REGULATIONS ON CAMERA SURVEILLANCE AT MAASTRICHT UNIVERSITY

Article 1 The aim of and basis for camera surveillance, necessity and proportionality

1. Maastricht University (hereinafter: UM) uses Camera Surveillance with the aim of:
   a. protecting the health and safety of employees and students and visitors to UM;
   b. safeguarding access to UM buildings and sites;
   c. protecting property present in UM buildings or on UM sites;
   d. recording incidents;
   e. regulating traffic flows for students, employees and visitors to UM for reasons of traffic safety.
2. The wish to represent the legitimate interests of UM in line with the aims set out in Paragraph 1 forms the basis for the processing of Personal Data by means of Camera Surveillance.
   The requirements of necessity and proportionality and all other legal requirements set out in the General Data Protection Regulation (GDPR) will be observed during all Camera Surveillance by UM.

Article 2 Scope

These regulations will apply in relation to all UM surveillance cameras. Cameras that are used to record lectures will fall outside the scope of this regulation.

Article 3 Definitions

1. ***GDPR****:* the General Data Protection Regulation (EU Regulation nr. 2016/679);
2. ***Data Subject***: the individual to whom Personal Data pertain (Article 4(1) of the GDPR);
3. ***Camera System***: the entirety of cameras, monitors, recording equipment, servers, junction boxes, connections and mountings or other forms of data transport of visual material and/or equipment;
4. ***Camera Surveillance***: the production of images of one or more individuals, using a clearly visible camera or cameras, the Controller having clearly notified the student, employee or visitor of the possibility of camera surveillance in generally accessible rooms in the university buildings and at university sites, not being the workplaces;
5. ***Operator***: the employee who watches the images live and who is responsible for operating the Camera System;
6. ***Third Party or Third Parties****:* a natural person or legal entity, public authority, agency or body other than the Data Subject, the Controller, the Processor, or any person who is authorised to process personal data under the direct authority of the Controller (Article 4(10) of the GDPR);
7. ***Data Protection Official (FG)***: the employee that the Executive Board has appointed to supervise compliance with and application of the GDPR;
8. ***Functional Manager***: the UM employee who is responsible for managing the Camera System on behalf of the Controller;
9. ***Authorised Employee***: the employee who has access to or works in the space designated as a video observation area;
10. ***Building Manager***: an employee who the Head of the Administrative Unit has appointed in this role;
11. ***Data***: the camera images captured and registered by the Camera System and possibly containing Personal Data;
12. ***Head of the Administrative Unit***: the dean of a faculty, or the director of a service centre or MUO;
13. ***Incident***: an observed act, accident or other occurrence requiring immediate action;
14. ***Personal Data***: every piece of Data pertaining to an identified or identifiable natural person (Article 4(1) of the GDPR);
15. ***Reception/Porter's Lodge****:* the space from which a porter or receptionist is able to view the live camera images;
16. ***System Owner***: the individual that the Executive Board has made responsible for the Camera System and its management (the Facility Services Director, for example);

17. ***Technical Manager***: the employee responsible for technical management of the Camera System;
18. ***Processor***: a natural person or legal entity, public authority, agency or other body that processes Personal Data on behalf of the Controller (Article 4(8) of the GDPR);
19. ***Controller***: a natural person or legal entity, public authority, agency or other body that establishes the object of and resources to be used for processing Personal Data, which he/she/it does either alone or with others. UM is the Controller in relation to the use of Camera Surveillance;
20. ***Processing Personal Data***: any operation or set of operations that is performed on Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4(2) of the GDPR);
21. ***Video Observation Area***: the closed-off space from which the images can be viewed via recording equipment. This could be an area/workplace chosen specifically for this purpose, where film images can be viewed using the technical facilities available.

Article 4 Tasks and responsibilities

1. The Executive Board (hereinafter: EB) at UM is responsible for Processing Personal Data.
2. The Facility Services Director has been appointed to the role of System Owner and is responsible for Camera Surveillance vis-à-vis the EB.
3. The System Owner is responsible for ensuring that effective technical and organisational measures are put in place to protect the Camera System.
4. The Facility Services Director has delegated management of the Camera System to the Functional Manager. The Functional Manager will decide on the positioning of cameras, responsibility for doing which has been delegated to the said manager by the Facility Services Director.
5. Technical management of Camera Surveillance has been conferred on the Technical Manager. Technical management will be effected subject to the responsibility of the System Owner.
6. Authorised Employees are appointed to this role by or on behalf of the EB and will have access to the camera images by virtue of their positions.
7. Operators and Authorised Employees are authorised to watch camera images live and to operate the Camera System. Both are obliged to treat these Data as confidential, in accordance with the provisions of Article 1.16 of the Collective Labour Agreement for Dutch Universities (*CAO Nederlandse Universiteiten*).
8. In the event of an Incident, the Operator, porter or receptionist will report it to the appropriate authority.

Article 5 The installation of cameras

1. Individuals are informed of the use of Camera Surveillance in various ways, including the use of signs or images on UM sites and at the entrances to UM buildings. Data Subjects will also be notified of the identity and contact details of the Controller, putting them in a position to exercise their rights, as referred to in Article 11 below or in Chapter III of the GDPR.
2. Cameras may be installed at the request of the Building Manager. Requests will be submitted to the Functional Manager. The Functional Manager will then carry out an assessment based on guidelines determined by the System Owner before deciding whether or not a camera may be installed.

Article 6 Hidden Camera Surveillance

1. In special circumstances, hidden cameras may be used temporarily at UM sites and in UM buildings to protect and ensure the security of persons and property if criminal offences or other reprehensible behaviour are suspected. The use of hidden Camera Surveillance may only be permitted with due observance of the legislative framework.
2. A hidden camera may only be installed with the permission of the EB.
3. The Functional Manager may propose the installation of a hidden camera after consulting the System Owner and the Head of the Administrative Unit in question and

after obtaining the advice of the Data Protection Official. The Building Manager in question will be notified should a hidden camera be installed.

Article 7 Security

The System Owner will ensure that appropriate technical and organisational measures are put in place to secure Personal Data against loss or any form of unlawful processing.
A risk assessment relating to the Camera System has been carried out in accordance with the UM classification guidelines. The risk profile has been assessed as Medium, Medium, Medium for Availability, Integrity and Confidentiality respectively. All security measures established by UM in relation to this risk profile have been implemented and are assessed on a regular basis.

Article 8 Access to the Camera System

1. Where individuals appointed by or on behalf of the EB require access to Data in relation to the performance of their duties, they will have direct access to Personal Data.
2. Unauthorised persons or Third Parties will not have any access to the Camera System.

Article 9 Reporting

1. A confidential logbook will be kept in which use of the Camera System is recorded.
2. The following will be recorded: the name of the Operator on duty, the date, time and any particulars such as malfunctions, Incidents, reports, demands for Data.
3. The logbook will be kept in a locked cupboard when not in use.
4. All particulars and irregularities observed will be reported to the Functional Manager immediately.
5. Each year, the Functional Manager will submit a report to the System Owner about Incidents, use of the logbook, findings in relation to the logbook records and consultation of the material.
6. When asked to do so, the Functional Manager will provide an overview listing the names of Operators and Authorised Employees.

Article 10 Managing Data; retention period

1. Data will only be used for the purposes stated in Article 1 of this regulation.
2. Data will not be retained any longer than necessary; the guideline is a retention period of 7 calendar days. By way of exception, the retention period is 14 calendar days during the week between Christmas and New Year's Eve when the UM is closed.
   Where there are well-founded reasons for deviating from the above, including the need to deal with an Incident that has been recorded on a camera, the Data in question will be retained as long as necessary for further investigation, for any measures to be put in place and until the Incident observed has been dealt with. The Executive Board or a duly authorized person shall decide whether there are well-founded reasons for deviating from the retention period.

Article 11 The rights of Data Subjects

1. In accordance with Chapter III of the GDPR, a Data Subject has a number of rights, including a right to information about Processing (Article 13 of the GDPR), right of access (Article 15 of the GDPR), right to erasure (Article 17 of the GDPR), right to restriction of Processing (Article 18 of the GDPR), right to Data portability (Article 20 of the GDPR) and right to object (Article 21 of the GDPR), all of the aforementioned with due observance of the relevant conditions and restrictions prescribed by law. If a Data Subject wishes to exercise one or more of the aforementioned rights, s/he will be required to submit a request to the EB via privacy@maastrichtuniversity.nl.
2. Access to Data will always be provided under the supervision of the Functional Manager or another Authorised Employee appointed to this role by or on behalf of the EB. Prior to

accessing Data, the Data Subject will provide proof of his/her identity in the presence of the persons referred to in the previous sentence. Data Subjects that gain access to Data will sign an access declaration.
3. Complaints relating to use of the Camera System and/or the conduct of employees involved in Camera Surveillance will be submitted to the EB in writing and will be dealt with in accordance with the procedure applicable in this respect.
4. The EB will decide on a request or complaint within six weeks of the date on which it is received.

Article 12 Release of Data and access by Third Parties

1. Data will only be issued to Third Parties, including investigating officers and the examining magistrate, on request, demand and/or on the basis of a verified legal basis. A request or demand of this nature must be directed to the EB via privacy@maastrichtuniversity.nl.
2. Data will be exchanged in joint consultation and in a secure manner.
3. Third Parties will only be permitted to access Data with due observance of current legislation and regulations.
4. Access will take place in accordance with Article 11(2).
5. The Third Party in question will sign for receipt of or access to the Data.
6. The EB will decide within six weeks of the date on which a request or demand is received.

Article 13 Manner of disclosure

The Regulations on Camera Surveillance at Maastricht University will be published online on the UM website.

Article 14 Final provisions

1. The EB will make a decision on all cases not provided for by this regulation.
2. These regulations will enter into force on the day after the date of its adoption by the EB and will replace the version adopted in 2006.

Once approved by the University Council and Local Consultative Body, adopted at the meeting of the Executive Board held on 18 December 2018.

Maastricht, 18-12-2018
JZ 18.003