MUNI
ECON

Directive of the Dean of the Faculty of Economics and Administration, Masaryk University, No. 2/2021

Camera system operation

(in the version effective from 1st January 2022)

Pursuant to Section 28 (1) of Act No. 111/1998 Coll., on Higher Education Institutions and on Amending and Supplementing Other Acts (Higher Education Act), as amended (hereinafter referred to as the "Higher Education Act"), I issue the following Directive:

Section 1
Subject Matter

1. This Directive lays down procedures for the processing, storage and management of recordings made by the camera system that is operated on the premises of the Faculty of Economics and Administration of Masaryk University, Lipová 41a, 602 00 Brno, in accordance with Act No. 101/2000 Coll., on Personal Data Protection , as amended (hereinafter referred to as the "Act").
2. Legal framework for the camera system operation:
    a. Act No. 101/2000 Coll., on Personal Data Protection, as amended,
    b. Act No. 262/2006 Coll., the Labour Code, as amended,
    c. Act No. 89/2012 Coll., the Civil Code, as amended,
    d. Opinion of the Office for Personal Data Protection No. 1/2006 – Operation of the camera system in terms of the Personal Data Protection Act,
    e. Statements and recommendations of the Office for Personal Data Protection on the possibility of installing a camera system on the school premises, 03/2007,
    f. Opinion of the Office for Personal Data Protection – Practical issues of camera system operation in schools and education, 05/2007,
    g. Opinion of the Office for Personal Data Protection – Camera system operation, 2012,
    h. ČSN EN series 50173 Information technology, as amended,
    i. ČSN EN series 50132 Alarm systems – CCTV, as amended,
    j. ČSN EN series 62676 Surveillance video systems for use in security applications, new ČSN series, until 2018 in parallel with the old series.

Section 2
List of terms and abbreviations

1. For the purposes of this Directive:
    a. *personal data* means any information relating to the identified or identifiable data subject – a data subject shall be considered identified or identifiable if the data subject can be, directly or indirectly, identified in particular by number, code or one or more elements specific to their physical, physiological, mental, economic, cultural or social identity;
    b. *sensitive data* means personal data indicating nationality, racial or ethnic origin, political attitudes, trade union membership, religion and philosophical beliefs, criminal

convictions, health and sexual life of the data subject and the data subject's genetic data; sensitive data is also biometric data that allows direct identification or authentication of the data subject;

c. *anonymous data* means such data that, either in their original form or after processing, cannot be related to an identified or identifiable data subject;

d. *data subject* means the natural person to whom the personal data relate;

e. *processing of personal data* means any operation or a set of operations that the controller or processor systematically carries out with personal data, either automatically or by other means; processing of personal data means, in particular, the collection, storage on a data medium, disclosure, modification or alterations, retrieval, use, transmission, dissemination, publication, storage, exchange, sorting or combination, blocking and disposal,

f. *collection of personal data* means a systematic procedure or a set of procedures aimed at obtaining personal data for the purpose of their further storage on an information medium for their immediate or later processing;

g. *storing personal data* means maintaining the data in a form that allows their further processing;

h. *blocking* means an operation or a set of operations that restrict the method or means of processing personal data for a specified period of time, with the exception of necessary interventions,

i. *destruction of personal data* means the physical destruction of their carrier, their physical deletion or their permanent exclusion from further processing,

j. *controller* means every subject that determines the purpose and means of the processing of personal data, carries out the processing and is responsible for it; the controller may authorise the processor to process personal data, unless a special law stipulates otherwise,

k. *processor* means any subject that, on the basis of a special act or authorisation by the controller, processes personal data in compliance with the law,

l. *published personal data* means personal data made available in particular by the mass media, other public communications or as part of a public list,

m. *record or personal data file* (*hereinafter referred to as a "data file"*) means any set of personal data sorted or made available in accordance with common or specific criteria,

n. *consent of the data subject* means the free and informed expression of the will of the data subject, the content of which is the data subject's consent to the processing of personal data,

o. *recipient* means every subject to which personal data are made available; the subject that processes personal data according to Sec. 3 para. 6 let. g) of the Act is not considered a recipient,

p. *authorised entity* means law enforcement authorities, the data subject and its legal representative, the subject that provided the consent pursuant to Sec. 5 of the Act.

Section 3
Camera system purpose

1. The purpose of the camera system installation is the protection of the property and safety of persons, prevention of damage, vandalism and crime committed on the property of the camera system operator and data subjects moving around the Lipová 41a premises, monitoring of the operation and use of the parking area and bike sheds of the Faculty of Economics and Administration and monitoring of experiments in experimental economics laboratories. The

operator of the camera system decided to install it after exhausting all possibilities of prevention and monitoring of incidents, including, for example, object protection of technology.

2. The camera system has a preventive function and is focused on the protection of the legitimate interests of the operator in the sense of the provisions of Sec. 5 para. e) of the Act. For this purpose, the camera system operator may obtain camera recordings without the consent of persons entering the monitored area, including employees, students, persons entering the premises for a short or irregular period, as well as persons moving in a public outside area around the premises – see the Opinion of the Office for Personal Data Protection (hereinafter referred to as "OPDP") in Annex No. 1.

3. The camera system is not used for systematic monitoring of people. The fixed setting of the camera lenses is such that the height of a body represents a maximum of 50% of the height of the entire camera shot. Detailed shots of persons are not displayed, so the right to privacy is not violated pursuant to Sec. 86 of Act No. 89/2012 Coll., the Civil Code.

4. The camera system is installed in such a way that the privacy of employees and students pursuant to Sec. 316 para. 2 of Act No. 262/2006 Coll., the Labour Code, as amended is not violated. This is achieved, for example, by monitoring only entrances, exits, parking areas, technically important areas or areas with high-value equipment.

Section 4
Camera system identification and its description

1. Identification (location) of the camera system:
Camera system in the Masaryk University premises, Faculty of Economics and Administration, Lipová 41a, Brno

2. Operator and administrator of the camera system:
Masaryk University, Faculty of Economics and Administration, Lipová 41a, 602 00 Brno, Company Identification No.: 00216224 (hereinafter referred to as the "faculty")

3. Personal data controller:
Masaryk University, Žerotínovo nám. 9, 601 77 Brno, Company Identification No.: 00216224

4. Contact details for requests and complaints:
Masaryk University, Faculty of Economics and Administration, Lipová 41a, 602 00 Brno, Company Reg. No.: 00216224

5. Service organization:
Information and Communication Technology Centre and Building Management of the Faculty of Economics and Administration, Masaryk University, Lipová 41a, 602 00 Brno

6. The list of cameras, their specification, placement of individual elements of the system around the premises, angles of view and images from individual cameras are given in Annex No. 2.

7. The cameras are located out of the normal reach of people moving in the monitored area. In all cases, these are day/night digital IP cameras. Indoor installed cameras are not in anti-vandal covers. Outdoor cameras are designed for use in extreme outdoor conditions. Video recordings are taken from all cameras. No sound is recorded by any camera, so no sensitive personal data is processed (see the Opinion of the OPDP in Annex 1).

8. Fixed camera shots – fields of vision – are set to provide a shot for "observation" of 25%, or "reconnaissance" of max. 50% (percentages indicate the equivalent of the height of a figure or face on the display monitor in relation to the height of the entire shot) in accordance with

applicable standards. A close-up shot of a face is not taken in any instance. Even the height of the cameras – min. 2 m above the floor – does not allow close-up shots of faces. The angle of view of the cameras is such that it does not allow the observation of details and/or body features which are not relevant to the designated purpose.

9. Data transfer between the cameras and the camera server is performed in the LAN data network on the premises of Masaryk University, Faculty of Economics and Administration. The data network architecture is classic, corresponding to ČSN EN series 50173. There is a dedicated segment in the data network, which is used only for the camera system, separate IP addresses are reserved for individual elements of the camera system. Physically, cabling is installed in ceilings or raised floors. The individual cables are in electrical installation pipes, on the surface or inside building structures.

10. Continuous image recording without sound recording is taken from all cameras. An image recording is stored on the camera server. The camera server settings do not allow keeping the recording longer than 12 days. Back-ups of the recordings are not made.

11. The camera server is located in the server room of the faculty, to which only a limited number of employees of the faculty and the Institute of Computer Science of Masaryk University have access. The server room is monitored by an alarm security and emergency system. In order to enter the room, it is necessary to perform an authenticated deactivation of the security system. If this is not done, an alarm sounds at the information facility of the camera system operator, whose staff in the event of an alarm follow their instructions for such a situation. The camera server itself is further monitored by other security elements of the faculty, so in case of HW or SW failure, the relevant employees of the operator in charge of technical supervision over the operation of the camera system are informed.

Section 5
Technical and organizational measures for securing the protection of personal data

1. The obligation of the camera system operator to take measures to prevent unauthorised or accidental access to personal data, their change, destruction or loss, unauthorised transfers, their other unauthorised processing, as well as other misuse of personal data is fulfilled in the form of restricted access (from personnel and technical point of view) to the camera system. This obligation applies even after the processing of personal data has ended. The faculty bursar decides on the allocation of the right of access to the camera system on the basis of an application specifying the reasons for access to the camera system.

2. Employees of the camera system operator, employees of the service organization or other persons who come into contact with personal and other data within the meaning of this Directive and protected by law are obliged to maintain confidentiality about personal data and security measures, the disclosure of which would endanger the security of personal data. The duty of confidentiality applies even after the termination of employment or relevant work. Each employee or a person who may come into contact with personal and other data within the meaning of this Directive and protected by law is obliged to sign a written non-disclosure declaration (see Annex 5). These declarations are archived in the personal files of employees in the personnel office of the camera system operator, or at the faculty bursar in the case of persons outside the faculty.

3. The camera system operator and individual employees authorised to access camera recordings or live footage from cameras (hereinafter referred to as “authorized persons”) are obliged to ensure compliance not only with the Act, but also with the provisions of Act No. 262/2006 Coll., the Labour Code, as amended, which prohibits covert and overt monitoring of employees in the workplace. They are also obliged to comply with all legal norms that guarantee individuals the right to privacy.

4. Authorised persons have access to the camera system only within the scope of their authorisation. The list of authorised persons, including a description of the level of their authorisation, is given in Annex No. 4. Authorised persons may not in any way take recordings of an image from cameras (with a camera, a camcorder, a mobile phone, a print screen or other means).

5. System administrators secure camera system settings and changes, camera definitions, data storage, server administration, and complete system programming. These people have complete access to data, including recordings. Each of them has their own user account for data management.

6. Persons with access to stored recordings with the right to read, copy, transfer, export or delete recordings may under no circumstances use the recordings for purposes other than for providing the recordings to authorised subjects upon their request. Every access to the recordings, its purpose and the person who gave an order to access the recordings is listed in the operation log of the camera system (a template in Annex 6).

7. The operation log is stored with the head of the operator's building management and, in their absence, with a person authorised by them. The operation log must not be lent to persons who have not signed a non-disclosure declaration within the meaning of this Directive. This obligation applies to all persons who manipulate in any way with the book. All decisive facts are recorded in the operation log (e.g. changes in the configuration of the camera system, service interventions, data on possible download or transmission of information, including specifications of when, to whom and for what purpose the information was transmitted, etc.). The authorised person who performs the download and transfer of records is responsible for making the recordings in the log. In the case of service interventions in the camera system, the head of the building management is responsible for the records in the operation log.

8. Live camera footage is not continuously monitored by any employee of the operator. To access the live image, it is necessary to log in with a username and a password. Information service employees have one shared password; the change of the password is performed irregularly, at least always when the staffing of the information service changes. Moreover, access for information service staff is limited to the IP address of the HW located in the information service.

9. Each entrance corridor from the outside of the faculty premises (monitored area) is labelled with an information notice board so that the data subject is notified of the camera system before entering the monitored area. The information notice board contains a pictogram of the camera, information that the area is monitored by a camera system with a recording, the identification of the operator of the camera system and a link to a place where more detailed information about the camera system can be obtained.

10. The maintenance of the camera system is carried out in accordance with the requirements of the standards applicable for this area. The operator of the camera system performs preventive service maintenance or eliminates individual current failures by its employees.

11. If it is necessary to expand the camera system, it is always necessary to ensure compliance with all legal regulations and standards applicable for this area. In particular, it is necessary to always ensure the protection of employees and students and their privacy so that it is not disproportionately invaded. System administrators are responsible for the assessment.

Section 6
Providing personal data from a camera system with recordings

1. Recordings made by the camera system may be transferred outside the camera system operator only as an official record to law enforcement authorities in the case of suspicion of committing a crime or misdemeanour or to the data subject based on their request in accordance with Sec. 12 of the Act.

2. Decision on providing the recordings is made by the faculty bursar. They assess the eligibility of the applicant, the justification of the request and/or the specification of the extent. In the case of a positive assessment of the request, they shall authorise the authorised person to search for the recording and to make a copy of the recording. The faculty bursar also decides on providing the recording to authorised subjects on the bursar's own initiative in the case of suspicion of committing a crime or misdemeanour. Every transfer of a recording must be recorded in the operation log. The actual transfer of the recording to the data subject must be documented by a record on the provision of personal data from the camera system (see Annex No. 7).

3. In return for the provision of a camera recording to the data subject, the camera system operator shall have the right to demand an appropriate fee not exceeding the costs necessary to provide the information. The data subject is informed by the faculty bursar, or a person authorised by them, on the reimbursement of costs including their expected amount. Subsequently, the total amount is communicated according to the actual cost and the data subject is obliged to pay this amount. A confirmation of the payment is issued (incoming cash receipt).

4. Any data subject who discovers or suspects that the camera system operator is carrying out the processing of their personal data contrary to the regulations on the protection of the data subject's private and personal life or contrary to the law, in particular if the personal data are inaccurate with regard to the purpose of their processing, can:
    a. ask the operator for an explanation,
    b. ask the operator to remedy the situation. In particular, this may involve blocking, correcting, supplementing or destruction of personal data.

5. If the data subject's request pursuant to the previous paragraph is found to be justified, the camera system operator shall immediately rectify the defective situation.

6. If the camera system operator does not comply with the data subject's request, the data subject has the right to contact the OPDP directly.

Section 7
Final Provisions

1. Other legal matters that are not regulated and contained in this Directive are governed by the Act, the relevant provisions of Act No. 262/2006 Coll., the Labour Code, as amended, and other generally binding legal regulations, including internal regulations of the faculty and Masaryk University.

2. I entrust the faculty bursar with the interpretation of individual provisions and the continuous updating of this Directive.

3. Compliance with this Directive is monitored by the faculty bursar and the head of the building management.

4. This Directive comes into force and effect on the date of its publication.

In Brno on 28th December 2021

prof. Mgr. Jiří Špalek, Ph.D.

Dean

electronically signed

Annexes

Annex No. 1 Statement of Approval of OPDP for the application of Sec. 5 para. 2 let. e) of the Act
Annex No. 2 The list of cameras, their specification, placement of individual elements of the system around the premises, angles of view and images from individual cameras
Annex No. 3 Floor plans with the location of the cameras
Annex No. 4 Employees with the right of access to the camera system
Annex No. 5 Non-disclosure declaration
Annex No. 6 Operation log of the camera system (template)
Annex No. 7 Record on the provision of personal data from the camera system