telecamere, le aree brandeggiabili, l'utilizzo di zoom, quali dati ed eventi rilevare, devono essere rapportati alle concrete finalità ed esigenze, e si dovranno evitare eccedenze; ad esempio si dovrà limitare la possibilità di brandeggio mediante l'impostazione di vincoli o di mascheramenti statici;
- le telecamere devono essere collocate, e più in generale la videosorveglianza deve essere adottata, solo quando altre misure meno "invasive" siano state ponderatamente valutate insufficienti o inattuabili;
- se l'installazione delle telecamere è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri accorgimenti quali ad esempio controlli da parte di addetti, sistemi di allarme, misure di protezione perimetrale e degli ingressi, abilitazione e controllo degli accessi;
- non è consentita l'installazione meramente dimostrativa o artefatta di telecamere non funzionanti o per finzione, che può essere legittimamente oggetto di contestazione;
- la non eccedenza e proporzionalità deve essere valutata, anche periodicamente, in ogni fase e modalità del trattamento; ad esempio, in fase di definizione e assegnazione dei profili di accesso ai dati, i profili dovranno essere configurati e assegnati in maniera che gli incaricati accedano alla minima quantità di dati necessaria per lo svolgimento dei compiti assegnati; come minimo si dovrà prevedere una fondamentale distinzione tra il profilo di tipo "utente normale" e un profilo più elevato di tipo "administrator";

6.5 Principio di finalità

Gli scopi perseguiti devono essere determinati, espliciti e legittimi, ai sensi dell'art. 5 del GDPR; sono pertanto esclusi utilizzi indeterminati, occulti e non legittimi. In particolare il titolare o il responsabile potranno perseguire solo finalità di sua pertinenza.

Potranno essere perseguite solo finalità determinate e rese trasparenti, ossia direttamente conoscibili attraverso adeguate comunicazioni e/o cartelli di avvertimento al pubblico (fatta salva l'eventuale attività di acquisizione di dati disposta da organi giudiziari o di polizia giudiziaria). E non finalità generiche o indeterminate, soprattutto quando esse siano incompatibili con gli scopi che vanno esplicitamente dichiarati e legittimamente perseguiti.

E' inoltre consentita la videosorveglianza come misura complementare volta a supportare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del titolare del trattamento o di terzi sulla base di immagini o riprese, in caso di atti illeciti.

Art. 7 – Utilizzi esplicitamente vietati

E' fatto in generale divieto di posizionare telecamere, e in ogni caso di utilizzare immagini e registrazioni, in luoghi chiusi, siano essi pubblici o privati. Nel caso si presenti l'esigenza

chiaramente dimostrabile e giustificabile, di effettuare riprese in luoghi chiusi pubblici o aperti al pubblico, si dovrà verificare e assicurare che le riprese avvengano nel pieno rispetto dello “Statuto dei lavoratori” e non violino il divieto, da parte del datore di lavoro, di effettuare controlli a distanza sull’attività dei dipendenti.

Art. 8 – Tipi di trattamenti autorizzati

Nell’installazione e nell’esercizio del sistema di videosorveglianza, sono autorizzati esclusivamente le seguenti tipologie di trattamenti:

- installazione e attivazione di nuove telecamere;
- creazione e gestione di gruppi e profili di utenti;
- consultazione immagini live da telecamera;
- messa a fuoco e brandeggiamento della telecamera;
- impostazione di limiti al brandeggiamento delle telecamere
- impostazione di zone oscurate staticamente
- registrazione di immagini;
- cancellazione di immagini;
- predisposizione delle soglie temporali e degli eventi di cancellazione immagini;
- consultazione immagini registrate;
- estrazione (duplicazione) immagini registrate;
- definizione aree di motion-detection;
- definizione azioni da eseguire in concomitanza di eventi di motion detection;
- accensione di sorgenti luminose o ad infrarosso;
- attivazione funzionalità di “speak-ip”;
- rilevazione e inventario degli indirizzi ip presenti in rete;
- rilevazione e inventario dei mac address presenti in rete;
- installazione e configurazione di software applicativo;
- installazione e configurazione di software di base;
 installazione di “patch” e “hot fix”;
- attivazione collegamenti da remoto;
- interventi generici di manutenzione e configurazione hardware e software;
- estrazione di files di log;
- conservazione di files di log per un periodo minimo di dodici mesi;
- apposizione di firma digitale qualificata o di codici hash a files di log.

Art. 9 – Tipologie di soggetti e di strutture coinvolte nelle operazioni di trattamento dei dati

Le operazioni di trattamento dei dati saranno svolte – a vario titolo – dalle seguenti tipologie di soggetti:

- Titolare del trattamento dei dati;
- Responsabile della protezione dei dati;
- Responsabile esterno del trattamento dei dati: sono i soggetti (persone fisiche o giuridiche) esterni al Liceo scientifico Torelli ai quali sono affidati, da parte del Liceo scientifico Torelli, alcune operazioni di trattamento dei dati e la messa in atto di alcune misure di sicurezza;
- Soggetti designati ed autorizzati al trattamento dei dati: sono i soggetti fisici (persone fisiche) che, designati per iscritto dal titolare, eseguono una o più operazioni di trattamento dei dati;
- Custode delle password di sistema: è il soggetto incaricato della custodia e della disponibilità – in caso di comprovata necessità e assenza o impossibilità da parte dell’amministratore di sistema - delle parole chiave corrispondenti ai vari profili di tipo “administrator” o equivalenti;

- Custode delle password applicative: è il soggetto incaricato della custodia e della disponibilità – in caso di comprovata necessità e assenza o impossibilità da parte dell’incaricato – delle parole chiave assegnate agli utenti finali;
- Soggetti incaricati della gestione e manutenzione degli strumenti elettronici, denominati anche “Amministratori di sistema”;
- Altre Pubbliche Amministrazioni che richiedano di accedere ai dati per lo svolgimento delle loro funzioni istituzionali: in questo caso l’accesso e l’utilizzo dei dati messi a disposizione dal Liceo scientifico Torelli, avrà luogo sotto la diretta responsabilità e titolarità della Pubblica Amministrazione o del soggetto richiedente: sarà pertanto cura della Pubblica Amministrazione o del soggetto richiedente verificare che l’accesso avvenga esclusivamente per lo svolgimento delle funzioni istituzionali, e non per il perseguimento di interessi o finalità personali o comunque non chiaramente riconducibili allo svolgimento di funzioni istituzionali o di compiti d’ufficio, senza che vi sia abuso d’ufficio. Sarà inoltre cura della Pubblica Amministrazione o del soggetto richiedente, o del soggetto al quale i dati sono comunicati o portati a conoscenza a seguito di motivata richiesta, mettere in atto quanto previsto dalla disciplina rilevante in materia di privacy e sicurezza, con particolare riferimento all’obbligo di designazione degli incaricati del trattamento, specificando puntualmente per iscritto l’ambito del trattamento consentito e assicurando che le operazioni di trattamento (compresa la mera consultazione, che è comunque una tipologia di trattamento) e l’accesso ai dati avvenga in modo da limitare l’accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Art. 10 – Accesso telematico da parte di soggetti incaricati di operazioni di assistenza o manutenzione

E’ previsto che per l’effettuazione di alcune operazioni di assistenza e manutenzione da parte di soggetti opportunamente designati in qualità di responsabili esterni del trattamento dei dati, possa avere luogo in modalità “telemantenzione”, laddove tale prassi sia esplicitamente prevista dai contratti di assistenza.

In ogni caso la gestione della telemanutenzione dovrà soddisfare come minimo i seguenti requisiti di base:

- telecamere digitali o analogiche;
- PC e apparati di memorizzazione dei dati;
- accesso al sistema di videosorveglianza negoziato ed autorizzato di volta in volta da personale designato per iscritto del Liceo scientifico Torelli.

Art. 11 – Modalità di designazione dei soggetti coinvolti nelle operazioni di trattamento

In generale i soggetti coinvolti nelle operazioni di trattamento dovranno essere designati per iscritto dal titolare del trattamento dei dati, con atto che specifichi chiaramente compiti e responsabilità assegnate. Per quanto i soggetti designati ed autorizzati al trattamento dei dati, oltre ai compiti e alle responsabilità affidate, dovrà essere chiaramente specificato l’ambito del trattamento consentito. La revisione della sussistenza delle condizioni per il mantenimento dell’ambito del trattamento consentito e del profilo di accesso dovranno essere oggetto di revisione da parte del responsabile o del titolare con frequenza almeno annuale.

Art. 12 – Designazione dei soggetti autorizzati

Coerentemente con quanto prescritto dal punto 3.3.2. del Provvedimento del Garante per la protezione dei dati personali del 8 aprile 2010, la designazione degli incaricati dovrà avvenire con modalità che permettano di esplicitare le tipologie di operazioni alle quali ciascun incaricato risulterà essere abilitato. L’ambito del trattamento consentito agli incaricati dovrà inoltre essere oggetto di verifica (ed eventuale modifica) almeno annuale.

Art. 13 – Tempi di conservazione delle immagini

I tempi di conservazione dei dati gestiti mediante il sistema di videosorveglianza dovranno tenere conto della tipologia di dati, delle finalità per le quali i dati sono acquisiti e trattati, nonché di eventuali prescrizioni/limiti imposti dalla attuale normativa in materia di videosorveglianza e protezione dei dati personali.

Per quanto riguarda le immagini acquisite mediante le telecamere convenzionali, in considerazione delle finalità individuate in precedenza, e della necessità di ottemperare al principio di non eccedenza e proporzionalità in tutte le operazioni di trattamento dei dati, le immagini registrate dovranno essere conservate per un tempo massimo di 3 giorni; dovrà comunque essere presente una funzionalità che permetta agevolmente di disattivare la cancellazione automatica – trascorso il tempo massimo di registrazione - delle immagini registrate (ad esempio in concomitanza della registrazione di atti vandalici), senza impedire o menomare la capacità di registrare le immagini “in diretta”. E’ inoltre prevista la possibilità che i tempi di memorizzazione delle immagini possano venire modificati a seguito di variazioni nelle finalità, di mutate esigenze, oppure di motivata richiesta proveniente da altri soggetti pubblici.

Art. 14 – Luogo e modalità di memorizzazione delle immagini

L’impianto di videosorveglianza è stato realizzato nella sede centrale di Fano in via Kennedy, 30.

Le immagini riprese dalle telecamere dovranno venire memorizzate in formato elettronico su un unico (o un numero limitato) supporto di memorizzazione di massa centralizzato e ben individuato all’interno di un unico e ben determinato apparato di tipo “server” (può essere comunque fatta salva la necessità di una memorizzazione “di backup” su un server remoto). Il suddetto server dovrà essere dedicato esclusivamente alla memorizzazione delle immagini registrate dalle telecamere del sistema di videosorveglianza, e non dovrà essere dedicato ad altri scopi. Se non diversamente disposto dal titolare con atto scritto, il server non dovrà essere collegato ad internet, oppure dovrà essere collegato solo in casi e per finalità specifiche e ben individuate, per intervalli di tempo il più possibile contenuti.

Non è consentita la memorizzazione “ordinaria” delle immagini in locale a livello di postazione “client”, o comunque su supporti e strumenti diversi dal succitato server centralizzato. La memorizzazione temporanea delle immagini in locale potrà avvenire solo in caso di estrazione di immagini, nel qual caso la copia temporanea locale delle immagini estratte dovrà essere cancellata non appena possibile.

Art. 15 – Cifratura dei dati trasmessi mediante apparati e tecnologie wireless

Qualora venisse introdotta la tecnologia wireless, i dati trasmessi mediante apparati wireless dovranno essere cifrati, in maniera che ne sia garantita la riservatezza. Come minimo dovranno essere applicati algoritmi di cifratura dotati di robustezza maggiore o uguale a DES (Data Encryption Standard).

Art. 16 – Ottemperanza al Provvedimento del 27-11-2008 del Garante per la protezione dei dati personali relativo al controllo dell’operato degli amministratori di sistema.

Sarà introdotto un meccanismo di logging (tracciatura) delle operazioni di amministrazione e gestione di sistema effettuate con profilo di administrator, per garantire l’ottemperanza a quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 27-11-2008 relativo al controllo dell’operato degli amministratori di sistema, il presente Regolamento prevede quanto segue:

- a livello di software di videosorveglianza, il meccanismo di logging (tracciatura) delle operazioni di amministrazione e gestione di sistema effettuate con profilo di administrator deve essere attivato (ed eventualmente configurato);

- a livello di software di videosorveglianza, il suddetto file di log non deve essere sovrascritto per un periodo minimo di tre mesi;
- il suddetto file di log non dovrà essere per nessun motivo cancellato, modificato o alterato;
- con frequenza al massimo semestrale, si dovrà procedere all'estrazione (copia) del suddetto file di log;
- la copia estratta del file di log dovrà essere generata in un formato non modificabile (pdf, tiff o altri formati non modificabili) e firmata digitalmente con certificato digitale emesso da una certification authority trusted di primo livello;
- la copia del file di log firmata digitalmente dovrà essere custodita in un luogo sicuro per un periodo di almeno 12 mesi;
- con frequenza semestrale si dovrà controllare l'operato degli amministratori di sistema, mediante analisi dei file di log e del registro delle operazioni di amministrazione e gestione di sistema effettuate sul sistema di videosorveglianza; alla conclusione delle operazioni di controllo / verifica dovrà essere redatto apposito verbale e relazione.

Art. 17 – Installazione di nuove telecamere

L'installazione di nuove telecamere dovrà essere autorizzata mediante atto deliberativo del Consiglio di Istituto. Preventivamente si dovrà verificare che:

- i luoghi ripresi;
 - le telecamere utilizzate;
 - la configurazione e la possibilità di utilizzo delle telecamere delle riprese e delle registrazioni effettuate;
- soddisfino i principi di liceità, necessità, non eccedenza e proporzionalità e finalità.

Art. 18 – Informativa

Gli interessati devono essere informati che stanno per accedere o che si trovano in una zona videosorvegliata, e dell'eventuale registrazione, mediante un modello semplificato di informativa "minima", riportata in allegato. In luoghi diversi dalle aree esterne il modello va integrato con almeno un avviso circostanziato che riporti, oltre agli elementi dell'informativa minima", anche gli altri elementi previsti dall'art. 13 del GDPR.

In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, vanno installati più cartelli.

E' necessario controllare periodicamente, con frequenza almeno mensile, che i cartelli siano presenti e ben leggibili, e non siano stati oggetto di atti vandalici o di eventi (es. crescita di rami o foglie, interposizione di altri elementi, etc.) che abbiano compromesso la piena leggibilità del testo e della rappresentazione iconica. In ogni caso, la leggibilità dovrà essere tempestivamente ripristinata e assicurata. Nella pagina seguente si riporta l'informativa che si dovrà affiggere bene in vista presso ciascuna telecamera.

Art. 19 – Riscontro all'interessato

In caso di esercizio da parte degli interessati dei diritti previsti dagli artt. da 15 a 21 del GDPR, il riscontro all'interessato dovrà venire fornito a cura del Titolare o da Responsabile del trattamento dei dati appositamente designato dal Titolare, **entro massimo 30 giorni dalla data di ricezione della richiesta**. Le richieste di cancellazione o blocco dei dati dovranno essere soddisfatte esclusivamente nei casi in cui il trattamento sia avvenuto in violazione di legge, e comunque solo su autorizzazione scritta del Dirigente Scolastico. Non potranno essere oggetto di cancellazione o modifica le immagini per le quali vi siano state richieste di estrazione o siano in corso indagini da parte degli organi di Polizia o da parte dell'Autorità Giudiziaria.

Art. 20 – Requisiti minimi sul luogo di collocazione del server

Il server di memorizzazione delle immagini dovrà essere fisicamente collocato all'interno di un locale che fornisca adeguate garanzie di sicurezza fisica e perimetrale. Di seguito si riportano i requisiti minimi che il locale dovrà soddisfare:

- locale ad utilizzo non promiscuo e dedicato esclusivamente a “sala macchine” o “sala server”, non agevolmente accessibile al pubblico e ai dipendenti (ad eccezione ovviamente dei dipendenti o collaboratori esplicitamente incaricati di operazioni di amministrazione e gestione di sistema);
- possibilità di regolamentare e di tenere traccia degli accessi al locale;
- locale di norma chiuso a chiave, con serratura e chiave funzionante;
- in caso vi siano finestre a piano terra, presenza di inferriate in ferro non dolce oppure presenza di vetri antisfondamento;
- assenza di carta, cartoni o altro materiale facilmente infiammabile all'interno del locale;
- presenza nelle vicinanze di almeno un estintore non a polvere, funzionante e regolarmente revisionato con frequenza almeno semestrale;
- presenza di adeguato impianto di condizionamento, che assicuri un livello di umidità e temperatura all'interno del range di corretto funzionamento degli apparati.

In aggiunta a quanto elencato, è auspicabile (ancorché non strettamente obbligatoria) la presenza di quanto segue:

- allarme volumetrico (attivato dalla variazione della volumetria all'interno dei locali) o di prossimità;
- presenza di sensori per la rilevazione del fumo e/o della temperatura;
- collegamento dei sensori e dell'allarme con centrale operativa di sicurezza oppure con le forze dell'ordine.

Art. 21 – Iniziale deroga ai requisiti minimi sul luogo di collocazione del server

E' comunque previsto dal presente regolamento che, a causa di vincoli e problematiche di varia natura, sia possibile collocare il server in un luogo che non soddisfi, soprattutto in una fase iniziale, tutti i requisiti elencati nel precedente articolo. In tal caso sarà sufficiente verificare e assicurare che il server, e più in generale gli apparati coinvolti, non siano a rischio palese di asportazione, danneggiamento o manomissione. Ad esempio, potrà essere giudicata come temporaneamente accettabile una situazione in cui il server non sia collocato in un locale ad utilizzo dedicato, ma sia collocato in un ufficio dove il personale presente negli orari d'ufficio possa assicurare a vista un adeguato presidio e controllo. Negli orari di chiusura ufficio o in caso di assenza di personale, potrà essere ritenuta sufficiente la presenza di una porta che sia però dotata di serratura e chiave funzionante, e possa essere tenuta chiusa in caso di assenza di personale.

Art. 22 – Requisiti minimi sugli strumenti elettronici, informatici e telematici.

Sarà introdotto un sistema operativo che coordini le apparecchiature di videosorveglianza.

In tal caso gli strumenti elettronici, informatici e telematici utilizzati nelle operazioni di trattamento dei dati, dovranno soddisfare i seguenti requisiti minimi:

- sistema operativo server e client non obsoleto e con supporto attivo da parte del fornitore; non sono consentiti sistemi operativi obsoleti o poco sicuri come ad esempio Windows 95 oppure Windows 98;
- server e client protetti da password iniziale di accesso al sistema operativo e alle risorse di rete; possibilità da parte dell'utente finale di modificare autonomamente la propria password; possibilità da parte dell'amministratore di sistema di disabilitare la user-id senza cancellarla;
- server e client protetti da password iniziale di accesso al programma applicativo; possibilità da parte dell'utente finale di modificare autonomamente la propria password; possibilità di disabilitare (da parte dell'amministratore di sistema) le user-id senza cancellarla;

- presenza di almeno due profili distinti: uno di tipo “administrator” e uno di tipo “utente normale”, sia a livello di sistema operativo sia a livello di programma applicativo;
- assegnazione e utilizzo delle user-id su base strettamente personale e non di gruppo;
- possibilità di individuare e rimuovere periodicamente le vulnerabilità e le configurazioni poco sicure a livello applicativo e di sistema operativo;
- protezione adeguata da virus e codici maligni;
- protezione perimetrale adeguata in caso di apertura, anche temporanea, ad Internet.

I requisiti di cui sopra dovranno essere verificati con frequenza annuale mediante verifiche in loco dei locali, degli apparati e dei programmi, effettuando un’analisi dei rischi e individuando le azioni correttive da mettere in atto. Periodicamente si dovrà inoltre verificare che le misure pianificate siano state messe in atto, e il livello di efficacia delle misure stesse.

Art. 23 – Cessazione del trattamento

In caso di cessazione del trattamento, i dati dovranno essere distrutti, ad eccezione di quelli per i quali siano in corso o vi siano state in passato richieste di estrazione, che dovranno essere conservati a cura del titolare per fini di documentazione e riscontro.

Art. 24 – Danni cagionati per effetto del trattamento dei dati personali

La materia è disciplinata dall’art. 82 del GDPR.

Art. 25 – Modifiche e integrazioni regolamentari

Il presente regolamento dovrà essere adeguato per recepire eventuali modifiche alla disciplina rilevante in materia di privacy e sicurezza, con particolare riferimento alle disposizioni e ai provvedimenti emanati dal Garante per la protezione dei dati personali.

Inoltre, il presente regolamento dovrà venire modificato nel caso dovessero mutare le finalità del sistema di videosorveglianza.

IL DIRIGENTE SCOLASTICO
Prof.ssa Renata Falcomer