Universiteit Utrecht

CCTV POLICY
UTRECHT UNIVERSITY

Version 1.0 - 30 September 2022

CCTV Policy Universiteit Utrecht

Contents

Introduction

Utrecht University (hereafter: UU) has put a closed circuit television (CCTV) surveillance system in place in and around the buildings and campuses that fall under the responsibility of our Executive Board. This is done in order to provide a safe and secure environment for students, staff and visitors as well as securing UU buildings and assets. This policy applies to the CCTV systems used by Facilities Services Centre (FSC) Security team to execute their tasks. CCTV footage is shown real-time in the FSC Control Room, at various service points and reception desks, and through incident reports driven by system operators. Video recordings are retained in UU systems, operated by Information Technical Services (ITS), for the purpose of camera surveillance. At this moment, there are approximately 400 security cameras in use at the UU.

The UU will have due regard to the General Data Protection Regulation (GDPR) and any other relevant data protection regulation when using CCTV cameras and recording footage. Digitally recording images constitutes a data processing activity, covered by the GDPR. The GDPR forms the framework within which the UU operates the camera surveillance systems.

The UU only uses CCTV at locations where this is necessary, and less far-reaching measures have not proven to be effective. Whether this is the case will be assessed per location and periodically evaluated.

The purpose of this CCTV Policy (hereafter: Policy) is to promote and warrant that:

- The UU complies with relevant laws and regulations for the protection of personal data;
- CCTV is deployed in an open and honest manner; and
- Students, employees, and visitors are sufficiently informed over the way in which the UU uses CCTV.

This Policy describes the roles, responsibilities, and procedures relating to CCTV within the UU and describes how data subjects can exercise their rights.

Chapter 1. Definitions

The concepts in this Policy have the meaning as defined in the General Data Protection Regulation and other relevant laws and regulations (hereafter: the **Law**), unless expressly stated otherwise.

1. **Accountable body:** the part of the organisation that is ultimately responsible for the correct use of CCTV. At the UU, that is the Executive Board, who have delegated this task to the FSC director.
2. **Authorised employee(s):** the person(s) with access to the CCTV equipment under the responsibility of the System operator.
3. **Camera surveillance:** surveillance with the help of cameras.
4. **Camera system:** all CCTV equipment, including cameras, monitors, recording equipment, and connections.
5. **Control room:** the central control room of the UU, staffed 24/7, where all Footage is shown.
6. **Control room operator:** the employee operating the camera system.
7. **Data Protection Officer (DPO):** an internal officer as described in article 37 of the GDPR.
8. **Data Subject:** the person recorded by the CCTV system. This can be a student, employee, or a visitor to the campus and/or buildings of the UU.
9. **Executive Board:** the board of the UU.
10. **Footage**: recordings made by and stored in the CCTV system.
11. **FSC director:** the director of the Facilities Service Centre (FSC) of the UU.
12. **Operational management:** care for the operational continuity of the CCTV system.
13. **Operational manager:** the person responsible for the day-to-day operational management of the system.

14. **Technical operator:** the employee responsible for the technical management of the system.
15. **Personal data:** any information relating to an identified or identifiable natural person (the data subject). In particular, all footage in which a person is recognisable.
16. **Processing of personal data:** any operation or set of operations which is performed on personal data or on sets of personal data. In relation to CCTV, this is specifically the recording, storing, sharing, and deleting of footage in which a person is recognisable.
17. **Server room:** the room in which the servers that store the footage are located. This room is secured, and not admissible to non-authorised persons.
18. **System operator:** the FSC runs the Operational management of the CCTV systems. The FSC director appoints an employee as the System operator, who will be responsible for the execution of the operational management.
19. **Technical system manager:** the systems operator who operates and attends to the technical part of the camera system.

Chapter 2. Scope

This policy is applicable to all camera surveillance on the campus and buildings of the UU, and is relevant to every processing of personal data taking place through the footage.

This policy is not applicable to camera surveillance taking place on the grounds and buildings that the UU leases out to third parties. If any camera surveillance takes place here, this occurs under the responsibility of the leasers. This policy is not applicable to the use of cameras during exams. If this takes place, separate rules and policies will be set up to govern this activity. This policy is not applicable to the monitoring of animals at the Faculty of Veterinary Medicine.

There are a few situations where the use of CCTV would form such a significant breach of privacy, that the UU chooses to never implement camera surveillance here. For example, spaces where people should not be disturbed, like toilets, showers, and changing rooms, are completely exempt from camera surveillance. We do not use hidden or secret camera surveillance. We do not use automatic facial recognition. Automatic numberplate recognition only happens at the barriers at our car parks, and never at other cameras on our campus.

Chapter 3. Purposes

Camera surveillance only takes place for the following purposes:

1. The protection of the property of the UU and the security and protection of the people located in our buildings and on our campus, as well as their belongings.
2. Recording incidents and emergencies for the later detection and prosecution of (alleged) crimes, and analysis of dangerous situations.
3. Regulating traffic flows (entrances and exits) to the university parking grounds and to buildings in case of emergencies.

Chapter 4. Roles and responsibilities

Camera surveillance occurs under the authority of the Executive Board of the UU. The FSC director is responsible for the operation of the camera systems. The FSC director appoints an operational manager to execute these tasks.

The operational manager is responsible for the operational management of and oversight over the implementation of the camera surveillance, and reports to the FSC director. The operational manager appoints authorised employees, who can control the camera system, view live footage, and watch recordings (under the conditions as set out in this policy).

The technical manager is responsible for the technical management of the system, and coordinates this with the operational manager. Third parties only have access to the camera equipment with permission of the technical manager, in the context of maintenance and operational management by those third parties.

All authorised employees treat the footage with confidentiality and integrity. An authorised employee may only use the footage as necessary for the performance of their tasks, and must not disclose any details about the footage with others. These agreements are laid down in a set of working instructions, which is shared with and signed by all authorised employees.

Chapter 5. Security measures

The UU has taken adequate technical and organisational measures to prevent unauthorised access to the camera equipment, and unauthorised deletion or other processing of the footage. The server room and the designated rooms where live footage and recordings can be reviewed are secured against break ins and vandalism. Footage is encrypted and stored on a secure system on a separate server.

The operational manager ensures that the images captured by the cameras are limited as much as possible to that which is necessary for the specific purposes for which the cameras have been placed. Where the purpose of the camera is to secure buildings, the camera covers the person in the image for a minimum of 10% (observation). Where the purpose of the cameras is the protection of belongings and people, the cameras are set up to cover at least 50% of the person in the image (recognition). Where necessary, images can be partially blurred or blacked out, so that only relevant parts of the terrain are recorded.

Chapter 6. Placing cameras

The operational manager and the technical manager jointly decide where cameras should be placed. The starting point for this is the Operational Standard Physical Security operated by FSC Security. Where necessary, the placement of the cameras is discussed with the FSC director, the Privacy Officer of FSC, and – where relevant – a representative of the faculty. When deciding whether and where to place a camera, an assessment is always made between the protection of the private life of the data subjects, and security of students, staff, visitors and UU buildings and assets.

Camera surveillance is only used for the purposes as mentioned in this Policy, at locations where this is necessary and other, less far-reaching measures have proven not to be effective. The necessity of camera surveillance at a specific location is periodically evaluated.

The presence of camera surveillance is made known through signs, stickers, and/or screens at the entrances and exits of terrains and buildings, and at specific locations within the buildings that make use of CCTV. Employees and visitors are informed of the purposes of CCTV and the conditions under which their personal data is processed through the publication of this Policy on our website and Intranet.

Chapter 7. Location of cameras

Cameras can be placed at the following locations:

1. Car parks, parking garages, and checkouts at these locations;
2. Bicycle storage areas;
3. At entrances and exits, including emergency exits, of UU buildings;
4. At the facades of buildings or on poles, where they may film parts of the public road;
5. Inside buildings, where the necessity of this is proven and there is no other option than the use of cameras.

Chapter 8. Viewing live streams or recordings

Live streams are effectively accessible to anyone with a view of a screen on which the live streams are shown. By placing these screen in such a way that these are only visible (for a longer period) by the people for whom they were intended, access is limited to:

a. Control Room operators;
b. Receptionists and servicepoint employees;
c. Operational managers;
d. Technical system operators;
e. The supplier of the system, when this is necessary for maintenance purposes and exclusively with permission of the Technical manager.

CCTV recordings are less accessible, as fewer employees require this access as part of their day-to-day activities. Access to CCTV recordings is limited to:

a. Control room operators;
b. Operational managers;
c. Technical system operators.

Employees in this last group are the only ones who can operate cameras (zooming in or out, moving cameras, etc.).

Chapter 9. Retention period

Recordings are retained for seven days. After seven days, they are automatically overwritten, unless:

a. The footage is relevant to an incident that occurred. In this case, recordings are retained for as long as necessary to deal with this incident and its aftermath; or
b. A subject access request as described in article 15 GDPR is submitted within this seven day period. In this case, the footage is stored until the request is approved and the data subject has seen the footage, or until the request is denied.

Chapter 10. Rights of data subjects

A data subject has a right of access to footage in which they are recognisable, and can request access or a copy of this footage for as long as it is not yet deleted. Because recorded persons are not automatically identified by the system, it is not possible to search the footage for specific persons. Therefore, should a data subject wish to exercise this right, it is necessary that they state the date, time, and location at which the requested footage was recorded. The data subject can also, where possible, provide an indication of the relevant time period for which they are requesting the footage.

A data subject has a right to deletion or blurring of footage in which they are recognisable, if the processing of their personal data infringes on the GDPR or if the personal data is not or no longer relevant for the purposes for which they were collected.

A data subject has a right to object to the use of their personal data by the UU. The UU will assess the objection of the data subject against the interests of the organisation. If the UU cannot comply with the request, reasons will be documented.

Requests for the exercise of these rights can be addressed to the Privacy Officer of the FSC (privacy.fsc@uu.nl).

Complaints on the use of CCTV or the actions of the system operator or authorised employees can be submitted in writing to the Executive Board. The Board will respond to complaints within four weeks.

A data subject can make a complaint about the processing of their personal data to the DPO (fg@uu.nl) or the independent supervisory authority for the protection of personal data, the Autoriteit Persoonsgegevens,[1] at all times. Should this not resolve their complaint, the data subject can also start a legal case at a competent court.

Chapter 11. Access to and disclosure of recordings to third parties

Footage is only made available to third parties if:

a) The police or public prosecution service orders the release of the footage in relation to an (alleged) crime;
b) The UU reports an (alleged) crime to the police;
c) A situation occurs where sharing the footage with third parties proves necessary, and this is considered both compatible with the purposes as stated in this Policy and there is an appropriate legal basis.

The Executive Board always assesses whether the order of the police or prosecutors has an adequate legal basis to justify the requested access and/or sharing before making the footage available. The Executive Board deputises the FSC Director to perform these tasks on its behalf.

All requests for access and/or sharing of footage by third parties must be submitted to the system operator. The system operator will inform the FSC director of the request. The Executive Board or the FSC director will decide on the outcome of the request as soon as possible, where they will explicitly take the data subjects' right to privacy into account.

Anyone to whom the footage is made available must identify themselves towards the system operator. Access to the footage takes place in the presence of the system operator or the authorised employee. The receiver must sign for the receipt of a copy of the footage.

Chapter 12. Final clauses

The Executive Board decides on all cases not covered by this policy.
This Policy is presented to the University Council for information.
This Policy will be published on the UU website and Intranet.

This Policy is established by the FSC director and is active since 12 October 2022.

[1] Autoriteit Persoonsgegevens |