SLEZSKÁ UNIVERZITA

Rector’s Directive No. 5/2022

Camera systems at the Silesian University in Opava

Opava, September 2022

SLEZSKÁ UNIVERZITA

Rector's Directive No. 5/2022

Camera systems at the Silesian University in Opava

Article 1

Introductory provisions

1) This Directive outlines the procedures governing the installation and management of CCTV systems by the Silesian University in Opava (hereinafter referred to as "the University") and the handling of any footage recorded by the systems.

2) The legal framework governing the operation of the CCTV system at the University relies primarily on the following legal regulations:

   a) European Convention on Human Rights and Fundamental Freedoms,

   b) The Charter of Fundamental Rights and Freedoms of the Czech Republic,

   c) Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (the "Regulation"),

   d) Act No. 110/2019 Coll., on the processing of personal data,

   e) Act No. 262/2006 Coll., Labour Code, as amended,

   f) Act No. 89/2012 Coll., Civil Code, as amended.

3) This Directive shall not apply to CCTV systems that are not intended for monitoring individuals' behaviour or involve surveillance of individuals.

Article 2

List of terms and abbreviations

1) "The CCTV system" refers to a permanent technical system that automatically captures and may store visual or audio outputs (recordings) from monitored locations.

2) "The CCTV system with recording" refers to a camera system that allows for the storage of video or audio output from monitored locations.

3) "Personal data" refers to any information concerning an identified or identifiable natural person. In the context of CCTV systems, personal data is only captured by a CCTV system if all of the following conditions are met:

   - the monitoring takes place in areas where the presence of natural persons (individuals) can be expected,
   - these individuals can be identified, primarily through visible identifying features such as their face (either through CCTV footage or in combination with other information, such as information from the access control system),
   - a record is created of the locations monitored.

4) "Data subject" refers to a natural person whose personal data is being processed.

5) "Processing" refers to any operation or set of operations performed on personal data or sets of personal data, whether automated or not, including collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other disclosure, alignment or combination, restriction, erasure or destruction.

6) "Administrator" refers to the University.

7) "Recipient" refers to a natural or legal person, public authority or other entity who receives the personal data.

8) "Consent" of the data subject refers to a voluntary, concrete, informed and unambiguous expression of the individual's will regarding the processing of their personal data that is given through a declaration or other clear acknowledgement.

Article 3

Basic principles of operation of the camera system operation

1) The University is permitted to operate the CCTV system under the following conditions:

   a) other means of achieving the objectives outlined in Article 6 have been exhausted, i.e. as a means of ultima ratio (principle of minimum use), and

   b) the monitoring of data subjects is carried out in a proportionate manner, limited to the extent necessary for the protection of the interests of the University or other parties (principle of data minimization).

2) The operation of the CCTV system shall not unduly infringe upon the rights of data subjects, particularly their right to privacy. This is typically achieved by monitoring only entrances, exits, car parks, technically important zones or areas with high-value equipment. Monitoring can also be limited to specific time periods rather than continuous surveillance.

3) As a general principle, the camera system must be operated in a manner that avoids excessive monitoring of public spaces, such as streets or squares (principle of prohibition of unreasonable monitoring of public spaces).

4) The University engages in CCTV surveillance solely through open (not covert) methods. The transparency of the surveillance is achieved by appropriately informing the data subjects about the presence of surveillance, typically by means of information signs and additional notices (transparency principle).

5) It is not permitted to make or transmit audio recordings from monitored locations via the university CCTV system (principle of prohibition of making or transmitting audio recordings).

Article 4

Basic principles of camera system operation with recording

1) Surveillance using a camera system with recording is only permissible if measures are in place to ensure that the recorded footage that allows identification of the data subjects will be stored only for a limited period of time. Typically, this period must not exceed 5 days, a maximum of 10 days. The recorded footage shall not be backed up (storage limitation principle).

2) Personal data generated during the operation of the camera system with recording must be processed in a manner that guarantees security and protection against unauthorized or unlawful processing, as well as protection against accidental loss, destruction or damage (principle of integrity and confidentiality).

3) Surveillance using a camera system with recording may only be done in cases provided for by law. At the University, this will generally involve monitoring based on the protection of legitimate interests of the University or third parties, as outlined in Article 6(1)(f) of the Regulation. The operator of the CCTV system may collect video footage without the consent of the data subjects, provided that the legitimate interests outweigh the fundamental rights and freedoms of the data subject (principle of lawfulness and proportionality of personal data processing).

4) In principle, the processing of personal data through a camera system with recording should not involve special categories of personal data, as defined in Article 9 of the Regulations. These categories include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for unique identification, data concerning health, sex life or sexual orientation of a natural person, as well as personal data related to criminal convictions and offences (principle of prohibition of processing special categories of data and data relating to criminal convictions and offences). However, the processing of such data may be permitted under specific circumstances as permitted by data protection legislation.

Article 5

Operation of the camera system by the University units

1) The head of the unit responsible for operating the relevant CCTV system (hereinafter referred to as “the CCTV system operator”) is authorized to decide on the operation, form and scope of the CCTV system. The head of the unit is accountable to the rector for ensuring compliance of the CCTV system with the internal regulations and standards of the University.

2) When there is a need to introduce or expand the CCTV system, strict adherence to all applicable legal regulations, internal rules and standards in this field is essential. Special care must be taken to protect the privacy of staff and students. The CCTV system operator is responsible for evaluating these aspects and shall seek the opinion of the Data Protection Officer before implementing or expanding the CCTV system.

3) The CCTV system operator is required to appoint a person (or persons) who will be responsible for the operation of the CCTV system within their unit (hereinafter referred to as “the designated person”). It is the responsibility of the CCTV system operator to ensure that the designated person is familiar with this standard

and adequately trained in the operation of the CCTV system. If no designated person is appointed, the head of the unit assumes responsibility for fulfilling the duties outlined in the Directive.

4) The fundamental characteristics of the CCTV system with recording are documented in the personal data processing register, as specified in the standard concerning the protection of personal data at the University.

Article 6

Purpose of the camera system and legal basis for processing

1) The university CCTV system generally serves the following purposes:

   a) protection of property and personal safety,

   b) prevention of damage, vandalism and crime committed on the property of the University or other individuals,

   c) monitoring access and entry to property used by the University,

   (d) enhancing the prevention of unauthorized interference with technological equipment,

   (e) capturing evidence and, if required or permitted by law, disclosing it to public authorities or other entities (e.g. an insurance company).

2) The university CCTV system is not intended for:

   a) systematic monitoring of the behaviour of data subjects or systematic and automated evaluation of such monitoring,

   b) monitoring of the behaviour of the university students.

3) The university CCTV system is not intended for monitoring its employees during or in connection with their work activities. However, the CCTV system operator may decide otherwise under specific conditions.

4) In justified cases, the CCTV system operator may establish additional processing purposes for a particular unit within the University.

5) The legal basis for the processing of personal data by the CCTV system with recording is typically a legitimate interest of the data controller pursuant to Article 6(1)(f) of the Directive. This legitimate interest lies in the protection of the values and interests of the University as described in paragraph 1.

6) The operator of the CCTV system with recording is obligated to establish a different legal basis for the operation of the CCTV system in specific cases pursuant to paragraph 4). The operator must provide a justification for this legal basis.

Article 7

Designated person

1) The designated person is responsible for taking measures to prevent unauthorized or accidental access, alteration, destruction, loss, unauthorized transfers and processing, or other misuse of personal data. This obligation remains in effect even after the processing of personal data has ceased.

2) Unless otherwise specified by the CCTV system operator, the designated person is obligated to:

   a) Ensure the implementation of the technical and organizational measures outlined in Article 9.

   b) Maintain the confidentiality of the processed personal data and the security measures in place to protect it. This obligation continues even after the termination of the employment relationship.

c) Ensure compliance with the information duty by placing information notices at all entrances to the university buildings or premises where the CCTV systems are in operation.

d) Ensure the continued functionality of the CCTV system.

e) In the event of a CCTV system failure, arrange for repairs or secure access to the relevant components of the CCTV system to a technician from the service organization and supervise the technician during the repair.

f) Safeguard their login details (username and password) for exporting recorded data.

g) Keep an operating log or similar record documenting activities related to the operation of the CCTV system (hereinafter referred to as "the operating log").

h) Record activities and events in the operating log that serve as evidence of system usage, including equipment failures, record exports and service interventions. Each record shall include the date, time and description of the activity (event) and the name and signature of the person recording it.

i) Assess the impact and compliance with applicable legislation when making changes to the installation or operation of CCTV systems.

Article 8

Persons authorized to monitor cameras and footage

1) Besides the head of the unit and the designated persons, only individuals whose work requires access to the camera system and imaging workstations (e.g. doorkeepers) or external individuals (e.g. service technicians) have access to the camera system and imaging workstations.

2) Individuals who come into contact with personal data obtained and processed by the camera system are obliged to maintain the confidentiality of personal data and security measures. Disclosure of this information would jeopardize the security of personal data. The obligation of confidentiality shall continue even after the termination of employment.

3) All employees authorized to view camera footage are required to:

   a) Use the CCTV system only for the intended purposes and in compliance with the law, internal regulations and university standards.

   b) Prevent unauthorized persons from viewing camera footage.

   c) Refrain from capturing images of the imaging workstations by any means (video camera, camera, mobile phone, screen capture or any other means).

   d) Inform the designated person in case of non-standard situations (e.g. system failure).

4) Only the head of the unit, the designated person or their representative have access to the CCTV footage. The head of the unit is authorized to grant access to the camera footage to other persons for compelling reasons.

Article 9

Implementation of technical and organizational measures for the protection of personal data

1) The CCTV system operator is responsible for implementing suitable technical and organizational measures for the protection of personal data.

2) The CCTV system operator must ensure the following:

   a) Cameras are protected with covers and positioned at a height beyond the reach of individuals in the monitored areas.

b) Transmission paths are secured to protect communication between cameras and servers.

c) Access to recording devices is granted only to authorized personnel on the basis of predefined conditions.

d) Interference with the recording equipment, including repair or maintenance, is allowed only with the permission of or in the presence of the designated person or a person authorized by the designated person.

e) Record exports are carried out only by the designated person or by a person authorized by the designated person and are limited to specific circumstances described below.

f) The media used to store the records are disposed of safely and securely.

3) The CCTV system operator must maintain documentation of the implemented technical and organizational measures.

Article 10

Camera setting

1) The operator of the camera system is responsible for minimizing the surveillance of public spaces (streets, squares, etc.). If monitoring of public spaces is necessary to fulfil the purpose of the CCTV system, the CCTV system operator must ensure that the monitoring is carried out only to the minimum extent required to fulfil the purpose of the monitoring. This can be achieved through appropriate routing, angle adjustments, the scope of the camera shot, etc.

2) The CCTV system operator is obligated to ensure that CCTV surveillance is not conducted in places where the right to privacy of persons can be expected to be higher. Such areas are toilets, showers, changing rooms, rest areas for employees or students, etc.

3) The operator of the CCTV system shall ensure that CCTV surveillance does not take place in areas designated for teaching purposes. In cases where monitoring of such premises is strictly necessary, the CCTV operator must ensure that the premises are not monitored at times when natural persons are authorized to be present or that the CCTV systems do not intentionally capture images of individuals.

4) However, if all relevant individuals have provided valid consent in accordance with the law (including the Civil Code, the Labour Code, and the Directive), CCTV surveillance in teaching premises in the presence of individuals may be permitted.

Article 11

Marking of monitored premises and performing information duty

1) The CCTV system operator is required to ensure that each monitored area is clearly marked with an information board, alerting individuals to the presence of the CCTV system before they enter the monitored area.

2) The information table must include, at a minimum:

a) a camera pictogram,

b) a notice indicating whether the premises are monitored with recording or without recording,

c) identification of the camera system operator (e.g. “The personal data processing administrator is the Silesian University in Opava” or a similar format),

d) a link to an information source with details on personal data processing (the university website or a designated person or department where more detailed information on the processing of personal data can be obtained).

3) Where appropriate, an information board can be produced not only in Czech but also in another language.

4) The Data Protection Officer is responsible for ensuring that general information regarding the processing of personal data by the CCTV system is regularly updated and available on the university website.

5) The individuals responsible for the relevant unit must provide necessary assistance to the Data Protection Officer or any other authorized personnel for the purpose of updating camera data on the university website.

Article 12

Provision of recorded personal data and publication of CCTV footage

1) Upon receiving a written request, a university unit will provide CCTV footage to another unit that demonstrates a legal interest supported by valid reasons.

2) As a matter of principle, CCTV footage is not shared with other entities. Exceptions to this principle include:

   a) providing footage to law enforcement authorities for the purpose of initiating or conducting criminal proceedings,

   b) providing footage to public authorities to initiate or conduct proceeding related to misdemeanours, administrative offences or similar cases,

   c) providing footage when required by law, court order or other public authorities,

   d) providing footage to other entities to protect the legitimate interests of the University (e.g. as evidence in civil court proceedings, or when reporting damage to an insurance company, etc.).

3) The University is also required to provide CCTV footage to the subject of the recording (Article 13).

4) Providing CCTV footage in other cases is generally not expected. In exceptional cases, the recording can be shared based on consultation with the Data Protection Officer.

5) The decision whether to provide CCTV footage shall be made by the designated person of the relevant unit or their representative. The designated person will evaluate the validity of the request, verify the identity of the applicant, the justification for the request and the extent of the disclosure. If the request is approved, the designated person shall retrieve the footage and make a copy of the relevant section.

6) The designated person shall decide on the provision of the record without delay. If this is not possible, they shall ensure that the relevant part of the recording is retained until the conditions for provision are met.

7) Each instance of providing CCTV footage must be documented in the operating log.

8) It is strictly prohibited to publish CCTV footage, including a copy or any other visual representation of the footage.

Article 13

Rights of the data subject

1) The rights of the data subject are defined in the directive and the internal standards issued by the University for the protection and processing of personal data.

2) In particular, the data subject has the following rights:

   a) the right to access personal data, including the provision of a copy of the relevant part of the footage concerning the data subject (subject to conditions specified in Article 15 of the Directive),

b) the right to request deletion of the relevant part of the footage (subject to conditions specified in Articles 17 to 19 of the Directive),

c) the right to request the restriction of processing (subject to conditions specified in Articles 18 and 19 of the Directive),

d) the right to lodge a complaint regarding the processing of personal data with a supervisory authority (subject to conditions specified in Article 77 of the Directive).

Article 14

Location and mode of operation of the camera system

1) The camera system is operated by the administrator within the premises and buildings of the University, as specified in Annexe 1.

2) The camera system operates primarily in continuous mode, or based on the settings of individual cameras.

3) The designated person of each university unit can provide information regarding the current location of the cameras, including the defined area of image capture.

Article 15

Employee monitoring by CCTV

1) Employee monitoring refers to the intentional and systematic use of a CCTV system to monitor the activities of employees during or related to their job activities. This includes monitoring work performance, adherence to work duties, and the use of university resources.

2) However, the incidental presence of an employee within the view of a camera or cameras, such as when entering buildings, moving through corridors, or in car parks, where the CCTV system is primarily used for a different purpose, does not constitute employee surveillance.

3) Employee monitoring by CCTV may only be conducted for reasons specified by law (particularly in Section 316 of the Labour Code). Employee surveillance is an exceptional measure that must be explicitly authorized by the head of the relevant unit.

4) Employee monitoring is permissible only if all of the following conditions are met:

   a) there is a compelling reason based on the specific nature of the activities of the University, its units, or the relevant department,

   b) all less invasive means of protecting the interests of the University have been exhausted or proven ineffective,

   c) monitoring will be carried out only to the extent necessary and proportionate to protect the interests of the University,

   d) the legal requirements for informing employees about the use of the CCTV system for employee monitoring, including its scope and methods, have been fulfilled; this includes complying with labour law provisions (and if the CCTV system records personal data, also the regulations on personal data protection).

5) Covert surveillance of university employees is strictly prohibited.

Article 16

Transitional and final provisions

1) Operators of CCTV systems are required to ensure that the components of all already existing CCTV systems comply with the provisions of this Directive within a period of 6 months from the date of its enforcement.
2) The Annexe Premises and Objects of the University with CCTV Operation is an integral part of this Directive.
3) This Directive shall enter into force and take effect on the date of its publication.

In Opava on

doc. Ing. Pavel Tuleja, Ph.D.

Rector

Annexe 1

Premises and Objects of the University with CCTV Operation

1) Faculty of Philosophy and Science:

A total of 35 cameras, 16 indoor and 19 outdoor, were installed in the buildings (and their surrounding areas):

Hradecká 665, 746 01 Opava

Masarykova třída 343, 746 01 Opava

Vávrovická 244, 746 01 Opava

Hauerova 728, 746 01 Opava

2) School of Business Administration:

A total of 54 cameras, 41 indoor and 13 outdoor, were installed in the buildings (and their surrounding areas):

Univerzitní náměstí 1934, 733 40 Karviná

Na Vyhlídce 1079, 735 06 Karviná

3) Faculty of Public Policies:

A total of 71 cameras, 59 indoor and 12 outdoor, were installed in the buildings (and their surrounding areas):

Bezručovo nám. 885, 746 01 Opava

4) Institute of Physics:

A total of 8 cameras, 3 indoor and 5 outdoor, were installed in the buildings (and their surrounding areas):

Bezručovo nám. 1150, 746 01 Opava

5) Rectorate:

A total of 28 cameras, 15 indoor and 13 outdoor, were installed in the buildings (and their surrounding areas):

Na Rybníčku 626/1, 746 01 Opava

Olbrichova 625, 746 01 Opava

Part of the University:	Rectorate
Designation:	**Rector's Directive**
Number:	**5/2022**
Name of the standard:	**Camera Systems at the Silesian University in Opava**
Approved by:	doc. Ing. Pavel Tuleja, Ph.D.
Derogation:	--
Valid from:	the date of publication in the public section of the website
Effective from:	the date of publication in the public section of the website
Release date:	6 September 2022
Published by:	Rector
Prepared by:	Mgr. Sabina Březinová
In cooperation with:	
Number of pages:	10
Number of annexes:	1
Method of publication:	Intranet/Public section of the university website