

CAMERA SURVEILLANCE REGULATIONS VRIJE UNIVERSITEIT AMSTERDAM

Vrije Universiteit Amsterdam camera surveillance regulations

This document is a translation. In the event of any ambiguity or uncertainty arising from the translation, the original Dutch version shall take precedence and govern the interpretation and understanding of the content.

Contents

Introduction	3
Article 1. Terms	3
Article 2. Scope of application.....	4
Article 3. Purposes.....	4
Article 4. Responsibility and division of labour	5
Article 5. Security	5
Article 6. Installation of cameras.....	5
Article 7. Temporary hidden camera surveillance	6
Article 8. Retention period.....	6
Article 9. Rights of Data Subjects	6
Article 10. Inspection and issuance of Images	7
Article 11. Final provisions	7

Introduction

Camera surveillance is used on grounds and in buildings of Vrije Universiteit Amsterdam (hereinafter: **VU**). The image information obtained from this camera surveillance is digitally recorded and is a processing of personal data.

The legal basis used by the VU for camera surveillance is looking after a legitimate interest of the VU. The deployment of camera surveillance is a necessary measure for the VU to:

- protect the health and safety of its students, staff and visitors on its premises and in its buildings;
- secure its premises and buildings;
- guard the property located on its premises or in its buildings; and
- record incidents.

Camera surveillance can infringe on the privacy of students, staff and visitors. VU therefore only uses camera surveillance at locations where it is necessary and less drastic measures are not effective. This is assessed per location and then periodically evaluated.

The purpose of these Regulations (hereinafter **Regulations**) is to promote and ensure that:

- the VU complies with applicable laws and regulations regarding the protection of personal data;
- camera surveillance is deployed with integrity; and
- students, staff and visitors are adequately informed about how the VU handles camera surveillance.

The Regulations describe tasks, responsibilities and procedures within the VU and describe how data subjects can exercise their rights.

Article 1. Terms

The terms in these Regulations have the meanings assigned to them by the General Data Protection Regulation and related laws and regulations (hereinafter: the **Act**), unless expressly stated otherwise. Furthermore, in these Regulations, the following terms shall have the following meanings:

- a. **Images:** the images obtained and recorded by the camera system.
- b. **Management:** ensure continuity of camera surveillance.
- c. **Administrator:** the Head of Security of the Facility Campus Organisation (FCO) of VU and in his absence his replacement.
- d. **Data subject:** the person who is recorded and registered by the camera system. This may be a student, employee or visitor to the VU grounds and/or buildings.
- e. **Authorised Officer:** the person authorised by the VU to access the equipment used for Camera Surveillance under the responsibility of the Manager or System Controller. In addition to Employees, this may also include those employed by VU without employment with VU, such as a temporary employee, seconded employee, ZZP or intern.
- f. **Camera surveillance:** surveillance using cameras.
- g. **Executive Board:** The Executive Board (CvB) of Vrije Universiteit Amsterdam.
- h. **Director FCO:** the director of the Facility Campus Organisation (FCO) of VU.

- i. **VU Data Protection Officer (FG):** an internal officer as referred to in Article 37 et seq. of the General Data Protection Regulation. The FG independently monitors compliance with laws and regulations relating to data protection and the VU's policy on the protection of Personal Data.
- j. **Incident:** an untoward incident or suspicion thereof.
- k. **Employee:** the person who has an employment contract with the VU Foundation.
- l. **Personal Data:** any information relating to an identified or identifiable natural person (the Data Subject). The term Personal Data is a broad concept that includes almost all data related to a natural person. It includes both objective and subjective data, regardless of whether the information is accurate. It concerns information about a person, such as his name, date of birth and gender. It also involves value judgements, such as an Employee's rating. Only in exceptional cases, information that concerns a natural person is not Personal Data.
- m. **System manager:** the property management manager (FCO) and in his absence his deputy.
- n. **Processing of personal data:** any operation or set of operations involving personal data, including in any case the collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, provision by means of transmission, dissemination or any other form of making available, bringing together, linking, as well as blocking, erasure or destruction of data.

Article 2. Scope of application

- 2.1 These Regulations apply to all premises and buildings where the VU uses Camera Surveillance¹ and cover any Processing of Personal Data that takes place on the basis of the Images.
- 2.2 These Regulations do not apply to land and buildings that the VU rents out to third parties. To the extent that Camera Surveillance takes place here, this is done under the responsibility of the tenants.
- 2.3 These Regulations do not cover the use of cameras for monitoring examinations.

Article 3. Purposes

- 3.1 The VU collects and processes the Images solely for the purposes of:
 - a. the protection of the health and safety of students, Employees and other Concerned Persons moving on VU premises or in buildings;
 - b. securing access to VU grounds and buildings;
 - c. the surveillance of items located on VU premises and in buildings;
 - d. recording Incidents; and
 - e. measuring the number of people on the grounds and in the buildings and premises of the VU.
- 3.2 The VU does not use artificial intelligence and/or facial recognition in its Camera Surveillance.

¹ These include land and buildings that VU owns, as well as those that VU rents.

Article 4. Responsibility and division of labour

- 4.1 The Executive Board is ultimately responsible for Camera Surveillance.
- 4.2 The Director FCO is responsible to the Executive Board for Camera Surveillance.
- 4.3 The Manager is responsible for managing and supervising the implementation of the Camera surveillance and reports on this to the Director FCO.
- 4.4 The Manager shall appoint Authorised Officers who may operate the camera system for the purposes set out in Article 3 and view and review the images live under the conditions set out in these Regulations.
- 4.5 The System Controller is responsible for the technical management of the Camera Surveillance and coordinates with the Manager in this respect. The System Controller shall appoint Authorised Officers who will be given access to the equipment used for Camera Surveillance within the framework of maintenance and management. Only with the consent of the System Controller shall third parties be given access to the equipment used for Camera Surveillance within the framework of maintenance and management.
- 4.6 All Authorised Officers shall treat the Images with confidentiality and integrity. An Authorised Officer shall not use the Images other than as necessary for the performance of the Authorised Officer's duties. The Authorised Officer is obliged to maintain confidentiality.

Article 5. Security

- 5.1 The VU shall take adequate technical and organisational measures to prevent unauthorised access to the equipment used for Camera Surveillance and loss or any form of unlawful processing of the Images.
- 5.2 The physical premises where the Images can be viewed and watched back live is accessible 24/7 to Be added officials and is secured against burglary and vandalism.
- 5.3 If the Images are stored, this shall be done encrypted and appropriately secured. If the storage location of the Images changes, the IT Service shall ensure comparable information security of the new storage location.

Article 6. Installation of cameras

- 6.1 The Administrator and System Controller shall jointly decide on the installation of cameras, where necessary in consultation with the Director FCO. A decision to place a camera always involves a proper balancing of the protection of the privacy of the Data Subjects on the one hand and the interests of the VU on the other.
- 6.2 Camera surveillance will be used only for the purposes stated in these Regulations, at locations where it is necessary and less intrusive measures are not effective. The need for Camera Surveillance at a particular location will be reviewed periodically.
- 6.3 In areas where persons need to be undisturbed, such as in toilets, showers and changing rooms, Camera Surveillance by definition constitutes too great an invasion of the privacy of the Data Subjects and Camera Surveillance is not permitted.
- 6.4 Camera surveillance is not intended to follow Data Subjects while performing their work or visiting. When cameras are installed, it is therefore avoided as much as possible that Data Subjects are unnecessarily in continuous view. At locations where there are increased security risks, such as a relatively high risk of aggression or theft, it is possible that Complainants may be continuously in view if this is necessary and less drastic measures are not effective.

- 6.5 The Camera Surveillance is made known by means of signs, stickers and/or screens at the entrances and exits of the grounds and buildings and at specific locations in the buildings where Camera Surveillance is used. By publishing these Regulations on VU's public website and intranet, Employees, students and other Data Subjects will be informed of the purposes of the Camera Surveillance and the circumstances under which their Personal Data will be processed.

Article 7. Temporary hidden camera surveillance

- 7.1 Only in exceptional situations may hidden cameras be temporarily deployed on the grounds and in the buildings of the VU. Hidden cameras will never be placed in the areas referred to in Article 6.3.
- 7.2 Concealed cameras will only be deployed for the purposes stated in Article 3, at locations where it is necessary and less intrusive measures are not effective. The need for Camera Surveillance at a particular location shall be periodically evaluated by the Manager, Director FCO and the System Manager. A hidden camera will only be used as a 'last resort' after other means have proved ineffective.
- 7.3 The decision to install a hidden camera is taken by the Executive Board.
- 7.4 The VU shall inform the Data Subjects of the deployment of hidden cameras as soon as their deployment is no longer necessary to achieve purposes as stated in Article 3.

Article 8. Retention period

- 8.1 Images are kept for a maximum of 10 days after which they are irreversibly deleted unless:
- the Images are related to an Incident. In this case, the Images will be retained until the investigation or treatment of the Incident is concluded; or
 - a request for inspection in accordance with Article 9.1 has been submitted and the Images have not yet been deleted. In that case, the Images will be kept until the request for inspection has been decided and - to the extent the request is granted - the Data Subject has had access to the Images.
 - it concerns Images that were made exclusively for the purpose mentioned in Article 3.1 (e) (pressure measurement). Those Images are deleted immediately after the pressure measurement has been made.

Article 9. Rights of Data Subjects

- 9.1A Data Subject has the right to inspect the Images if he/she is recognisably in the picture and the Images have not yet been erased. The VU may refuse access, for example if this is necessary in the interests of preventing, detecting and prosecuting criminal offences or to protect the rights and freedoms of others. Persons who suspect that they have been recognisably in the picture may request inspection. The VU will then first consider whether the Images contain the applicant's data. If this is the case, the inspection request will be processed.
- 9.2 A Data Subject has the right, without having to explicitly request it, to removal or blocking (think "blurring") of the Images on which he/she is recognisably in the picture, insofar as his/her Personal Data are processed unlawfully or the Personal Data are not or no longer relevant for the purpose for which they were collected.
- 9.3A Data Subject has the right to object to the use of his/her Personal Data by the VU. If the objection is well-founded, the VU will immediately terminate the relevant data processing.
- 9.4 The requests referred to in Articles 9.1, 9.2 and 9.3 may be addressed to the Data Protection Officer. This also applies to the exercise of other rights the Data Subject has on the basis of the Act. The Data Protection Officer of the VU will inform the Data Subject as soon as possible, in any event within four weeks, on behalf of the VU, whether the request will be complied with.

- 9.5 Complaints relating to the application of Camera Surveillance and to the conduct of the Manager or the Authorised Officers may be made in writing to the Director FCO. The Director FCO shall respond to the complaint within six weeks.
- 9.6 The Data Subject may at any time lodge a complaint with the Personal Data Authority about the Processing of Personal Data by the VU.
- 9.7 The Data Subject may at any time apply to the competent court in relation to the manner in which Personal Data are processed by the VU.

Article 10. Inspection and issuance of Images

- 10.1 Inspection of the Images and issuance of the Images to third parties will only take place:
 - a. at the request of the police or the public prosecutor;
 - b. when reporting a (suspected) offence; and
 - c. in other cases where this is compatible with purposes as stated in these Regulations and the Act provides a basis for doing so.
- 10.2 The CvB always reviews whether the police or public prosecutor's request provides a sufficient basis for the requested inspection and/or issue.
- 10.3 A request for inspection and/or issue of the Statues by third parties who are not Data Subjects must be submitted to the Manager. The Manager will inform the Director FCO and the BoIP in this respect. The CvB will decide on the request as soon as possible, whereby the CvB will expressly take into account the right to protection of the privacy of the Data Subjects.
- 10.4 Any person authorised to inspect the Statues or to receive a copy thereof must identify himself beforehand to the Manager. Inspection of the Statues will take place in the presence of the Manager or an Authorised Officer. Receipt of a copy of the Statues requires a signature.

Article 11. Final provisions

- 11.1 In cases not covered by these Regulations, the Executive Board decides.
- 11.2 These Regulations are published on the VU website and intranet.

These Regulations were adopted by the Executive Board, after consent of the USR on 31 May 2023 and consent of the Works Council on 27 June 2023, and came into force on 17 July 2023.
