rijksuniversiteit groningen

Camera surveillance policy University of Groningen May 23, 2025

Summary

Camera surveillance is used on the grounds and in and around the buildings of the University of Groningen (hereinafter: **UG**). The image and audio information and other data obtained from this surveillance may contain personal data. Camera surveillance therefore infringes on the privacy of students, staff and visitors. The UG must therefore comply with the General Data Protection Regulation (hereinafter **GDPR**) and other applicable laws and regulations when processing this type of information.

The deployment of camera surveillance is a necessary measure for the UG to:

- protect the safety of employees, students and visitors on its premises and in its buildings;
- secure its grounds, buildings and other structures and prevent or detect damage thereto;
- guard the property located on its premises or in its buildings; and
- prevent and detect incidents.

The UG only uses camera surveillance if it is necessary, proportionate and less drastic measures are not effective (subsidiarity). This is assessed per location and evaluated periodically.

The purpose of this policy is to promote and ensure that:

- the UG complies with the laws and regulations applicable to camera surveillance;
- camera surveillance is used for the above purposes;
- internal responsibilities for the decision to and implementation of camera surveillance are clear;
- students, employees and visitors are adequately informed about how the UG handles camera surveillance.

The policy describes the duties, responsibilities and procedures within the UG and describes how data subjects can exercise their rights.

Article 1. Definitions

For the purposes of this policy, the following definitions shall apply:

a. **Analysis Data**: data, including Personal Data, generated using the Camera System based on/about the Recordings, such as data processed about numbers of people in a room.
b. **Data Subject**: the natural person, as referred to in Article 4(1) GDPR, whose Personal Data is or may be processed in the performance of Camera Surveillance. A Data Subject may, for example, be a student, employee or visitor of the premises and/or buildings of the UG.
c. **Camera System**: the set of cameras, display equipment and supporting hardware and software used to conduct Camera Surveillance.
d. **Camera Surveillance**: the making of Recordings with cameras of persons, premises, buildings and/or things for the purposes described below in Article 3.
e. **Real Estate Organization Director**: the director of the real estate organization of the UG, part of University Services, Cluster Campus & Community.
f. **DPIA**: Data Protection Impact Assessment referred to in Article 35 GDPR.
g. **Covert Camera Surveillance:** conducting Camera Surveillance with hidden cameras, without informing the Data Subject prior to or during such surveillance.
h. **Head of Administrative and Legal Affairs**: the Head of the Administrative and Legal Affairs department (BJZ), part of University Services, Staff Division of Governance & Legal.
i. **Incident**: incident that appears to indicate punishable, unlawful or prohibited actions by persons or an incident that results in damage to or unauthorized use of any premises and buildings of the UG or property of the UG or third parties.
j. **Location**: the premises and buildings and/or other set up on and/or within which Camera Surveillance is conducted.
k. **Recordings**: the video and/or audio recordings, either *live* or after capture, obtained by camera surveillance, including the Personal Data contained in the recordings.
l. **Personal Data**: any information about an identified or identifiable natural person (the Data Subject), as referred to in Article 4(1) GDPR.
m. **UG:** University of Groningen.
n. **Security Manager**: the security manager of the UG, also the Head of the Physical Security Organization of the UG, part of University Services, Cluster Campus & Community, cluster support department.
o. **Processing**: any action or set of actions with respect to the Recordings, Personal Data and Analysis Data, including processing as referred to in Article 4 sub 2 GDPR.

Article 2. Scope of application

1. This policy applies to all Locations where the UG uses Camera Surveillance and relates to each Processing. This policy is a guideline as referred to in section 3.14 of the UG's General Data Protection Policy.[1] In the event of any conflict between these two policy documents, this Camera Surveillance Policy shall prevail.
2. This policy does not apply to:
   a. Use of cameras for the purpose of recording and broadcasting lectures, academic ceremonies and other meetings;
   b. Use of cameras for the purpose of consultation;
   c. Processing of video and audio material in the context of scientific research;
   d. Use of cameras for the purpose of surveillance during (online) tests and exams.
   e. Camera surveillance in buildings or premises of the UG that are not used by the UG itself, for example because the UG rents them out.
   f. Using process cameras for business operations purposes that produce Recordings or Analytical Data that do not contain Personal Data.

Article 3. Purposes

1. Camera surveillance and the Processing of Recordings is done solely for the following purposes:
   a. protecting the safety of employees, students and visitors on the premises and in the buildings of the UG;
   b. securing the grounds, buildings and other premises of the UG and preventing or detecting their damage;
   c. guarding property located on UG premises or in its buildings; and
   d. preventing and detecting Incidents.
2. Generating Analysis Data using a Camera System requires the prior consent of the Executive Board as does the processing of Analysis Data for purposes other than those described in paragraph 1 of this article. This consent is requested by the board of the faculty or the management of the department that intends to generate and process Analysis Data.
3. The use of Camera Surveillance, Recordings and/or Analysis Data for purposes other than those described above requires a prior decision by the Executive Board with the consent of the University Council. The Executive Board will seek the advice of the Data Protection Officer of the UG before making such a decision.
4. The UG does not use facial recognition in its Camera Surveillance.
5. If the RUG wishes to record audio when making Recordings for the purpose of Camera Surveillance, a DPIA must be carried out by the responsible faculty board or departmental management for this purpose.
6. Before acting on Recordings and/or Analysis Data, they are reviewed by an authorized UG staff member.

[1] See: https://www.rug.nl/about-ug/organization/rules-and-regulations/general/20211129-algemeen-beleid-bescherming-persoonsgegevens-3-0-def.pdf

Article 4. Division of duties, responsibilities and powers

1. The Executive Board of the UG is ultimately responsible for Camera Surveillance.
2. The Real Estate Organization Director is charged with:
    a. Procuring and furnishing non-mobile "earth and nail proof" Camera Systems for the purpose of Camera Surveillance maintained by the UG in accordance with a programme of requirements and specifications prepared by the UG;
    b. Having the Camera System equipment and software meet the requirements of the GDPR, this policy and the UG's privacy and information security policy, in consultation with the BJZ department and the Privacy & Security Coordinator of its organizational unit. This includes:
        i. That the equipment and software are manufactured and furnished *privacy & security by design* and that the application of the requirements of this policy is technologically enforced to the maximum extent possible;
        ii. That the agreements required under the GDPR have been made with the Camera System suppliers regarding the processing and security of Recordings and Analysis Data;
        iii. That Recordings and Analysis Data are processed exclusively within the European Economic Area;
        iv. That Recordings and Analysis Data are stored only on systems designated by the Real Estate Organization Director and are not further disseminated unlawfully or kept longer than necessary.
3. The Security Manager is responsible for:
    a. Advising faculty boards and department directors on the placement, adjustment and commissioning of a Camera System at a Location;
    b. Advising faculty boards and departmental managements on the renewal of access to live Recordings for employees of receptions, front offices and control rooms of the faculty or department;
    c. Assisting faculty and departments in conducting a DPIA;
    d. Managing the access rights of employees of the UG physical security organization to Recordings made in line with this policy;
    e. Preparing and publishing a Privacy Statement on Camera Surveillance, which informs Data Subjects in accordance with the requirements of the GDPR about the Processing of Personal Data resulting from Camera Surveillance.
    f. The exercise of the duties, responsibilities and powers assigned above to the Real Estate Organization Director in cases where the Camera System is mobile.
4. Faculty Boards and Department Directors are charged with:
    a. Making a decision regarding the conduct of Camera Surveillance at a Location used by their faculty or department;

b. Use of the Camera System in compliance with the legal obligations under the GDPR and other applicable laws and regulations, this policy and the UG Privacy and Information Security Policy. This includes:
   i. that the use of Camera Surveillance is for the purposes authorized by this policy and less intrusive means to achieve those purposes are not sufficiently effective;
   ii. that the necessity, subsidiarity and proportionality of the Camera Surveillance and related processing operations be assessed prior to making a decision to do so and then minimum every three years evaluated, where necessary with a DPIA;
   iii. that the advice of the Real Estate Organization Director and the Security Manager be sought prior to the installation of a Camera System;
   iv. that for Camera Surveillance, only Camera Systems included in the portfolio of The Real Estate Organization Director and the Security Manager will be purchased;
   v. that only employees of the faculty/department for whom it is necessary are granted access to the Recordings, Analysis Data and Personal Data;
   vi. that Data Subjects are informed of the Camera Surveillance at the Locations where the Faculty Board or Management conducts Camera Surveillance;
   vii. that the need for Camera Surveillance is minimum every three years evaluated and is carried out in accordance with this policy. The faculty board or management shall designate an employee to ensure the implementation of the obligations set forth in the preceding paragraph.

5. In carrying out their duties, responsibilities and powers, the Real Estate Organization Director, the Security Manager and the Faculty Boards and Managements of Services shall seek prior advice from the Privacy & Security Coordinator of their organizational unit.
6. The independent UG Data Protection Officer monitors compliance with this policy and reports on it at least annually to the Executive Board in his annual data protection report. This report is submitted to the University Council for information after the Executive Board has taken note of it.

Article 5. Placing cameras, informing Data Subjects

1. When deciding to install a Camera System, a proper consideration is always made between the protection of the privacy of the Data Subjects on the one hand and the interests of the UG on the other. The authorized Privacy & Security Coordinator of the faculty or department advises whether a DPIA should be carried out.
2. In Locations where persons need to be undisturbed, such as in restrooms, showers and locker rooms, Camera Surveillance is not permitted at any time.

3. Camera surveillance will be used only for the purposes stated in this policy, in locations where it is necessary, proportionate and less intrusive measures are not (sufficiently) effective.
4. The need for Camera Surveillance at a particular Location will be reviewed minimum every three years. In the event that the Camera System is mobile, the necessity will be reconsidered within a maximum of 3 months.
5. Camera surveillance is made known by means of signs, stickers and/or displays at the entrances and exits of the Locations with Camera surveillance, as well as in the Locations. These refer to a publication of this policy and a privacy statement on the public website of the UG. Data Subjects shall be informed of the purposes of the Camera Surveillance, the circumstances under which their Personal Data are processed and the rights they have with respect to the Processing of their Personal Data.
6. Camera surveillance is not intended to follow Data Subjects as they perform their work or visit. 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, Data Subjects may be continuously monitored if this is necessary and less drastic measures are not (sufficiently) effective.
7. The Real Estate Organization Director and the Security Manager will provide a useful record of installed Camera Systems with a record of where they are installed.

Article 6. Retention periods

1. The Recordings and Analysis Data are retained for up to 14 days after they are created, after which they are irreversibly deleted unless:
    a. the Recordings and/or Analysis Data are related to an Incident. In that case, Images will be retained for a period of up to four weeks after the investigation or treatment of the Incident is concluded; or
    b. a request has been made by a Data Subject regarding the Recordings and/or Analysis Data. In this case, the Recordings will be retained until the procedure to process the request has been completed.

Article 7. Access to Recordings

1. Recordings and Analysis Data made with Camera Surveillance are only accessible to employees of the UG and other persons for whom this is necessary for the purposes specified in Article 3, paragraph 1. They should receive instructions for the purpose of careful handling of the Recordings and Analysis Data in accordance with the GDPR and this policy before access is granted.
2. Access to Recordings and Analysis Data shall, whenever possible, take place within the Camera System in which the Recordings and Analysis Data are recorded so that no copies of the Recordings and Analysis Data are made and stored on any other data medium.
3. Access to *live* images and audio will in principle only be provided to:

   a. Employees of receptions, front offices and control rooms working at the Locations where and/or around which the Recordings are made;
   b. Employees of the Physical Security Organization.
4. Access to stored Recordings and Analysis Data is provided in principle only to:
   a. Employees of the Physical Security Organization;
   b. Other employees responsible for the physical security of the UG or responsible for securing or managing goods and property of the UG, after review and approval of the Security Manager.
5. The Security Manager records the access granted to stored Recordings and Analysis Data. The Security Manager checks access rights to Camera Systems at least annually to eliminate unauthorized access as much as possible.

Article 8. Covert Camera Surveillance.

1. Only in special circumstances may covert cameras be used at UG locations. There must be a reasonable suspicion of criminal or fraudulent acts by the person or persons on whom the Covert Camera Surveillance is focused.
2. The decision to conduct Covert Camera Surveillance is made by the Executive Board based on a justification prepared by the responsible faculty or departmental management, with the advice of the Head of Administrative and Legal Affairs (BJZ).
3. The Head of BJZ is responsible for conducting an overarching DPIA on Covert Camera Surveillance. The University Council will receive a copy of this DPIA for information.
4. Covert Camera Surveillance is always temporary for a period proposed by the appropriate faculty or department management. This period is a maximum of 3 months.
5. Covert Camera Surveillance is permitted at clearly delineated Locations and only aimed at demonstrating actions as referred to in paragraph 1. University-wide or faculty-wide Covert Camera Surveillance is not permitted.
6. Covert camera surveillance can only be used as a 'last resort' after other means have proven to be insufficiently effective. Covert Camera Surveillance is carried out by independent persons, who are not employed by the UG if necessary.
7. The UG will subsequently inform the Data Subject(s) about the deployment of Covert Camera Surveillance as soon as its deployment is no longer necessary to achieve purposes as stated in Article 8 (1).
8. The Recordings made with Covert Camera Surveillance are accessible only to members of the appropriate faculty or departmental management, the Head of Administrative and Legal Affairs, the Data Protection Officer and members of the Executive Board. This is contrary to Article 7(3) and (4) of this policy.
9. The retention periods mentioned in Article 6 also apply to Recordings made with Covert Camera Surveillance.

Article 9. Inspection and disclosure of Recordings to third parties.

1. Inspection and provision of the Recordings and/or Analysis Data to third parties will only take place:
   a. at the request of the police or prosecutor's office;
   b. When reporting (a suspected) crime; or
   c. in other cases when it is compatible with purposes stated in this policy and the law provides a basis for doing so.
2. Requests to inspect and issue Recordings and/or Analysis Data should be submitted to the Head of Administrative and Legal Affairs of the UG. The Head of Administrative and Legal Affairs assesses whether the request from the police or the prosecutor's office provides a sufficient basis for the requested access and/or issue. The Head of Administrative and Legal Affairs has the mandate to decide on behalf of the Executive Board on a request for inspection or issue.
3. Actual execution of the request is done by the Security Manager. Any person who may inspect the Recordings and/or Analysis Data or receive a copy thereof must present identification to the Security Manager beforehand. The Security Manager records the request and decision to provide it.

Article 10. Rights of Data Subjects.

1. A Data Subject has the right to inspect the Personal Data recorded in the Recordings and Analysis Data. The UG is entitled to ask the Data Subject to explain where and when Recordings were made of them according to the Data Subject, before it starts processing a request for inspection.
2. The UG may refuse access if, for example, it is necessary in the interests of preventing, detecting and prosecuting criminal offenses or to protect the rights and freedoms of others.
3. A Data Subject has the right to have Personal Data concerning them deleted or blocked to the extent that such Personal Data is unlawfully processed or the Personal Data is not or is no longer relevant for the purpose for which it was collected.
4. A Data Subject has the right to object to the use of their Personal Data by the UG. The UG will weigh the Data Subject's objection against the interests of the organization. If the Data Subject's objection is well-founded, the UG will terminate the Processing in question.
5. The requests referred to in paragraphs 1, 3 and 4 can be addressed to the Privacy Central Office at privacy@rug.nl

Article 11. Complaints

1. A Data Subject may at any time contact the Data Protection Officer of the UG on any matter relating to the processing of their Personal Data. This can be done by e-mail at fg@rug.nl.
2. Complaints about the application of Camera Surveillance and the implementation of this policy, may be submitted in writing to the Executive Board according to the procedure of the general complaints procedure of the UG.[2]
3. The Data Subject may at any time lodge a complaint with the Personal Data Authority[3] about the processing of Personal Data by the UG.

Article 12. Final Provisions

1. After approval by the University Council, this policy was adopted by the Executive Board on May 23, 2025 and applied from that time.
2. This policy replaces the University of Groningen Camera Surveillance Regulations, last adopted on July 13, 2015.
3. Management of this policy is vested in the Chief Privacy Officer of the UG.
4. In cases not covered by this policy, the Board of the University shall decide with due regard to the applicable rights and powers of the University Council.
5. This policy shall be reviewed no later than three years after the day it became applicable.

[2] See: https://www.rug.nl/about-ug/organization/rules-and-regulations/vertrouwelijkheid-klachten-bezwaar-beroep/algemene-klachtenregeling
[3] See the AP's website: https://www.autoriteitpersoonsgegevens.nl/een-tip-of-klacht-indienen-bij-de-ap#het-meldformulier.