COLLECTION OF DECISIONS AND ORDINANCES OF THE UNIVERSITY OF SOUTH BOHEMIA IN ČESKÉ BUDĚJOVICE

Number: R 571 Date: 6 December 2024

Rector's ordinance regulating the rules of operation of the CCTV system

In accordance with the following generally binding legal regulations and in relation to the Rector's ordinance setting rules for the protection and processing of personal data,[1] I am issuing this ordinance:

Part One
General part

Article I
Subject of modification

1. This ordinance sets binding rules for the establishment and operation of the CCTV system by the University of South Bohemia in České Budějovice (hereinafter referred to as the '**University**') and for the handling of recordings made by this CCTV system.
2. The legal framework for the establishment and operation of the University's CCTV system is based mainly on the following legal regulations:
    a) European Convention on Human Rights and Fundamental Freedoms,
    b) Resolution of the Presidium of the Czech National Council No 2/1993, on the proclamation of the Charter of Fundamental Rights and Freedoms as part of the constitutional order 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, on the processing of personal data,
    e) Act No 262/2006, Labour Code, as amended,
    f) Act No 89/2012, Civil Code, as amended.
3. This ordinance is based on the Methodology for the design and operation of CCTV systems in terms of processing and protection of personal data of the Office for Personal Data Protection.

Article II
List of terms and abbreviations

1. **'CCTV system'** is understood as an automatically operated permanent technical system enabling the acquisition and, where appropriate, storage of video or audio recordings from monitored locations.
2. **'CCTV system with recording'** is understood as a CCTV system that allows for the storage of visual or, where appropriate, audio recordings of monitored locations. Where this ordinance refers to a CCTV system, it is always intended to mean a CCTV system with recording, unless otherwise specified below.
3. The **'operator'** of the entire camera system is the University as a whole. The Rectorate, faculties and other constituent parts of the University are the operators of the relevant parts of the CCTV system (Article V of this ordinance).

[1] Rector's Ordinance No R 378 of 17 May 2018 setting the rules for the protection and processing of personal data

4. Other terms used in this ordinance are defined in the Rector's Ordinance setting rules for the protection and processing of personal data (R 378). Given the subject matter of this ordinance, the terms are supplemented and clarified as follows:
   a) **'Personal data'** is understood as any information about an identified or identifiable natural person. In relation to CCTV systems, personal data is only captured by a CCTV system if all of the following conditions are met:
      I. if records are taken and stored from monitored locations where the entry of natural persons can be expected,
      II. the captured individuals are identifiable, i.e. their identifying features, particularly their face, are visible (based on the CCTV footage or in conjunction with other information, e.g. together with data from the access control system); and
      III. a record is made and kept of the locations monitored.
   b) The **'data subject'** in relation to CCTV systems is the natural person who is captured by the CCTV system.
   c) The **'processing'** of personal data is understood any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated processes, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other disclosure, alignment or combination, restriction, erasure or destruction.
   d) The **'administrator'** of the personal data captured by the CCTV system is the University.
   e) The **'recipient'** of personal data is understood as a natural or legal person, a public authority or another entity to which personal data are provided.

Article III
Basic principles of operation of the camera system

The following principles must always be observed when the University operates a CCTV system:

a) The acquisition and retention of CCTV footage is undertaken where other means of achieving the purposes set out in Article 4 of this ordinance have been exhausted and at the same time, the monitoring of data subjects by the CCTV system is carried out in a proportionate manner and only to the extent necessary to protect the interests of the University or other persons (principle of data minimisation).
b) The operation of the CCTV system must not unduly interfere with the rights of the data subject, in particular, the data subject's right to privacy (principle of non-infringement).
c) The University's camera system should be operated in such a way as to avoid unreasonable monitoring of public spaces, i.e. streets, squares, etc. (principle of prohibition of unreasonable monitoring of public spaces).
d) The camera system is operated by the University in an open manner only (not covertly). The openness of the operation is achieved by the University informing data subjects about the surveillance in an appropriate manner, in particular by means of information signs and additional information provided (transparency principle).
e) It is not permitted to make or transmit audio recordings from monitored locations via the University's CCTV system (principle of prohibition of making or transmitting audio recordings).
f) The operation of a camera system with recording is only possible if it is ensured that the recording is stored in a form that allows the identification of data subjects only for a limited period of time (storage limitation principle).
g) Personal data generated during the operation of the camera system with recording must be processed in a manner that ensures their proper security and protection against unauthorised or unlawful processing, or against accidental loss, destruction or damage (principle of integrity and confidentiality).
h) Recording and storage of footage by the CCTV system is only possible in cases provided for by law. The operator of a CCTV system may take CCTV footage on the basis of a relevant legal ground for a predetermined purpose in a proportionate manner (principle of lawfulness and principle of proportionality of processing of personal data).

i) The processing of personal data carried out by means of a camera system with recording does not, in principle, include the processing of data of so-called special categories of personal data pursuant to Article 9 of the regulation, i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data for the purpose of unique identification of a natural person and data concerning the health, sex life or sexual orientation of a natural person, as well as the processing of personal data relating to criminal convictions and offences (principle of prohibition of processing of special categories of data and data relating to criminal convictions and offences). However, the processing of these types of personal data is permitted where permitted by the University's data protection standard.

Article IV
Purpose of the camera system, legal basis for processing personal data

1. The purpose of operating the University's CCTV system is:
   a) protection of property and safety (life and health) of persons,
   b) prevention of damage, vandalism and crime committed on the property of the University or other persons,
   c) monitoring access and entry to property used by the University,
   d) to increase the level of prevention of unauthorised interference with technological equipment,
   e) to capture of the evidence and the possibility of disclosing it to public authorities or other entities (e.g. insurance companies) if such disclosure is required or permitted by law.
2. The purpose of the University's CCTV system is not, for example:
   a) systematic monitoring of the behaviour of data subjects in general or systematic or automated evaluation of such monitoring,
   b) monitoring the behaviour of the University's students,
   c) monitoring of its employees in the course of or in connection with their work.
3. The operator of the CCTV system is entitled, after consultation with the Data Protection Officer, to specify purposes other than those listed above for processing by the CCTV system of the University unit in writing; he/she shall justify these purposes.
4. The legal basis for the processing of personal data by the recording camera system is the legitimate interest of the administrator pursuant to Article 6(1)(f) of the regulation, as the processing is necessary to protect the values and interests described in section 1.
5. The operator of the CCTV system shall be entitled, in consultation with the Data Protection Officer, to specify in writing another legal basis for the operation of the CCTV system in specific cases; he shall justify this legal basis.

Article V
Rights of the data subject

1. The rights of the data subject are set out in the regulation and further regulated by the Rector's Ordinance setting rules for the protection and processing of personal data (R 378).
2. In particular, the data subject has the right to:
   a) access the personal data, including the provision of a copy of the part of the record relating to the data subject (under the conditions of Article 15 of the regulation),
   b) erasure (under the conditions of Articles 17 to 19 of the regulation),
   c) restrict processing (under the conditions of Articles 18 and 19 of the regulation),
   d) a notification regarding an erasure or restriction of processing (under the conditions of Article 19 of the regulation),
   e) object to processing (under the conditions of Article 21 of the Regulation); and
   f) lodge a complaint about the processing of personal data with a supervisory authority (under the conditions of Article 77 of the Regulation).

3. The data subject may exercise their rights in accordance with the procedure set out in the public section of the University's website (listed in the footer of https://www.jcu.cz/ – data protection).

Part Two
Operation of the camera system

Article VI
Operation of the CCTV system by the University and its constituent parts

1. The camera system is operated by the administrator in designated areas and buildings of the University.
2. The camera system is basically operated in a 24/7 mode, or according to individual cameras.
3. The Rector, Deans of faculties and Directors of other constituent parts of the University (hereinafter collectively referred to as '**heads of the constituent parts**') decide on the introduction and changes to parts of the CCTV system that relate to buildings and properties under the management of a given unit of the University. The rectorate, faculty or other part of the University is the operator of these parts of the CCTV system (hereinafter referred to as '**CCTV system operator**'). The head of the University constituent part is responsible to the Rector for the compliance of the CCTV system with the legal regulations and internal standards of the university.
4. The operator of the camera system is responsible particularly for ensuring that data subjects are informed (placement of information boards according to Article XI), for the correct placement and direction of individual cameras, for their proper maintenance and for the fulfilment of other obligations of the operator of the camera system according to this ordinance.
5. In the event of the introduction or extension of a CCTV system, all applicable legislation must be complied with. In particular, the privacy of staff, students and other persons being filmed must be protected. The operator must consider the privacy implications and seek the written opinion of the Data Protection Officer before introducing or extending any CCTV system. Prior to physically placing and connecting a camera to the CCTV system, the operator is required to hand the camera over to a CIT staff member for testing and pre-configuration.
6. The software administration and development of the University-wide CCTV system is provided by the Centre of Information Technology (hereinafter referred to as '**CIT**'). The CIT employee responsible for the administration and development of the University's CCTV system according to his/her job title (hereinafter referred to as '**CIT employee**') is responsible particularly for the correct handling of requests for access to the University's CCTV footage (Article XII), the maintenance of the operating log (Article VII(3)) and the fulfilment of other obligations under this ordinance.
7. Each unit of the University is authorised to designate a person who will be responsible for the operation of the CCTV system at that unit (hereinafter referred to as the '**responsible person**'). The responsible person must be familiar with this arrangement and trained in the operation of the CCTV system. If no responsible person is designated, the head of the unit is responsible for the performance of the duties of the responsible person under this ordinance.
8. The basic characteristics of the operating CCTV system with recording are documented through the University's Personal Data Processing Register.

Article VII
CIT employee and responsible person

1. The CIT employee and the responsible person are obliged to take such measures to prevent unauthorised or accidental access to personal data, their alteration, destruction or loss, unauthorised transfers, other unauthorised processing or other misuse of personal data. This obligation shall continue to apply even after the processing of personal data has ceased.
2. The responsible person is obliged to:
    a) ensure the adoption of the technical and organisational measures referred to in Article 9(2) of this ordinance,

b) maintain confidentiality of the personal data processed and the security measures to protect it. This obligation shall continue after the end of the employment relationship,
c) ensure compliance with the information obligation by placing information boards at all entrances to the University's buildings or land used by the University in which or on which CCTV systems are operated,
d) ensure the permanent operability of individual cameras of the relevant part of the CCTV system,
e) in the event of a malfunction of the cameras, to ensure repair, or to provide access to the relevant components of the camera system to a technician of the service organisation and to ensure supervision of his/her activities during his/her presence,
f) assess the impact of such changes and inform the CIT employee and the Data Protection Officer in advance, in the event of changes in the location of individual cameras (e.g. relocation, change of lens orientation).

3. The CIT employee is required to:
   a) ensure the adoption of the technical and organisational measures referred to in Article 9(3) of this ordinance,
   b) protect his/her login details (username, password) for exporting recorded data,
   c) keep a camera system operation log or similar record of activities related to the operation of the camera system (hereinafter referred to as the '**operation log**') in the University's information system,
   d) record activities and events that serve to prove the use of the system in the operating log, in particular failures of individual devices, exports of records and service interventions. Each record shall contain at least the date, time and description of the activity (event) and shall show the name of the person recording the event,
   e) maintain a list of specific current camera locations in the University's information system, including defining the images captured.
4. The CIT employee and the responsible person (CIT and the University constituent part) are required to provide mutual assistance in the implementation of this ordinance.

Article VIII
Persons authorised to monitor cameras and recordings

1. Access to the CCTV footage is restricted to CIT employees only. Only a CIT employee is authorised to export the footage (make a copy); anyone wishing to make a copy of the footage must have his/her permission (Article XII). The responsible person of the University constituent part operating the individual parts of the CCTV system may access the recordings.
2. In addition to the CIT employees and the responsible person, only persons whose access to the CCTV system and imaging workstations is required by the nature of their work (doormen, cashiers) or, if necessary, external persons (service technicians) have access to the CCTV system and imaging workstations.
3. Persons coming into contact with personal data captured and processed by the CCTV system are obliged to maintain the confidentiality of personal data. All employees are obliged to maintain the confidentiality of security measures whose disclosure would compromise the security of personal data. The obligation of confidentiality continues after the end of employment.
4. All employees authorized to view camera footage are required:
   a) to use the CCTV system only for the purposes for which it is intended and in accordance with the law, internal regulations and University standards,
   b) not to allow unauthorised persons to view the camera footage,
   c) not to take screen captures of CCTV screens in any way (by camera, camera, mobile phone, screen capture or other means),
   d) inform the CIT employee or the person responsible in non-standard situations (e.g. malfunction) .

Article IX
Technical and organisational measures

1. The administrator of the CCTV system is obliged to ensure the security of the CCTV system and the protection of personal data, its availability, confidentiality and integrity through technical and organisational measures.
2. The operator of the CCTV system shall ensure in particular:
   a) protection of cameras by protective covers and placement at a height beyond the normal range of persons moving in the monitored areas; in the case of outdoor cameras, also protection from the weather,
   b) protection of transmission paths by suitable security of communication between cameras, NVR recording devices and servers (if they are located in the building of the constituent part),
   c) that intervention in individual cameras, transmission routes and NVR recording devices (if they are located in the building of the constituent part), including actions related to their repair or servicing, is possible only with the permission or in the presence of a responsible person of the relevant constituent part of the University, or a person authorized by it.
3. In particular, the CIT employee shall ensure:
   a) that access to the image of individual cameras is limited to authorised persons based on predefined permissions,
   b) that access to recordings from individual cameras is limited to authorised persons based on predefined permissions,
   c) that no one outside it has an unauthorised opportunity to export records, with data export only in the cases described below (Article XII).
4. The administrator of the CCTV system is obliged to document the technical and organisational measures.

Article X
Camera coverage

1. The operator of the camera system is obliged to ensure, in cooperation with the CIT employee, that the monitoring of public spaces (e.g. streets, squares) by the camera system is minimised. If the monitoring of a public space is necessary to fulfil the stated purpose of the CCTV system, the CCTV system operator shall ensure that the monitoring of the public space is carried out only to the minimum extent possible to achieve the purpose of the monitoring (e.g. by appropriate routing or suitable adjustment of the angle and extent of the camera view).
2. The operator of the CCTV system is obliged to ensure that CCTV surveillance does not take place in places where the exercise of the right to privacy of persons can be expected to be higher. Such areas are in particular toilets, showers, changing rooms, rest areas for employees or students, etc.
3. The operator of the CCTV system ensures that CCTV surveillance does not take place in areas intended for instruction. Where the monitoring of such instruction premises is strictly necessary, the CCTV operator ensures that such premises are not monitored at times when natural persons are authorised to be present in those premises or positions the CCTV system so that it does not target natural persons.
4. However, CCTV surveillance in the presence of individuals in the premises intended for instruction is possible if all the subjects concerned have duly consented to such surveillance in accordance with the law (the Civil Code, the Labour Code, and the regulation).
5. The operator of the CCTV system is responsible for ensuring that the camera coverage (angle of view, zoom level, etc.) does not allow observation of details or physical features that are not relevant to the stated purpose of the CCTV system.

Article XI
Marking of monitored areas (information board), fulfilment of information obligation

1. The operator of the CCTV system is obliged to ensure that each monitored area is marked with an information board so that the data subject is alerted to the CCTV system before entering the monitored area.

2. The information table contains at least:
   a) camera pictogram,
   b) an indication that the premises are monitored by a CCTV system with recording,
   c) unambiguous identification of the personal data administrator operating the camera system (in the form 'The University of South Bohemia in České Budějovice is the personal data administrator' or similar),
   d) a link to an information source containing more information about the processing of personal data and the rights of the data subject (the University's website and contact address).
3. Where appropriate, an information board can be produced not only in Czech but also in another language.
4. The Data Protection Officer will ensure the processing and continuous updating of information on the processing of personal data by the camera system in the public section of the University's website. The responsible persons of the University's constituent parts and the CIT employee will provide the Data Protection Officer with the necessary cooperation.

Article XII
Provision of copies of CCTV footage (footage exports)

1. The CIT staff member may provide footage from the University's CCTV system to a constituent part of the University on the basis of a written justified request.
2. As a matter of principle, CCTV footage is not transferred to other entities. An exception to this principle is the transfer:
   a) to law enforcement authorities for the purpose of initiating or conducting criminal proceedings,
   b) to public authorities in the context of initiating or conducting offence proceedings or similar proceedings,
   c) in other cases where the University is required by law, court or other public authority to provide the record,
   d) to other entities for the purpose of protecting the legitimate interests of the University, its employees and students (e.g. for the purpose of providing evidence in civil court proceedings, to prove the occurrence of a damage event to an insurance company, etc.)
3. Furthermore, the transfer shall take place if the data subject himself requests access to the record (Article 5 of this ordinance).
4. Transfers in other cases are not envisaged; exceptionally, transfers in other cases may be made in consultation with the Data Protection Officer.
5. Requests for records are received by a CIT employee. Requesting parties who have established a user account with the University are required to submit a request through the University's designated information system (currently available at: https://servicedesk.jcu.cz/). Other applicants submit a written request through normal channels. The request must include, at a minimum, identification of the requesting party, a specification of the record requested, and a justification. A request template is attached as Annexe 1 to this ordinance.
6. The decision to provide the record is made by the CIT employee. In doing so, he or she verifies the identity of the requesting party and assesses the validity of the request, the justification for the request, the specification of the scope of the disclosure and requests the opinion of the Data Protection Officer. In the event of a positive outcome of the assessment of the request, the CIT staff member shall make a copy of the relevant part of the record and transmit it in a manner that provides the necessary protection for personal data.
7. The CIT staff member decides on the provision of the record, as a rule, without undue delay and ensures that the relevant part of the record is retained for the time necessary to assess the validity of the request and to transmit the record.
8. A record shall be made in the operating log of each transfer of a record.
9. Publication of the CCTV footage with the recording, or a copy or other visual representation of such footage, is prohibited.

Part Three
Special cases of operation of the CCTV system

Article XIII
Recording camera in a University vehicle

1. If the operator of the camera system so decides, a recording camera may also be placed in a vehicle used by the University.
2. The purpose of recording cameras placed in University vehicles is to protect the property or other rights of the owner or user of the vehicle and to use the recording in connection with the resolution of a traffic incident or an attack on a property in use by the University; the purpose is not to systematically monitor University employees or other entities.
3. The management of recording cameras in the University vehicle is provided by the operator of the camera system.
4. The responsible person ensures that the use of a recording camera in a University vehicle does not invade the privacy of the employee or other subjects.
5. In the case of recording cameras in a University vehicle, there is no need to carry out a so-called data protection impact assessment, provided that the camera takes pictures of the public road, monitoring the necessary area in front of or behind the vehicle, for the purpose of documenting the accident and its investigation by the competent authorities. The camera technology must not have parameters that allow for simultaneous or subsequent processing of other data (for example, processing of biometric characteristics of the persons captured, processing of the recordings or data from them in other systems for other purposes).

Part Four
Transitional and final provisions

Article XIV
Transitional and final provisions

1. The individual constituent parts of the University are obliged to ensure compliance of the camera systems already in operation with this ordinance no later than 3 months from the date of this ordinance taking effect.
2. This ordinance rescinds the Ordinance of the Director of the CIT USB No 2/2007 on the Handling of Data obtained by the USB camera system of 2 July 2007.
3. This ordinance comes into force on the date of its issue and takes effect on 1 January 2025.

prof. Ing. Pavel Kozák, Ph.D., m. p.
Rector

Prepared by: Data Protection Officer, Centre of Information Technology

Distribution list: USB management, Deans of USB faculties, Directors of all other constituent parts of USB

Annexe: Request and protocol templates for providing footage from the University's CCTV system