

Erasmus University Rotterdam Camera Surveillance Policy Framework 2026-2031

This policy document was adopted by the Executive Board on 22 September 2026.
This policy document was approved by the University Council on 16 July 2026.
This policy document shall enter into force on 1 October 2026.

Department : ABD, BZ, Integral Safety

Version : 0.44EN

Contents

1	Introduction and scope	2
2	Objectives of camera surveillance.....	3
2.1	<i>Operation and deployment</i>	3
2.2	<i>Scope and limits of deployment.....</i>	3
3	Types of Camera Surveillance	4
3.1	<i>Permanent camera surveillance</i>	4
3.1.1	Fixed cameras.....	4
3.1.2	PTZ cameras	4
3.1.3	Licence plate recognition.....	4
3.2	<i>Temporary additional camera surveillance.....</i>	5
3.3	<i>Covert camera surveillance</i>	5
4	Criteria and principles for camera surveillance.....	7
4.1	<i>Generic procedure for requests for camera surveillance</i>	7
4.2	<i>Location categories for camera surveillance</i>	8
4.2.1	Locations with a structural need for camera surveillance.....	8
4.2.2	Locations where camera surveillance is permitted under conditions.....	10
4.2.3	Locations where camera surveillance is in principle not permitted	11
4.2.4	Locations where camera surveillance is never permitted	11
4.3	<i>External EUR locations (ISS, EUC, C&C Putselaan).....</i>	11
5	Privacy and safeguards	12
5.1	<i>Legal basis for processing of data.....</i>	12
5.2	<i>Safeguards.....</i>	12
6	Application and evaluation.....	14
6.1	<i>Interpretation</i>	14
6.2	<i>Management of Policy Framework.....</i>	14
6.3	<i>Translation.....</i>	14
6.4	<i>Entry into force, duration and evaluation.....</i>	14
6.5	<i>Short title.....</i>	14
	Annex 1 – Authorisation matrix	15

1 Introduction and scope

The campus of Erasmus University Rotterdam (EUR) has an open and accessible character. To maintain this character and at the same time ensure a safe environment, EUR has used camera surveillance for many years as part of a broader safety approach. Cameras are installed at specific locations on campus to enhance safety.

EUR does not regard camera surveillance as the answer to all safety issues, and certainly not as an end in itself; it is always a means towards broader safety objectives. Camera surveillance is always part of a broader package of safety measures, such as regular patrols, good lighting and clear sightlines. This overall package of measures falls outside the scope of this Policy Framework, which specifically concerns camera surveillance. The availability of alternative measures does, however, have implications for this framework: when deciding to install cameras, EUR always explicitly weighs necessity, proportionality and subsidiarity.

EUR recognises that there is an inherent tension between camera surveillance and the right to privacy. A certain level of interference with the privacy of students, staff and visitors is considered necessary to comply with the duty of care for their safety. EUR therefore carefully balances, in each case, the objective pursued on the one hand and the impact on privacy on the other, and takes measures to minimise as far as possible the impact of camera surveillance.

This Policy Framework explains why and how EUR uses camera surveillance and it applies to all EUR grounds and buildings. With this Policy Framework, EUR aims to ensure that the use of camera surveillance is predictable, transparent and understandable. It also sets out the conditions under which EUR may use camera surveillance. In addition, this Policy Framework describes the safeguards that EUR implements to limit the impact of camera surveillance on privacy. The formal procedures and governance are laid down in the Camera Surveillance Regulations EUR 2026.

This Policy Framework and the Camera Surveillance Regulations EUR 2026 together form the framework for the use of camera surveillance at EUR. This Policy Framework primarily sets out the objectives, criteria and location categories for the installation and use of cameras; the Regulations contain the detailed procedures and the conditions for the processing of camera footage and other data. This Policy Framework relates solely to camera surveillance for the purpose of promoting safety in EUR buildings and on EUR grounds. Other forms of camera use, for example for teaching, research or operational purposes, fall outside the scope of this Policy Framework.

2 Objectives of camera surveillance

Camera surveillance is used to protect the safety and health of students, staff and third parties, to secure access to and use of EUR buildings and grounds, and to protect EUR property. Camera surveillance also helps to prevent, detect and bring to an end incidents. EUR achieves these objectives by implementing a broad range of safety measures, of which camera surveillance is an important component.

2.1 Operation and deployment

In principle, camera surveillance is used primarily to prevent incidents. The visible presence of cameras can discourage potential offences and undesirable behaviour, thereby helping to prevent incidents. In addition, camera surveillance enables the campus security to detect unusual or high-risk situations at an early stage and, where necessary, to intervene preventively.

Camera surveillance also supports direct intervention in incidents and emergencies: camera footage can be used to assess situations, direct the deployment of security staff, take appropriate measures and, where necessary, inform and guide the emergency services in a timely and effective manner. After an incident, camera footage can be used to establish the course of events and, where applicable, to support criminal investigation and prosecution.

The presence of camera surveillance can also contribute to the sense of safety experienced by students, staff and visitors, provided it is used in a visible, proportionate and transparent way. However, an increase in the sense of safety is never the primary reason for installing cameras; without additional measures, this would create a false sense of security.

2.2 Scope and limits of deployment

The use of camera surveillance by EUR is limited by the right to privacy and other fundamental rights and freedoms of students, staff and visitors. For every decision on the use of camera surveillance, EUR therefore carefully weighs, on the one hand, the safety interests that need to be protected and, on the other hand, the impact on privacy.

Camera surveillance is used solely to promote safety and order in EUR buildings and on EUR grounds and is explicitly not intended to restrict the rights and freedoms of students and staff – such as freedom of expression and the rights of assembly and demonstration. A concrete example is camera surveillance during demonstrations: this is used to safeguard the safety of everyone present, including participants, and not to restrict the right to demonstrate or other fundamental freedoms.

3 Types of Camera Surveillance

EUR uses several forms of camera surveillance. As a rule, EUR relies on permanent, visible cameras. Where circumstances give reason to do so, EUR may also deploy temporary additional camera surveillance, for example in the form of mobile cameras. Temporary additional camera surveillance is applied on the basis of the same criteria and safeguards as permanent camera surveillance, and differs mainly in the limited duration of its deployment and its technical set-up. In very exceptional cases, EUR may use covert camera surveillance. This form of camera surveillance may have a greater impact on the privacy of students, staff and visitors. For that reason, additional conditions and safeguards apply.

3.1 Permanent camera surveillance

Permanent camera surveillance is used to monitor specific EUR locations on a structural basis over a longer period of time. This permanent network forms the foundation of camera surveillance on EUR grounds and in EUR buildings. Cameras are only installed on the basis of a risk analysis and an assessment against the criteria set out in Chapter 4. The procedure for decision-making and the processing of camera footage is laid down in the Camera Surveillance Regulations EUR 2026.

Within permanent camera surveillance, EUR uses different types of cameras, including fixed cameras and PTZ cameras.

3.1.1 Fixed cameras

Fixed cameras are cameras that are permanently directed in a single fixed direction and cannot be actively controlled. They only record a predefined field of view. Fixed cameras are used to maintain continuous visibility of specific locations, such as entrances to buildings and central areas on campus.

3.1.2 PTZ cameras

PTZ (Pan-Tilt-Zoom) cameras are cameras that can be controlled remotely by the control room operator in the security control room. These cameras can be rotated, tilted and zoomed, and therefore make it possible to respond to real-time situations.

When a PTZ camera is not actively controlled, it functions as a fixed camera with a preset viewing direction. Active control of a PTZ camera takes place only where there is reason to do so, for example in the event of an incident. In such cases, the camera can temporarily be directed at a different location, for example to follow the movement of an unwelcome person on site or to assess a potentially unsafe situation in more detail.

3.1.3 Licence plate recognition

In addition to regular camera surveillance in car parks, licence plate recognition cameras are also used. These cameras are installed at the entrances to car parks on Campus Woudestein and are used for payment purposes. Because these cameras are not used for camera surveillance to promote safety within the meaning of this Policy Framework, they fall outside its scope. Separate frameworks and procedures apply to the processing of licence plate data.

3.2 Temporary additional camera surveillance

In addition to permanent camera surveillance, EUR may use temporary additional camera surveillance where there is a specific need to do so. Temporary additional camera surveillance is understood to mean the temporary expansion of the existing camera network on the basis of a specific threat, an increased risk or a special situation, where permanent camera surveillance does not provide sufficient coverage or possibilities.

Temporary additional camera surveillance is deployed to monitor a specific area or location for a predetermined period. In practice, this often involves mobile or flexibly deployable cameras. These may be either fixed cameras or PTZ cameras.

Temporary additional camera surveillance is only used where (imminent) disturbances or incidents occur, or where such disturbances or incidents can reasonably be expected on the basis of concrete signals or previous experience. In addition, for events it may be decided to deploy temporary additional camera surveillance where the nature, scale or location of the event gives reason to do so. In all cases, temporary cameras are directed solely at the relevant area and used solely for the purpose for which they have been installed.

When temporary additional camera surveillance is deployed, the purpose, duration and scope of the surveillance are set out and justified in advance. Once the predetermined period has ended, the temporary additional camera surveillance is evaluated. On the basis of this evaluation, a decision may be taken to end the surveillance, to extend its use for a limited period, or – where there is a structural need – to convert it into permanent camera surveillance. The procedure for the deployment of temporary additional camera surveillance is laid down in the Camera Surveillance Regulations EUR 2026.

3.3 Covert camera surveillance

As a rule, camera surveillance at EUR is visible to everyone present on EUR grounds or in EUR buildings. This visibility is desirable because it contributes to the preventive effect of camera surveillance. Only in very exceptional cases may EUR use covert camera surveillance. In doing so, EUR follows the guidelines of the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*).

Covert camera surveillance is used only as an *ultimum remedium*. It is only permitted where regular camera surveillance and other measures taken by EUR have demonstrably failed to stop structural incidents, and where there are reasonable or well-founded suspicions of criminal offences or other seriously reprehensible behaviour.

In addition to the Data Protection Impact Assessment (DPIA) that EUR carries out on camera surveillance as a whole, EUR performs a separate DPIA specifically for covert camera surveillance as a processing category. This DPIA is generic in nature and describes the additional risks and safeguards that apply to covert camera surveillance. For each decision to use covert camera surveillance, it is assessed whether that decision is consistent with the principles and conditions set out in this generic DPIA. The measures described in the DPIA include both organisational and technical safeguards aimed at preventing and detecting misuse during implementation, such as a strict limitation of access to camera footage to a small group of authorised staff, logging and periodic review of access records, and mandatory instruction and confidentiality obligations for staff who have access to covert camera surveillance.

The decision to deploy covert camera surveillance is always taken by the Executive Board, in accordance with the Camera Surveillance Regulations EUR 2026. Covert camera surveillance is always temporary in nature; its duration and scope are explicitly defined in advance.

Once covert camera surveillance has ended, the University Council and the staff and students concerned are informed of this, subject to any restrictions arising from ongoing investigations or proceedings. The procedure for the deployment of covert camera surveillance and for the processing of the resulting camera footage is laid down in the Camera Surveillance Regulations EUR 2026.

4 Criteria and principles for camera surveillance

Camera surveillance inherently involves a tension between safety and the protection of privacy. To deal with this carefully, EUR uses a fixed method for deploying camera surveillance. All proposals are assessed against the criteria of necessity, proportionality and subsidiarity, and an explicit privacy assessment is carried out. In addition, camera surveillance is not designed on an *ad hoc* basis, but embedded in a coherent design of the camera network: the campus and buildings are divided into different categories of locations, for which it is laid down per category whether, and under what conditions, camera surveillance may be used.

4.1 Generic procedure for requests for camera surveillance

The formal procedures for requesting and assessing camera surveillance are set out in Chapter IV of the Camera Surveillance Regulations EUR 2026. In principle, requests for establishing or modifying camera surveillance are assessed by the Camera Surveillance Review Team.

The Camera Surveillance Review Team is a multidisciplinary team comprising, at a minimum, the Advisor Integral Safety, the Privacy Officer ABD and the Service Manager Park Management/CCTV of RE&F. Together, they contribute expertise on safety, privacy, and technical and facilities aspects, and jointly weigh these perspectives in their assessments. In addition, the University Council may appoint its own representative to participate in the Review Team. This representative has an advisory role within the team and represents the interests of students and staff at EUR. Additional experts may be involved where necessary.

The Review Team assesses requests against the following criteria:

- Necessity: a clear objective is formulated for installing a camera or expanding camera surveillance, which fits within EUR's overall objectives for camera surveillance. The necessity follows from a risk analysis carried out by Team Integral Safety.
- Proportionality: the use of camera surveillance, by definition, interferes with the privacy of students, staff and visitors. The nature and extent of this interference must be reasonably proportionate to the intended objective of the camera surveillance.
- Subsidiarity: camera surveillance is only used where the intended objective cannot be achieved with a less intrusive measure, or where such measures have proven insufficiently effective.
- Explicit balancing of interests: EUR also carries out an explicit balancing of interests. In that assessment, EUR's interests in safety, order and protection of property are weighed against the interests of data subjects. As a rule, these interests are identified in the Legitimate Interest Assessment (LIA) as part of the Data Protection Impact Assessment (DPIA) that is carried out for the camera surveillance system as a whole. For specific decisions on camera surveillance, it is assessed whether these decisions are in line with the interests, principles and safeguards described in the LIA and DPIA. The representative of the University Council may in particular advise on the interests of data subjects that are affected.

Once it has completed its assessment, the Camera Surveillance Review Team issues a recommendation on the requested deployment of camera surveillance. This recommendation is then subject to a limited review by the Chief Privacy Officer. Where necessary, the Data Protection Officer may issue a binding opinion.

4.2 Location categories for camera surveillance

To apply the general criteria set out in paragraph 4.1 consistently, EUR uses a system of location categories. The underlying premise is that camera surveillance is a structural part of the safety design in some areas, whereas in other areas it may only be used after a specific risk analysis, in other situations it can be considered only in highly exceptional cases, and in some places, it is not appropriate at all.

This system avoids *ad hoc* decisions and makes the use of camera surveillance predictable, transparent and understandable. The categories are further elaborated in paragraphs 4.2.1 to 4.2.4.

4.2.1 Locations with a structural need for camera surveillance

These are locations where camera surveillance is always, or as a rule, used because, when designing the safety measures, it was determined that camera surveillance is a necessary measure within EUR's broader safety approach. For these locations it has, in general terms, been substantiated that camera surveillance is necessary, proportionate and subsidiary, and that the balance of privacy interests is acceptable. This justification is set out in this Policy Framework, the LIA and the DPIA for camera surveillance.

For proposals for new or modified camera positions in these locations, a full balancing of interests does not need to be repeated each time. The assessment focuses on whether:

- the proposed camera fits within the general objectives, scope and safeguards for this category; and
- there are no specific circumstances that argue against installing a camera at the location concerned.

This category includes at least the following types of locations:

Entrances Campus Woudestein and buildings

The grounds of Campus Woudestein and the buildings on those grounds have a public character, with multiple physical access routes and open connections to public space. In practice, this makes it difficult to detect unwanted visitors in good time. This hampers both the prevention of incidents, because early intervention by the campus security becomes more difficult, and the possibility of investigation and follow-up afterwards, because usable footage is often not available.

To mitigate these risks, while maintaining the open character of the campus and buildings as far as possible, EUR installs fixed cameras at all access routes to the grounds and at the entrances and exits of buildings. These cameras are directed at the immediate access zones and not at areas where people stay. They are not used to follow the conduct of individuals over longer periods, but solely to gain insight into who enters and leaves the grounds and buildings, for the purpose of safety and incident handling.

Alternative measures, such as more intensive patrols or additional physical barriers, would only be effective at higher cost and with a greater impact on the accessibility and use of the campus. From the perspective of subsidiarity, camera surveillance is therefore used as an additional measure, in combination with existing measures such as lighting, the design of walking routes and the presence of security staff.

Central outdoor areas and spaces between buildings on Campus Woudestein

At Campus Woudestein, EUR also uses a coherent network of cameras, limiting the number of blind spots as far as possible. In terms of its size and the number of buildings, Campus Woudestein is such that effective monitoring by physical presence of security staff alone is not feasible in practice. The camera network enables the campus security to gain an adequate level of situational awareness within a short period in the event of an incident, so that appropriate measures can be taken and the emergency services can be directed where necessary.

The network of fixed cameras and PTZ cameras allows the control room operator, in the event of an incident, to gain targeted visibility of the situation, for example by directing a PTZ camera at the location concerned. In exceptional situations, the network can also be used, solely manually and not via AI-based systems, to follow a person for a limited period across (part of) the grounds. This is only permitted where there is a concrete reason and a reasonable suspicion, and only where necessary for the purposes of camera surveillance as set out in this Policy Framework, for example in the case of seriously undesirable or threatening behaviour or where a suspicious situation moves across campus. Such monitoring is limited to the relevant route and period and is not used for structural behaviour monitoring of individuals.

An alternative, such as structurally deploying more security staff on the grounds or (temporarily) closing off parts of the campus, would have a greater impact on day-to-day accessibility and use of the campus, and would not provide the same level of overview and ability to respond quickly. Against this background, the coherent camera network on Campus Woudestein is regarded as a necessary and, in relation to the risks and available alternatives, proportionate measure.

Car parks

In EUR car parks, a comprehensive network of CCTV cameras is used. This network has a dual purpose. Primarily, it serves to protect people in emergencies: it provides direct insight into the situation and makes it possible to determine whether people are still present, for example in the event of fire or another emergency situation. In addition, the camera network helps to reduce property offences, such as theft and vandalism. Studies of comparable locations show that camera surveillance in car parks can have a significant preventive effect on such incidents.¹

Business-critical IT infrastructure

Within EUR's camera surveillance, particular attention is paid to business-critical IT infrastructure. This includes data centres and other IT facilities classified as business-critical. Camera surveillance is always used at these locations. EDIS and Integral Safety jointly determine this classification.

The primary purpose is to ensure and strengthen information security. Camera surveillance helps to prevent, detect and investigate unauthorised access and is therefore an important part of the physical security measures around business-critical IT infrastructure. EUR also considers this camera surveillance necessary in order to comply with ISO 27001/27002 standards and the associated requirements for the physical security of data centres and other critical IT facilities.

Given the specific function of these rooms, their strictly limited access and the fact that they are only entered for technical and management work, the impact on the privacy of staff and students is limited.

¹ See, for instance: Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2019). CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology & Public Policy*, 18(1), 135–159. <https://doi.org/10.1111/1745-9133.12419>

4.2.2 Locations where camera surveillance is permitted under conditions

These are locations where camera surveillance is not used as standard, but where it may be an appropriate measure depending on the circumstances. For each camera, a separate risk analysis is carried out and an explicit assessment is made of whether camera surveillance is necessary, proportionate and subsidiary. It is also assessed whether the balancing of interests and safeguards in the LIA and DPIA adequately cover the proposed use, or whether additional measures are needed. Decision-making on camera surveillance at these locations follows the procedure in Article 4.2 of the Camera Surveillance Regulations EUR 2026.

This category includes at least the following types of locations:

Camera surveillance in buildings: central areas and access to office areas

Within EUR buildings, camera surveillance is used sparingly. EUR consciously weighs safety, privacy and the preservation of an open and pleasant working and study environment. Although incidents such as theft and burglary have occurred in the past, where a more extensive camera network might have helped in gathering evidence, this does not, in EUR's view, outweigh the negative effects of large-scale use of cameras inside buildings.

In addition to cameras at entrances and exits, EUR may use camera surveillance in central areas within buildings, such as central entrance halls and public areas adjacent to lecture rooms (but not the lecture rooms themselves), main corridors, stairwells and lift lobbies. This use is primarily intended to monitor flows of people and to detect incidents at an early stage.

In office areas with an increased risk of unauthorised access, EUR may use camera surveillance at the access point. This camera surveillance is always part of a broader set of security measures, as described in EUR's access and compartmentalisation policy. EUR ensures that only the access point to the office area is filmed, and not adjacent workstations. Such camera positions may also be installed at a substantiated request from an Administrator for the benefit of their service or faculty.

Other high-risk areas

In addition, there are specific areas where there is an increased risk of incidents, property offences or unauthorised access, and where camera surveillance may be an appropriate additional measure. These areas are identified in a risk analysis. Examples include:

- technical rooms where unauthorised access poses safety or continuity risks (for example rooms with air-handling installations);
- Main Equipment Rooms (MER) and Satellite Equipment Rooms (SER), where (vital) IT infrastructure is located. Depending on the location and function of these rooms, there may be an increased risk of unauthorised access, or the functioning of vital facilities may directly depend on their availability and integrity;
- locations where previous incidents or a specific threat have been identified;
- art storage and galleries;
- storage of examination papers and IT equipment used during examinations;
- storage of certificates and diplomas;
- mail and logistics rooms;
- bicycle parking facilities.

This list is illustrative and not exhaustive.

4.2.3 Locations where camera surveillance is in principle not permitted

These are locations where camera surveillance is, in principle, not used because the interference with privacy is significant. This includes:

- office areas and workstations;
- study spaces and self-study rooms;
- teaching rooms.

In these rooms, cameras are not installed for regular safety purposes. Only in very exceptional, compelling cases, where there is a concrete and specific threat to the safety of individuals and less intrusive measures have proven insufficiently effective, may temporary additional camera surveillance be considered.

Such a proposal is dealt with under the additional procedure in Article 4.3(5) of the Camera Surveillance Regulations EUR 2026. The request is assessed by the Camera Surveillance Review Team and the Data Protection Officer. The maximum duration of such deployment is three months, with no possibility of extension or conversion into permanent camera surveillance.

It may occur that a camera installed at a location referred to in paragraphs 4.2.1 or 4.2.2 also has (partial) visibility of a workstation. This may, for example, be the case for a camera in a central hall where there is also a catering facility. In such cases, EUR ensures that the camera is positioned in such a way that the workstation is not structurally in view. Where this is not (fully) possible, the part of the image in which the workstation is visible is permanently masked in the camera system software.

4.2.4 Locations where camera surveillance is never permitted

Finally, there are locations where camera surveillance is completely excluded, regardless of the circumstances. This exclusion directly reflects Article 4.1(5) of the Camera Surveillance Regulations EUR 2026. Camera surveillance does not take place here in any form (permanent, temporary or covert). This concerns at least:

- toilets, showers and changing rooms;
- rooms for confidential conversations, such as consultation rooms or counselling rooms;
- special rooms such as quiet and meditation rooms, and lactation rooms.

For these locations, any safety issues must always be addressed by other means, such as physical presence of security staff, structural measures or organisational arrangements, and not through camera surveillance. Deviation from this exclusion is not possible under Article 4.1(5) of the Camera Surveillance Regulations EUR 2026.

4.3 External EUR locations (ISS, EUC, C&C Putselaan)

At external locations managed by EUR, such as ISS, EUC and C&C Putselaan, camera surveillance may also be a structural part of the safety design. As a starting point, the same principles and location categories apply as set out in this chapter.

The nature and surroundings of these locations differ from Campus Woudestein: they are buildings in an urban environment, with different public spaces and usage patterns. The Camera Plan for these locations is therefore based on a specific risk analysis for each location. On that basis, EUR may make different choices in the use of camera surveillance than on Campus Woudestein, for example in the balance between cameras on the exterior and cameras in internal circulation areas, provided these choices are in line with this Policy Framework and implemented in accordance with the procedures in the Camera Surveillance Regulations EUR 2026.

5 Privacy and safeguards

As described earlier, there is an inherent tension between the use of camera surveillance and the protection of the privacy of those concerned. EUR therefore applies clear criteria for the use of camera surveillance and takes measures to mitigate its impact as far as possible. These measures are partly based on legal obligations and compliance requirements, and partly reflect EUR's conviction that the use of camera surveillance must be careful, restrained and responsible.

5.1 Legal basis for processing of data

The legal basis for processing of data is legitimate interest (Article 6(1)(f) GDPR). The relevant interest is to provide a safe environment and to maintain order in EUR buildings and on EUR grounds. On this basis, the Executive Board may adopt rules and, among other things, prescribe that instruments such as camera surveillance be used in certain situations.² The legal basis and purposes of camera surveillance are further set out in Article 1.2 of the Camera Surveillance Regulations EUR 2026. Processing and any further processing of personal data takes place only insofar as it is compatible with the purposes identified in those Regulations (i.e., purpose limitation).

In line with the GDPR, EUR further details this legal basis and the associated balancing of interests in:

- a Legitimate Interest Assessment (LIA), in which EUR's legitimate interests are identified and weighed against the interests and rights of data subjects;
- a Data Protection Impact Assessment (DPIA), in which the privacy risks of the camera system are mapped and appropriate mitigating measures are determined.

The LIA and DPIA relate to the camera surveillance system as a whole and form the basis for assessing specific requests for camera surveillance.

5.2 Safeguards

To limit the impact of camera surveillance on the privacy of students, staff and visitors, EUR has put in place a coherent set of physical, technical and organisational safeguards, complemented by independent oversight and participation.

The physical safeguards include the security measures for the central control room and the rooms in which the camera system equipment is located. These rooms are not freely accessible and may only be entered by a limited number of authorised staff, thereby restricting the group of people who can view camera footage. Screens showing live footage are positioned in such a way as to prevent unauthorised viewing as far as possible.

² Artikel 7.57h WHW

The technical safeguards relate to information security and the configuration of the camera system. The camera system complies with the requirements laid down in EUR's privacy and information security policies; the service units RE&F and EDIS jointly ensure IT and information security. Within the camera system, logging and an audit trail are used so that unauthorised use or misuse of camera footage can be detected and subsequently reviewed. Where necessary, parts of the image are permanently masked, for example where workstations or other sensitive zones would otherwise be visible.

EUR also deliberately deviates from the commonly used retention period of 28 days: where no incident has been identified, footage is automatically and irreversibly deleted after no more than fourteen days, unless there is an incident or a request from a data subject as referred to in the Camera Surveillance Regulations EUR 2026.

In addition to these active technical safeguards, EUR also explicitly refrains from using certain functionalities of the CCTV system. For example, the audio-recording function of cameras is disabled. EUR also explicitly does not use AI-based applications such as facial recognition or automated tracking of individuals. If the CCTV system used by EUR contains such functionalities, they are disabled by default and not available for use. In addition, it is contractually stipulated that suppliers of the CCTV system may not process EUR data for the training of AI models.

The decision not to use AI applications is a conscious one. Smart software could theoretically enhance privacy, for example by allowing a camera normally to remain "blank" and only alert the control room operator when an incident is detected. At present, however, EUR considers the risks too great, for example risks of ethnic profiling or unlawful processing of personal data. In EUR's view, these risks currently outweigh the potential benefits.

As a limited exception, EUR may use intelligent motion detection. This functionality is used outside opening hours to alert the control room operator in a targeted way to possible irregularities. Cameras only generate an alarm when they detect specific movements, such as the presence of persons or vehicles, and not for every random change in the image. The analysis required for this motion detection takes place locally in the camera and does not use any cloud-based applications.

The organisational safeguards concern access to, use of and control over the camera system. Access to the camera system and to camera footage is restricted and governed by an authorisation matrix, which is attached to this Policy Framework as an annex and managed in accordance with Article 3.4 of the Camera Surveillance Regulations EUR 2026. Only a limited number of staff members have access to camera footage by virtue of their role. The Head of EUR Security manages the authorisations, reviews them periodically and ensures that staff members are instructed in advance on the proper use of the camera system and the handling of personal data. Security staff, including control room operators, are screened before they are allowed to work with the camera system and receive targeted training on its use. EUR is cautious in sharing live footage and recorded footage with third parties; the conditions under which access and disclosure are permitted are set out in Chapter V of the Camera Surveillance Regulations EUR 2026.

The overall set of safeguards, and compliance with the privacy framework, is overseen by the Chief Privacy Officer (CPO) and the Data Protection Officer (DPO), as described in Chapter II of the Camera Surveillance Regulations EUR 2026. They independently assess whether camera surveillance complies with the GDPR and with internal privacy and security policies, advise on risks and mitigating measures, and may carry out or commission audits of the design and use of the camera system. They also monitor the implementation of the measures and balancing of interests set out in the LIA and DPIA.

In addition, the University Council has a supervisory role. The Executive Board reports annually to the University Council on the use of camera surveillance, including changes to the Camera Plan and the authorisation matrix, the deployment of temporary additional camera surveillance and covert camera surveillance, and access to and disclosure of camera footage to third parties, in accordance with the provisions of the Regulations.

6 Application and evaluation

6.1 Interpretation

In matters relating to the subjects governed by this Policy Framework, in which this Policy Framework does not provide, or where this Policy Framework gives rise to multiple interpretations, the Executive Board shall decide.

6.2 Management of Policy Framework

This Policy Framework is managed by the General Management Directorate (ABD), service unit Administrative Affairs (BZ), Team Integral Safety.

6.3 Translation

If this Policy Framework is translated and a discrepancy arises between the English translation and the Dutch text, the Dutch text shall prevail.

6.4 Entry into force, duration and evaluation

This Policy Framework shall enter into force on 1 October 2026, after approval by the University Council and adoption by the Executive Board.

This Policy Framework shall have a maximum duration of five years and shall in any event expire on 30 July 2031. After four years, an evaluation of this Policy Framework shall take place, on the basis of which a revised Policy Framework shall be developed. If circumstances so require, the Executive Board may adopt amendments to this Policy Framework at an earlier point in time than the period referred to in the second sentence, provided that the University Council has approved those amendments.

6.5 Short title

This Policy Framework may be cited as: Camera Surveillance Policy Framework EUR 2026.

Annex 1 – Authorisation matrix

The following types of authorisations are distinguished:

- A. live viewing of camera footage;
- B. viewing camera footage stored within the regular retention period;
- C. viewing camera footage stored beyond the regular retention period;
- D. storing camera footage beyond the regular retention period in accordance with Article 3.2 of the Camera Surveillance Regulations EUR 2026;
- E. editing stored camera footage (blurring or sharpening certain parts of the footage; exporting);
- F. granting the police access to live footage during an incident in accordance with Article 5.1 of the Camera Surveillance Regulations EUR 2026;
- G. granting access to and sharing of stored camera footage with third parties in accordance with Article 5.2 of the Camera Surveillance Regulations EUR 2026;
- H. granting access to stored camera footage to data subjects in accordance with Article 5.3 of the Camera Surveillance Regulations EUR 2026;
- I. live viewing of camera footage for the purposes of technical checks, maintenance, adjustments and installation.

The following officers have, by virtue of their position and/or tasks, a structural need for specific types of access to the camera system and to the camera footage and data obtained through camera surveillance:

Function	A	B	C	D	E	F	G	H	I
Advisor Integral Safety and Head of EUR Security	x	x	x	x	x	x	x	x	x
Privacy Officer ABD, CPO, DPO	x	x	x						
Operations Manager EUR Security	x	x		x ³		x			x
Control room operators	x	x				x			
Security officers	x	x							
Staff employed by the Contractor under RE&F who carry out technical checks, maintenance or installation activities for the camera system									x

³ The Operations Manager EUR Security has, within the software system, the authorisation to retain Camera Footage beyond the regular retention period. This is purely an operational role; the decision to store Camera Footage for a longer period is always taken by the Advisor Integral Safety or the Head of EUR Security.