

Erasmus University Rotterdam Camera Surveillance Regulations 2026–2031

These Regulations were adopted by the Executive Board on 22 September 2026.

These Regulations were approved by the University Council on 16 July 2026.

These Regulations shall enter into force on 1 October 2026.

Department : ABD, BZ, Integral Safety & Security

Version : 0.44EN

Contents

Chapter I – Purpose, Scope and Principles	2
Article 1.1 – Introduction	2
Article 1.2 – Purpose and legal basis of Camera Surveillance	2
Article 1.3 – Scope of the Regulations	2
Article 1.4 – Hierarchy and governance	2
Chapter II – Roles and responsibilities	3
Article 2.1 – Executive Board	3
Article 2.2 – Operation and system administration (first-line Officers)	3
Article 2.3 – Risk management and compliance (second-line Officers)	3
Article 2.4 – Independent oversight and participation (third-line Officers)	4
Chapter III – Recording, use and security of Camera Footage	4
Article 3.1 – Use of Camera Footage and types of Data	4
Article 3.2 – Retention period for Camera Footage	4
Article 3.3 – Authorisation and confidentiality in accessing Camera Footage	5
Article 3.4 – Physical security and locations for viewing Camera Footage	5
Chapter IV – Establishing and modifying Camera Surveillance	5
Article 4.1 – Policy framework, Camera Plan and exclusions	5
Article 4.2 – General procedure for requesting and implementing Camera Surveillance	6
Article 4.3 – Additional provisions for temporary additional Camera Surveillance	6
Article 4.4 – Separate procedure for Covert Camera Surveillance	6
Chapter V – Access, sharing and rights of Data Subjects	7
Article 5.1 – Access to live Camera Footage by the police	7
Article 5.2 – Access to and sharing of Camera Footage with Third Parties	7
Article 5.3 – Rights of Data Subjects	8
Chapter VI – Record-keeping and reporting	8
Article 6.1 – Registration and internal reporting on Camera Surveillance	8
Article 6.2 – Annual reporting to the University Council	8
Chapter VII – Final and transitional provisions	9
Article 7.1 – Interpretation	9
Article 7.2 – Management of the Regulations	9
Article 7.3 – Translation	9
Article 7.4 – Publication	9
Article 7.5 – Entry into force, duration and evaluation	9
Article 7.6 – Short title	9
Article 7.7 – Repeal	9
Chapter VIII – Definitions	10

Chapter I – Purpose, Scope and Principles

Article 1.1 – Introduction

These Regulations apply to all locations of EUR where Camera Surveillance is carried out by means of fixed and mobile Cameras.

They set out the framework and procedures relating to all aspects of Camera Surveillance, with a view to the proper and responsible use of the Camera System and the protection of the privacy of Students, Officers and Third Parties present in EUR Buildings and on EUR Grounds.

Article 1.2 – Purpose and legal basis of Camera Surveillance

1. The deployment of Camera Surveillance, and the use and recording of Camera Footage, shall take place solely for the following purposes:
 - a. safeguarding and protecting the safety and health of all persons present in EUR Buildings or on EUR Grounds;
 - b. safeguarding and protecting EUR Buildings, Grounds, facilities and property;
 - c. preventing, detecting, and responding to Incidents;
 - d. recording Incidents for the subsequent investigation and prosecution of (alleged) criminal offences and for the analysis of Incidents.
2. The legal basis for the Processing is Legitimate Interest (Article 6(1)(f) GDPR). EUR shall only use Camera Surveillance where this is necessary and proportionate and where less intrusive measures are not effective (subsidiarity). EUR will always make a careful assessment between, on the one hand, the protection of the privacy of Data Subjects and, on the other hand, the interests of EUR. This assessment is further elaborated in the Policy Framework.
3. Processing and further processing of Data and Personal Data shall take place solely insofar as it is compatible with the purposes referred to in paragraph 1.

Article 1.3 – Scope of the Regulations

1. These Regulations apply to all persons present in EUR Buildings or on EUR Grounds.
2. These Regulations cover all fixed and mobile Cameras in all Buildings and on all Grounds that are used by EUR for the purposes of Camera Surveillance in line with the objectives described in Article 1.2(1) of these Regulations.
3. Cameras used for the following purposes fall, in any event, outside the scope of these Regulations:
 - a. use of Cameras for the recording and broadcasting of lectures, academic ceremonies and other events;
 - b. use of Cameras for the conduct of meetings;
 - c. use of Cameras in the context of scientific research;
 - d. use of Cameras for proctoring or invigilation during (online) tests and examinations;
 - e. use of license-plate recognition Cameras for car park management.
4. Tenants of EUR, as well as Third Parties who own a Building situated on land made available by EUR under a ground lease or building right, and who do not fall under the hierarchical responsibility of the Controller, are themselves Controllers for the Camera Footage that they generate with their own system. The way in which they have organised their Camera Surveillance must comply with the GDPR and may not conflict with the provisions of these Regulations.
5. Where paragraph 4 applies, EUR shall receive the information required on the setup of the Camera Surveillance, as agreed in the tenancy agreement, user agreement, ground lease or building rights agreement with the Third Party.

Article 1.4 – Hierarchy and governance

1. Camera Surveillance is, first and foremost, governed by the applicable legislation and regulations. Where provisions of these Regulations conflict with higher-ranking legislation or regulations, that legislation or those regulations shall prevail.
2. These Regulations set out the binding framework for Camera Surveillance within EUR. Policy documents, including the Policy Framework, provide further detail to these Regulations and are therefore subordinate to them.

3. In designing, implementing and monitoring Camera Surveillance, EUR applies the so-called "three lines of defence" model. This model means that (i) line management bears primary responsibility for careful implementation, (ii) independent functions monitor compliance and advise on risks and control measures, and (iii) internal audit independently assesses whether the system of control measures is functioning effectively. These roles are further elaborated in Chapter II of these Regulations.

Chapter II – Roles and responsibilities

Article 2.1 – Executive Board

1. The Executive Board is authorised to issue rules and take measures relating to the proper order within the Buildings and on the Grounds of the institution.¹
2. The Executive Board bears ultimate responsibility for the Processing of Personal Data within EUR and is therefore responsible for Camera Surveillance.

Article 2.2 – Operation and system administration (first-line Officers)

1. The Head of EUR Security designs the Camera Plan in accordance with the framework laid down in these Regulations and the Policy Framework. In this capacity, the Head of EUR Security acts as the applicant for Camera Surveillance.
2. Security Guards, employed by a Contractor or by EUR, are responsible for operating the Camera System and viewing Camera Footage. This forms part of the detection of and response to irregularities, under the direct supervision of the Operations Manager EUR Security.
3. The technical maintenance of the Camera System, as well as the installation of new Cameras, is carried out by Officers employed by a Contractor, under the coordination of the Director of RE&F.
4. Officers employed by EUR or by a Contractor ensure, under the coordination of the Director of EDIS, the IT security of the Camera System. They ensure that the system at all times complies with the applicable technical and security standards, the EUR privacy and information security policies and applicable legislation and regulations. For the Contractors referred to in paragraphs 2, 3 and 4, a work instruction has been drawn up which sets out the rules, arrangements and instructions regarding access to and use of the Camera System and Camera Footage.

Article 2.3 – Risk management and compliance (second-line Officers)

1. The service unit Administrative Affairs, Team Integral Safety & Security, is responsible for drafting and updating these Regulations and the Policy Framework, and for advising on their application within EUR.
2. The Advisor Integral Safety & Security (Administrative Affairs), the Privacy Officer ABD (Legal Affairs) and the Service Manager Park Management/CCTV (RE&F) jointly form the Camera Surveillance Review Team.
3. The University Council may appoint from among its members a representative who will participate in the Camera Surveillance Review Team as an advisory member. If the University Council makes use of this option, it shall also appoint a deputy. The representative contributes to the balancing of interests by the Review Team from the perspective of students and staff.
4. In cases where an application cannot be postponed, the representative will be given the opportunity to provide his or her advice within 48 hours; the absence of a response within this period does not prevent the Review Team from taking a decision.
5. The members of the Camera Surveillance Review Team treat as confidential all information they receive in the course of their duties. They do not disclose any information about individual applications or internal deliberations.
6. By way of derogation from paragraph 5, the representative of the University Council may share positive recommendations of the Camera Surveillance Review Team with the University Council in a closed meeting.
7. The Camera Surveillance Review Team is responsible for assessing:
 - a. applications for permanent Camera Surveillance as referred to in Article 4.2;
 - b. applications for temporary additional Camera Surveillance as referred to in Articles 4.2 and 4.3;
8. Where the nature or complexity of an application so requires, the Camera Surveillance Review Team may involve additional internal or external expertise in the assessment.

¹ Article 7.57h WHW

9. The Camera Surveillance Review Team oversees the performance and updating of a DPIA for:
 - a. these Regulations and the Policy Framework;
 - b. the use of Covert Camera Surveillance as described in Article 4.4.
 The Camera Surveillance Review Team reports on the DPIA to the Executive Board and advises on necessary measures.

Article 2.4 – Independent oversight and participation (third-line Officers)

1. The Chief Privacy Officer (CPO) is responsible for safeguarding the privacy framework and for overseeing the careful Processing of Personal Data in the context of Camera Surveillance.
2. The Data Protection Officer (DPO) performs, in relation to Camera Surveillance, an independent supervisory role. The DPO performs their statutory tasks without substantive instruction and reports directly to the Executive Board.
3. In the context of Camera Surveillance, the DPO oversees the Processing of Personal Data and compliance with the resulting statutory obligations, and is authorised to conduct audits. The findings are reported to the Executive Board.
4. The University Council has the right of consent in respect of these Regulations and the Policy Framework.
5. The University Council also has an oversight role in relation to Camera Surveillance. In that context, the University Council receives an annual report from the Executive Board as referred to in Article 6.2.

Chapter III – Recording, use and security of Camera Footage

Article 3.1 – Use of Camera Footage and types of Data

1. The collection and Processing by EUR of Data and Personal Data obtained through Camera Surveillance shall only be permitted for the purposes referred to in Article 1.2(1) of these Regulations.
2. The Data and Personal Data that are Processed are:
 - a. Camera Footage in and around the immediate vicinity of the Buildings, as well as of the exterior of those Buildings and the Grounds;
 - b. Data relating to the date and time at which, and the place where, the Camera Footage was recorded.
3. The Cameras have the technical capability to record audio. EUR does not use this functionality.
4. Editing of Camera Footage shall only take place for the purpose of enhancing or obscuring specific parts of that Camera Footage.

Article 3.2 – Retention period for Camera Footage

1. Insofar as Camera Footage is stored in the Camera System, such Camera Footage shall be automatically and irreversibly deleted no later than fourteen days after recording, unless:
 - a. the Camera Footage relates to an Incident. In that case, the relevant Camera Footage shall be retained for as long as necessary for further investigation and any measures to be taken, and until the Incident has been handled. After the Incident has been handled, the relevant Camera Footage (and any copies or printouts made) shall be destroyed. If legal proceedings ensue, the images shall be preserved until a court judgment has become final and binding;
 - b. a request has been submitted by a Data Subject in relation to the Camera Footage and/or Personal Data. In that case, the Camera Footage shall be retained until the procedure for handling the request has been completed.
2. The Head of EUR Security or the Advisor Integral Safety & Security shall determine whether there are grounds as referred to in paragraph 1 to extend the retention period and shall instruct that the relevant Camera Footage be secured.
3. Where there is uncertainty regarding the applicability of the exceptions referred to in paragraph 1, the Head of EUR Security or the Advisor Integral Safety & Security shall consult the Privacy Officer ABD.

Article 3.3 – Authorisation and confidentiality in accessing Camera Footage

1. Only those Officers who, by virtue of their role and/or tasks, require access to Camera Footage and Data for the purposes referred to in Article 1.2 shall be granted access. Such access is laid down in an authorisation matrix, which is attached as an appendix to the Policy Framework. The authorisation matrix is maintained by the Team Integral Safety & Security.
2. The Head of EUR Security or the Advisor Integral Safety & Security may, in deviation from the authorisation matrix, temporarily authorise Officers to exercise additional powers, subject to any conditions attached to that authorisation and solely for a predefined task or activity.
3. All Officers who become aware of Data and Personal Data obtained from Camera Footage shall treat such information as confidential and handle it with due care, in accordance with the GDPR and EUR policies. To this end, they receive instructions before being granted access. Insofar as this is not already provided for under employment law, the responsible Administration Unit shall conclude a confidentiality agreement with the Officers concerned.
4. The Head of EUR Security shall maintain a record of all Officers who have been granted authorisation. The Head of EUR Security shall review access rights to the Camera System at least annually, in order to minimise the risk of unauthorised access.

Article 3.4 – Physical security and locations for viewing Camera Footage

1. The Central Control Room, the Server Room and the room in which the technical maintenance of the Camera System is carried out are equipped with an access control system and are only accessible to Officers authorised to access those rooms.
2. Camera Footage shall only be viewed at the location designated as the Central Control Room.
3. By way of exception to paragraph 2, Camera Footage may be viewed at the reception desks at the EUC, ISS and Putselaan locations. In such cases, the monitors are positioned in such a way that the images can be viewed for any length of time only by the Security Guard or receptionist on duty.
4. During crisis situations, Camera Footage may be viewed in rooms other than those referred to in paragraph 2. In such situations, technical and organisational measures shall be taken to prevent unauthorised viewing as far as is reasonably possible.

Chapter IV – Establishing and modifying Camera Surveillance

Article 4.1 – Policy framework, Camera Plan and exclusions

1. The basis for Camera Surveillance at EUR is permanent Camera Surveillance using fixed Cameras. In addition, EUR may deploy temporary additional or Covert Camera Surveillance using fixed or mobile Cameras.
2. The Policy Framework describes these forms of Camera Surveillance and sets out the framework within which the different forms are applied.
3. The location, purpose and type of Cameras used within permanent Camera Surveillance are laid down in the Camera Plan. The Camera Plan is drawn up in accordance with these Regulations and the location categories and associated conditions set out in the Policy Framework.
4. As a rule, Camera Surveillance shall not be applied in areas where the interference with privacy is significant. This shall in any event include:
 - a. office areas and workstations;
 - b. study areas and self-study rooms;
 - c. teaching rooms.

Only in very exceptional, compelling cases, where there is a specific and concrete threat to the safety of persons, may temporary additional Camera Surveillance be deployed in such areas.

5. Camera Surveillance shall under no circumstances take place in areas by their nature incompatible with Camera Surveillance. This shall in any event include:
 - a. toilets and showers;
 - b. changing rooms;
 - c. rooms for confidential conversations, such as consultation rooms or counselling rooms;
 - d. special rooms such as quiet and meditation rooms, and lactation rooms;
 - e. rooms of a similar nature.

Article 4.2 – General procedure for requesting and implementing Camera Surveillance

1. This Article sets out the general procedure for requesting and implementing Camera Surveillance.. This procedure applies without limitation to permanent Camera Surveillance and likewise to temporary additional Camera Surveillance, unless Article 4.3 expressly provide otherwise.
2. The Head of EUR Security shall act as the applicant for permanent and temporary additional Camera Surveillance. In addition, an Administrator may submit, for their Administration Unit, an application for the installation of additional Cameras.
3. Applications shall be submitted to the Camera Surveillance Review Team. The Camera Surveillance Review Team shall assess each application with regard to:
 - a. compliance with these Regulations and the Policy Framework;
 - b. necessity, proportionality and subsidiarity, insofar as these are not already set out in the Policy Framework;
 - c. the balancing of interests between the interests of Data Subjects and the interests of EUR, insofar as this does not already follow from the DPIA;
 - d. the technical feasibility and cost of installation.

On this basis, the Camera Surveillance Review Team shall issue a reasoned recommendation in Writing.

4. As an additional safeguard, the CPO shall independently review the recommendation of the Camera Surveillance Review Team. This review shall be marginal in nature and shall focus in particular on the balancing of interests carried out.
5. If the Camera Surveillance Review Team issues a positive recommendation on the application and the CPO raises no objections, the application shall be granted. Where the application concerns permanent or temporary additional Camera Surveillance, RE&F shall ensure installation.
6. If the Camera Surveillance Review Team establishes that Camera Surveillance is necessary, but either the Camera Surveillance Review Team or the CPO issues a negative privacy opinion, the application shall be submitted to the DPO for assessment.
7. The DPO shall issue a written recommendation on the application, which shall be followed by EUR. If the recommendation is positive, the application shall be granted; if the recommendation is negative, the application shall be rejected.

Article 4.3 – Additional provisions for temporary additional Camera Surveillance

1. Temporary additional Camera Surveillance may only be deployed where the reason for, purpose of and necessity for the Camera Surveillance can reasonably be expected to be of a temporary nature.
2. Temporary Camera Surveillance shall be deployed for a period of no more than six months. This period may be extended once, by an immediately subsequent period of no more than six months.
3. When assessing an application as referred to in Article 4.2(3), the Camera Surveillance Review Team shall determine the purpose and duration of the temporary additional Camera Surveillance.
4. After expiry of the period referred to in paragraph 2, the Camera Surveillance Review Team shall evaluate the deployment of the temporary additional Camera Surveillance and decide whether to extend or terminate it, or – where there is a structural need – to convert it into permanent Camera Surveillance. In the event of conversion into permanent Camera Surveillance, the procedure referred to in Article 4.2 shall be followed anew.
5. By way of derogation from the procedure referred to in Article 4.2, temporary additional Camera Surveillance at the locations referred to in Article 4.1(4) shall only be deployed after review by the Camera Surveillance Review Team and a positive recommendation in Writing from the DPO, which shall be followed by EUR. By way of derogation from paragraphs 2 and 4 of this Article, such Camera Surveillance shall only be deployed for a period of no more than three months and may not be extended or converted into permanent Camera Surveillance.

Article 4.4 – Separate procedure for Covert Camera Surveillance

1. By way of derogation from Article 4.2, only the procedure set out in this Article shall apply to the deployment of Covert Camera Surveillance.
2. Covert Camera Surveillance shall only be deployed where normal Camera Surveillance and other measures taken by EUR have not resulted in the cessation of structural Incidents, and where there are well-founded suspicions of criminal offences or other seriously reprehensible behaviour.

3. Covert Camera Surveillance shall be deployed for a period of no more than one month and may be extended once, by an immediately subsequent period of no more than one month. Camera Surveillance shall be deployed in such a way that the interference with the privacy of Students, Officers and Third Parties is kept to a minimum.
4. Covert Camera Surveillance shall only be permitted with the prior written consent of the Executive Board, stating the purpose, duration and conditions under which the Covert Camera Surveillance will be deployed.
5. The Head of Integral Safety & Security may submit a request to the Executive Board for the deployment of Covert Camera Surveillance.
6. The proposed decision to deploy Covert Camera Surveillance shall, prior to deployment, be reviewed by the DPO, who shall issue a recommendation in Writing.
7. The Executive Board shall inform the University Council without delay after termination of the Covert Camera Surveillance. In doing so, the Executive Board shall provide information on the purpose and duration of the deployment and shall submit the DPO's recommendation.
8. The Students, Officers and Third Parties concerned shall, insofar as reasonably possible, be informed after the deployment has ended about the Covert Camera Surveillance that was applied.
9. Where the Covert Camera Surveillance (also) relates to (a member of) the Executive Board, "Executive Board" in this Article shall be read as "Supervisory Board".

Chapter V – Access, sharing and rights of Data Subjects

Article 5.1 – Access to live Camera Footage by the police

1. The Camera System is configured in such a way that, at the request of EUR or at the request of the police, it is possible to grant the police access to live Camera Footage.
2. Live Camera Footage shall only be shared where this is:
 - a. necessary for the protection of the vital interests of the Data Subject or of another natural person;
 - b. necessary for the general public interest relating to public order, national security and/or the national interest;
 - c. necessary for the protection of the interests of EUR, insofar as this concerns criminal offences that have been, or on the basis of facts and circumstances are expected to be, committed against EUR or against persons in its service.
3. The Control Room Operator may determine, whether or not after consultation with the Head of EUR Security or the Advisor Integral Safety & Security, whether it is necessary for the police to view live Camera Footage.
4. The Control Room Operator shall contact the police and activate the switch so that the live Camera Footage is shown. As soon as the need for the police to view the live Camera Footage has ceased, the switch shall be deactivated and the police shall no longer have access to the Camera Footage.
5. The live viewing of Camera Footage by the police shall be recorded by the Control Room Operator.

Article 5.2 – Access to and sharing of Camera Footage with Third Parties

1. Upon demand or order by Law Enforcement Authorities or the Intelligence Agency, access may be granted to (recorded) Camera Footage in the context of the performance of their public-law tasks or on the basis of a statutory provision.
2. Camera Footage shall only be shared upon demand by the police or on the basis of a written order by the examining magistrate or (assistant) public prosecutor, where such demand or order has a statutory basis.
3. Any request, demand or written order from Third Parties shall be addressed to the Head of EUR Security or the Advisor Integral Safety & Security.
4. The Camera Footage and Data shall be transferred in a secure manner by the Head of EUR Security or the Advisor Integral Safety & Security to the Third Party, with the representative of the relevant Third Party signing for access to and/or sharing of the Camera Footage.
5. Access to and sharing of Camera Footage shall be recorded by the Head of EUR Security.

6. EUR may, without a prior request, demand or order from a Third Party, share Camera Footage already collected with Law Enforcement Authorities if and insofar as:
 - a. such sharing is compatible with the purposes of the Processing as described in Article 1.2(1) of these Regulations and, in doing so, due account is taken of the nature of the data, the relationship between EUR and the Data Subject and the consequences for the Data Subject; or
 - b. such sharing is necessary on the basis of legislation to safeguard national security, public security, the investigation and prosecution of criminal offences, and the protection of the rights and freedoms of Data Subjects or others, such as:
 - i. EUR's public task under the WHW to ensure a safe working and learning environment;
 - ii. the protection of the interests of EUR in respect of criminal offences that have been, or are expected to be, committed against EUR or its Staff (UAVG);
 - iii. the establishment, exercise or defence of legal claims (UAVG).

In assessing any sharing, the Data Protection Officer shall be actively involved. Paragraphs 4 and 5 shall apply *mutatis mutandis*.
7. No access to or sharing of Camera Footage shall be granted to other Third Parties, except with the explicit consent of the Data Subject(s) and in compliance with applicable legislation and regulations.

Article 5.3 – Rights of Data Subjects

1. Data Subjects shall be informed of the Camera Surveillance by means of signs, stickers and/or screens at the entrances and exits of the Grounds and/or Buildings. These shall refer to these Regulations and to the EUR Privacy Statement.
2. The legal basis of Legitimate Interest grants the Data Subject the right to object to the Processing of their Personal Data.
3. Data Subjects also have the right of access to, rectification of and erasure of Camera Footage in which they appear.²
4. A request by a Data Subject to exercise one or more of these rights may be submitted in accordance with the procedure set out in the EUR Privacy Statement.
5. Access to Camera Footage shall always take place under the supervision of the Head of EUR Security and/or the Advisor Integral Safety & Security.

Chapter VI – Record-keeping and reporting

Article 6.1 – Registration and internal reporting on Camera Surveillance

1. A confidential logbook shall be kept of the use of the Camera System, Camera Footage and other Data.
2. The Head of EUR Security shall report at least annually to the Executive Board on the design and use of Camera Surveillance, including a report on access to and disclosure of Camera Footage as referred to in Chapter V.

Article 6.2 – Annual reporting to the University Council

The Executive Board shall report annually to the University Council on the Camera Surveillance applied in the preceding year, providing in particular an overview of:

- a. changes in the authorisation matrix as referred to in Article 3.3(1);
- b. temporarily granted authorisations as referred to in Article 3.3(3);
- c. changes in the Camera Plan as referred to in Article 4.1;
- d. the deployment of temporary additional Camera Surveillance as referred to in Article 4.3;
- e. the deployment of Covert Camera Surveillance as referred to in Article 4.4;
- f. Incidents in which live Camera Footage was shared with the police as referred to in Article 5.1;
- g. access to and sharing of Camera Footage with Third Parties as referred to in Article 5.2.

² Art. 15-22 AVG

Chapter VII – Final and transitional provisions

Article 7.1 – Interpretation

In matters relating to the subjects governed by these Regulations, in which these Regulations do not provide, or where these Regulations give rise to multiple interpretations, the Executive Board shall decide.

Article 7.2 – Management of the Regulations

These Regulations are managed by the General Management Directorate (ABD), service unit Administrative Affairs (BZ), Team Integral Safety & Security.

Article 7.3 – Translation

If a discrepancy arises between the English translation and the Dutch text, the Dutch text shall prevail.

Article 7.4 – Publication

The Executive Board shall publish these Regulations on the EUR website.

Article 7.5 – Entry into force, duration and evaluation

1. These Regulations shall enter into force on 1 October 2026, after approval by the University Council and adoption by the Executive Board.
2. These Regulations shall have a maximum duration of five years and shall expire on 30 July 2031.
3. After four years, an evaluation of these Regulations shall take place, on the basis of which new Regulations shall be developed.
4. If circumstances so require, the Executive Board may adopt amendments to these Regulations at an earlier point in time than the period referred to in paragraph 2, provided that the University Council has approved those amendments.

Article 7.6 – Short title

These Regulations may be cited as: Camera Surveillance Regulations EUR 2026.

Article 7.7 – Repeal

On the date of entry into force of these Regulations, *Reglement Cameratoezicht EUR 2013* shall be repealed.

Chapter VIII – Definitions

In these Regulations, the following terms shall have the meanings set out below:

1. **GDPR (AVG)**
General Data Protection Regulation (EU Regulation No 2016/679) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data.
2. **Awb**
Dutch General Administrative Law Act (Algemene wet bestuursrecht).
3. **BBR-EUR**
Management and Administration Regulations Erasmus University Rotterdam (Bestuurs- en Beheersreglement EUR), as referred to in Article 9(4) WHW.
4. **Administrator (Beheerder)**
The person charged with the performance of Administrative tasks on the instructions, in the name and under the responsibility of the Executive Board (in an administrative law sense) and EUR (in a private law sense);
5. **Administration Unit (Beheerseenheid)**
An organisational unit established by the Executive Board within which management is carried out by the Administrator.
6. **Policy Framework**
Camera Surveillance Policy Framework EUR 2026
7. **Data Subject (Betrokkene)**
An identified or identifiable natural person to whom Personal Data relate (in accordance with Article 4(1) GDPR). This may be a Student, Officer or Third Party who has obtained access to EUR Buildings and Grounds.
8. **Security Guard (Beveiligingsbeambte)**
An Officer who, on behalf of EUR, is charged with supervising and enforcing the safety of persons present on EUR Grounds.
9. **Camera**
An optical and electronic device, either fixed or mobile, that can record moving images and sound and subsequently transmit the images in encoded form to the server so that the images can be viewed live and stored for the purpose described in Article 1.2(1) of these Regulations.
10. **Camera Footage (Camerabeelden)**
The live and recorded video images obtained by the Camera System. Such images may contain Personal Data.
11. **Camera Plan (Cameraplan)**
An overview, adopted by or on behalf of EUR, of all camera positions for permanent Camera Surveillance, in which, for each Camera, at least the location, the purpose of the Camera Surveillance and the type of Camera are recorded.
12. **Camera System (Cmerasysteem)**
The entirety of Cameras, monitors, recording equipment, servers, junction boxes, connections and mounts, or other means of data transmission of image material and equipment used for the purpose of carrying out Camera Surveillance.
13. **Camera Surveillance (Cameratoezicht)**
Surveillance using fixed and mobile Cameras, on a structural and/or incidental basis.
14. **Central Control Room (Centrale meldkamer)**
The centrally located room where Camera Footage can be viewed live, and where recorded Camera Footage stored within the applicable retention period can be viewed, edited and saved to an information carrier.
15. **Control Room Operator (Centralist)**
A Security Guard, employed by a Contractor or by EUR, who is responsible for the operational Camera Surveillance by viewing live Camera Footage from all Cameras connected to the EUR Camera System and taking action where necessary.
16. **Executive Board (College)**
The Executive Board of Erasmus University Rotterdam, a Management Body as referred to in Article 1.1(1)(a) Awb.

17. **Contractor**
The company or organisation engaged by EUR to perform part of the tasks associated with Camera Surveillance.
18. **CPO**
Chief Privacy Officer.
19. **DPIA**
Data Protection Impact Assessment. A prior and systematic assessment of the intended Processing of Personal Data in the context of Camera Surveillance, aimed at identifying and mitigating privacy risks. The results of the DPIA are recorded in Writing. In the DPIA, EUR makes a reasoned assessment between the privacy interests of Students, Officers and Third Parties and the necessity, proportionality and subsidiarity of the Camera Surveillance.
20. **Third Party / Third Parties (Derde(n))**
Any party other than the Data Subject or Interested Party; a natural or legal person, public authority, service or other body not being the Data Subject, the Controller or any person who, under the direct authority of the Controller, is authorised to process Personal Data (Article 4(10) GDPR).
21. **EDIS**
Erasmus Digitalisation & Information Services.
22. **EUR**
The legal entity established under public law named Erasmus University Rotterdam.
23. **DPO (FG)**
Data Protection Officer.
24. **Officer (Functionaris)**
A member of the Staff (persons who have an employment contract with EUR) or a person working for EUR on some other basis, in a defined or undefined post.
25. **Building (Gebouw)**
Any structure accessible to persons, enclosed in whole or in part by walls, with or without a roof. The Building is owned by EUR, is used by EUR or is located on Grounds of EUR.
26. **Data (Gegevens)**
Data generated or recorded in the context of Camera Surveillance, other than Camera Footage and Personal Data, including log data and technical and administrative metadata, such as date, time, camera number, location or GPS data, system and access logs and other comparable data relating to the operation, management and use of the Camera System.
27. **Legitimate Interest (Gerechvaardigd belang)**
The Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a Third Party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require the protection of Personal Data, in particular where the Data Subject is a child (Article 6(1)(f) GDPR).
28. **Covert Camera Surveillance (Heimelijk Cameratoezicht)**
The recording of Camera Footage with (hidden) Cameras that have been installed in order to capture persons in an identifiable manner without the presence of the Cameras having been made clearly known.
29. **Tenant (Huurder)**
A Third Party who rents or uses space from EUR.
30. **Incident**
An unforeseen and/or unwanted event, disruption or disturbance of order and safety, health and/or a (suspected) criminal offence.
31. **Intelligence Agency (Inlichtingendienst)**
The General Intelligence and Security Service (AIVD).
32. **Law Enforcement Authorities (Opsporingsdiensten)**
Comprising: (a) the police (criminal investigation in general), (b) the Fiscal Intelligence and Investigation Service (FIOD), (c) the Human Environment and Transport Inspectorate, (d) the Intelligence and Investigation Service (ILT-IOD), and (e) the Netherlands Food and Consumer Product Safety Authority Intelligence and Investigation Service (NVWA-IOD) and the Netherlands Labour Authority, Directorate of Investigations (NLA-DO), (b to e being special investigation services).
33. **Personal Data (Persoonsgegevens)**
Any data relating to a Data Subject that are or will be processed by the Processor in any way (in accordance with Article 4(1) GDPR).

- 34. Regulations (Reglement)**
Camera Surveillance Regulations EUR 2026.
- 35. RE&F**
Real Estate & Facilities.
- 36. Server Room (Serruimte)**
The secured room in which the server or recording equipment on which the recorded Camera Footage is stored is located.
- 37. Written / in Writing (Schriftelijk)**
Laid down in writing on paper or "by electronic means" as referred to in Article 2:13 Awb.
- 38. Student:**
An individual who is enrolled at and admitted to EUR, as referred to in Chapter 7, Title 3 WHW.
- 39. Grounds (Terrein)**
Any land owned by EUR, used by EUR, or on which a Building is located.
- 40. Controller (Verwerkingsverantwoordelijke)**
A natural or legal person, public authority, service or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
- 41. Processing of Personal Data (Verwerking van Persoonsgegevens)**
Any operation or set of operations which is performed on Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of Personal Data (Article 4(2) GDPR).
- 42. WHW**
Dutch Higher Education and Research Act (Wet op het hoger onderwijs en wetenschappelijk onderzoek).