Directive of the Faculty of Informatics of Masaryk University No. 4/2017

Operation of the camera system

(as amended with effect from 20 November 2017)

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

Article 1
Subject of modification

(1) This Directive sets out the procedures for processing, storing and managing records taken by the camera system operated on the premises of the Faculty of Informatics of Masaryk University, Botanická 68a, 602 00 Brno, in accordance with Act No. 101/2000 Coll., on the Protection of Personal Data, as amended (hereinafter referred to as "the Act").

(2) Legal framework for the operation of the CCTV system:
   a) Act No. 101/2000 Coll. , on the protection of personal data, as amended,
   b) Act No. 262/2006 Coll. , Labour Code, as amended,
   c) Act No. 89/2012 Coll. , Civil Code, as amended,
   d) Opinion of the Office for Personal Data Protection No. 1/2006 - Operation of a camera system in terms of the Personal Data Protection Act,
   e) Statement and recommendation of the Office for Personal Data Protection on the possibility of installing a camera system in the school premises, 03/2007,
   f) Opinion of the Office for Personal Data Protection - Practical issues of operating CCTV systems in schools and education, 05/2007,
   g) Opinion of the Office for Personal Data Protection - Operation of CCTV systems, 2012,
   h) CSN EN 50173 Information Technology series, current edition,
   i) EN 50132 Alarm systems - CCTV, current edition,
   j) ČSN EN 62676 Surveillance video systems for use in security applications, new series of ČSN, until 2018 in parallel with the old series.

Article 2
List of terms and abbreviations

(1) For the purposes of this Directive:
   a) *any* information relating to an identified or identifiable data subject. A data subject shall be deemed to be identified or identifiable if the data subject can be identified, directly or indirectly, in particular by reference to a number, a code or one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity,
   b) *sensitive data shall include* personal data revealing the national, racial or ethnic origin, political opinions, trade union membership, religion or philosophical beliefs, criminal convictions, health or sex life of the data subject and genetic data of the data subject;

sensitive data shall also include biometric data which allow direct identification or authentication of the data subject,

c) *anonymous data is data which,* either in its original form or after processing, cannot be linked to an identified or identifiable data subject,

d) *the data subject* is the natural person to whom the personal data relate,

e) *processing of personal data means* any operation or set of operations which the controller or processor carries out systematically with personal data, whether by automated means or by other means; processing of personal data shall mean, in particular, collection, storage on a medium, disclosure, adaptation or alteration, retrieval, use, transmission, dissemination, disclosure, storage, exchange, classification or combination, blocking and destruction,

f) *collection of personal data* a systematic procedure or set of procedures designed to obtain personal data for the purpose of storing them on a storage medium for immediate or subsequent processing,

g) *storing personal data* by keeping the data in a form that allows it to be further processed,

h) *by blocking,* an operation or set of operations which restricts the manner or means of processing personal data for a specified period of time, except for necessary interventions,

i) *destruction of personal data* means the physical destruction of the medium, their physical erasure or their permanent exclusion from further processing,

j) *the controller is* any entity that determines the purpose and means of processing personal data, carries out the processing and is responsible for it; the controller may authorise or entrust the processor with the processing of personal data, unless a specific law provides otherwise,

k) *a processor is* any entity which, on the basis of a specific law or a mandate from the controller, processes personal data in accordance with the law,

l) *published personal data* personal data made available in particular by mass media, other public communication or as part of a public list,

m) *a record or dataset of personal data (hereinafter referred to as a 'dataset')* any set of personal data organised or made available according to common or specific criteria,

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

o) *the recipient shall be* any entity to which the personal data are disclosed; an entity which processes personal data pursuant to Article 3(6)(g) of the Act shall not be considered a recipient,

p) *authorised subject* means law enforcement authorities, administrative authorities for conducting offence proceedings, the data subject and his/her legal representative, the subject who has provided consent pursuant to Section 5 of the Act.

Article 3
Purpose of the camera system

(1) The purpose of the installation of the camera system is to protect property and safety of persons, prevention of damage, vandalism and crime committed on the property of the operator of the camera system and data subjects moving in the Botanická 68a area, as well as to increase the level of prevention of unauthorized interference in technological equipment, such as machinery of technical security infrastructure of the faculty (server rooms, LV substations, SLP substations, etc.). The operator of the CCTV system decided to install it after having exhausted all possibilities

of prevention, avoidance and monitoring of incidents, including, for example, subject protection of technology.

(2) The camera system has a preventive function and is aimed at protecting the legitimate interests of the operator within the meaning of Section 5(2)(e) of the Act. For this purpose, the operator of the CCTV system may make CCTV recordings without the consent of persons entering the recorded area, including employees, students, persons entering the premises on a short-term or irregular basis, as well as persons moving in the publicly accessible outdoor area around the premises - see the opinion of the Office for Personal Data Protection (hereinafter referred to as the "Office for Personal Data Protection") in Annex 1.

(3) The camera system is not used for systematic surveillance of persons. The fixed setting of the camera lenses is such that the height of the figure is no more than 50% of the height of the entire camera frame. Close-ups of persons are not displayed, so there is no violation of the right to privacy under Section 86 of Act No. 89/2012 Coll., the Civil Code.

(4) The CCTV system is installed in such a way as to avoid any invasion of the privacy of employees and students in accordance with Section 316(2) of Act No. 262/2006 Coll., the Labour Code, as amended. This is achieved, for example, by ensuring that only entrances, exits, car parks, technically important areas or areas with equipment of high purchase value are monitored.

Article 4
Identification of the camera system and its description

(1) Identification (location) of the camera system: **CCTV system in the area of Botanická 68a, Brno**

(2) Entry in the register of personal data processing, registration with the OOOÚ: 00000727/031

(3) Operator and administrator of the camera system: the Faculty of Informatics of Masaryk University,
Botanická 68a, 602 00 Brno, ID: 00216224
(hereinafter also referred to as "Faculty")

(4) Data Controller: Masaryk University, Žerotínovo nám. 9,
601 77 Brno, ID: 00216224

(5) Contact details for receiving requests and complaints: Faculty of Informatics of Masaryk University,
Botanická 68a, 602 00 Brno, ID: 00216224

(6) Service organizations: ASEC - elektrosystémy s.r.o., Pražákova 52,
619 00 Brno, ID No.: 26277930

(7) The list of cameras, their specifications, the location of individual elements of the system within the premises, the viewing angles and images from individual cameras are given in Annex 2.

(8) The cameras are placed out of the normal range of people moving in the monitored area. In all cases they are day/night switched digital IP cameras. The installed cameras are not in antivandal-proof enclosures, some of the cameras used outdoors (facades of individual buildings) are installed in outdoor weather-conditioned enclosures. All cameras are video recorded. No sound is captured or recorded from any of the cameras, so no sensitive personal data is processed (see the opinion of the ÚOOÚ in Annex 1).

(9) Fixed camera shots - fields of view - are set to provide a maximum of 25% "observation" or 50% "reconnaissance" (the percentages indicate the equivalent size of the figure or face on the display monitor in relation to the height of the entire frame) in accordance with the applicable standards. In no case is a close-up of the face taken. Even the height of the cameras - at least 2 m above the floor - does not allow for close-ups of faces. The angle of view of the cameras shall be such as not to allow observation of details and/or bodily features which are not relevant for the purpose.

(10) The data transmission between the cameras and the camera server is implemented in the FI MU LAN data network. The architecture of the data network is classical, corresponding to ČSN EN 50173 series. 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. At the physical level, the cabling is installed in the ceilings or in the double floors. Individual cables are routed in conduits, on the surface or inside building structures.

(11) Continuous video recording without sound recording is made from all cameras, the video recording is stored on the camera server. The settings of the camera server do not allow the recordings to be stored for more than 7 days. Backup of the recording is not performed.

(12) The camera server is located in a locked data cabinet in the FI data centre in Building A, to which a limited number of FI employees have access. The data centre area is monitored by an alarm and emergency system; to enter the data centre, the security system must be authentically deactivated. Otherwise, an alarm is raised at the reception desk of the CCTV system operator, whose staff follow the instructions for this situation in the event of an alarm. The camera server itself is further monitored by other FI security elements, so that in the event of a HW or SW failure, the relevant staff of the operator in charge of technical supervision of the operation of the camera system are informed.

Article 5
Technical and organisational measures to ensure the protection of personal data

(1) The obligation of the operator of the CCTV system to take such measures to prevent unauthorised or accidental access to personal data, their alteration, destruction or loss, unauthorised transmissions, other unauthorised processing, as well as other misuse of personal data is fulfilled in the form of restricted access (both in terms of personnel and technical) to the CCTV system. This obligation shall continue to apply even after the processing of personal data has ceased. The granting of the right of access to the CCTV system is decided by the Secretary of the Faculty on the basis of a request specifying the reasons for access to the CCTV system.

(2) Employees of the operator of the camera system, employees of the service organization, or other persons coming into contact with personal and other data protected by law within the meaning of this Directive are obliged to maintain confidentiality of personal data and security measures, the disclosure of which would jeopardize the security of personal data. The obligation of confidentiality shall continue after the end of employment or relevant work. Every employee or person who may come into contact with personal and other data protected by law within the meaning of this Directive is required to sign a written declaration of confidentiality (see Annex 5). These declarations are archived in the personnel files of the employees at the personnel department of the CCTV system operator, or at the Faculty Secretary in the case of persons outside FI.

(3) The operator of the CCTV system and individual employees authorised to access the CCTV footage or live footage from the cameras (hereinafter referred to as "authorised persons") are obliged to comply not only with the law, but also with the provisions of Act No. 262/2006 Coll., the Labour Code, as amended, which prohibits both covert and overt surveillance of employees in the

workplace. Likewise, they are obliged to comply with all legal norms that guarantee an individual's right to privacy.

(4) Authorised persons have access to the CCTV system only within the scope of their authorisation. A list of authorised persons, including a description of their level of authorisation, is given in Annex 4. Authorised persons shall not make any visual recordings of images from the cameras (by camera, camera, mobile phone, printscreen or any other means).

(5) System administrators provide settings and changes to the camera system, camera definitions, data storage, server administration and complete system programming. These persons have complete access to the data, including recordings. For data management, each of them has their own user account.

(6) Persons with access to stored records with the right to read, copy, transfer, export or delete the records shall not, under any circumstances, use the records for any purpose other than to provide the record to authorized entities upon request. Any access to the recordings, the purpose of the access and the person who instructed the access shall be recorded in the CCTV operating log (see Annex 6 for a specimen).

(7) The operating log is kept by the head of the building management of the operator and in his absence by a person authorised by him. The logbook shall not be lent to persons who have not signed a declaration of confidentiality within the meaning of this Directive. This obligation shall apply to all persons carrying out any handling of the register. All relevant facts (e.g. changes in the configuration of the camera system, service interventions, details of any downloading or transfer of information, including a specification of when, to whom and for what purpose the information was transferred, etc.) shall be recorded in the logbook. The authorised person who downloads and transfers the records shall be responsible for the recording. In the case of service interventions on the CCTV system, the head of building management is responsible for the entry in the operating log.

(8) The live footage from the cameras is not continuously monitored by any employee of the operator. To access the live feed, a login with a username and password is required. Reception staff share a single password, and passwords are changed irregularly, at least whenever the reception staff changes. In addition, access for reception staff is limited to the IP address of the HW located at the reception desk.

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

(10) Maintenance of the CCTV system is carried out in accordance with the requirements of the standards applicable in this area. The operator of the CCTV system has a service contract for preventive maintenance or for the removal of individual current faults on the basis of a call from the CCTV system operator. The service organisation is obliged to comply with all legal regulations and standards applicable to this area, as well as to maintain confidentiality of personal data and security measures, the disclosure of which would compromise the security of personal data.

(11) In the event of the need to expand the CCTV system, it is always necessary to ensure compliance with all legal regulations and standards applicable in this area, in particular, it is always necessary to protect employees and students and their privacy so that it is not unduly interfered with. System administrators are responsible for the assessment.

Article 7

Provision of personal data from CCTV footage

(1) The recordings made by the CCTV system may be handed over outside the CCTV system operator only on a protocol basis, to the law enforcement authorities and administrative authorities for the conduct of misdemeanour proceedings in the event of suspicion of a criminal offence or misdemeanour, or to the data subject on the basis of his/her request in accordance with the provisions of Section 12 of the Act.

(2) The decision to provide the record is issued by the Secretary of the Faculty. He/she shall consider the eligibility of the applicant, the justification for the request, and the specification of the scope. In the event of a positive assessment of the request, he/she shall authorise the authorised person to search for the record and make a copy of the record. The Secretary of the Faculty shall also decide to provide the record to authorised bodies on his/her own initiative in the event of suspicion of a crime or offence. A record must be made in the operational log of each transfer of footage, and the actual transfer of footage to the data subject must be documented by a protocol on the provision of personal data from the CCTV system (see Annex 7).

(3) The operator of the CCTV system has the right to request a reasonable fee for the provision of the CCTV footage to the data subject, not exceeding the costs necessary to provide the information. The Secretary of the Faculty, or a person authorised by him/her, shall inform the data subject of any request for reimbursement of costs, including the estimated amount, prior to their provision. The total amount is then communicated as appropriate and the data subject is obliged to pay this amount. A confirmation of the payment is issued (cash receipt).

(4) Any data subject who becomes aware or believes that the operator of a CCTV system is processing his or her personal data in a way that is contrary to 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, may:

a) ask the operator for an explanation,

b) require the operator to remedy the situation. In particular, this may involve blocking, correcting, supplementing or destroying personal data.

(5) If the data subject's request pursuant to the preceding paragraph is found to be justified, the CCTV system operator shall remedy the defective condition without delay.

(6) If the operator of the CCTV system does not comply with the data subject's request, the data subject has the right to apply directly to the ORO.

Article 8

Final provisions

(1) Other legal issues that are not regulated and contained in these regulations 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 the internal regulations of the Faculty and Masaryk University.

(2) I entrust the interpretation of individual provisions and the continuous updating of this Directive to the Secretary of the Faculty.

(3) The Faculty Secretary and the Building Administrator shall monitor compliance with this policy.

(4) This Directive shall enter into force and effect on the date of its publication.

Brno, 20 November 2017

Jiri Zlatuska
Dean FI

Attachments:

Annex No. 1Consensus statement of the OOOO on the application of Section 5(2)(e) of the Act
Annex No. 2List of cameras, their specifications, location of individual elements of the system within the premises, viewing angles and images from individual cameras
Annex No. 3Plans showing the location of cameras
Annex 4Workers with access rights to the CCTV system
Annex 5Declaration of confidentiality
Annex 6Camera system operation log (model)
Annex 7Protocol on the provision of personal data from the CCTV system
Annex No. 8Registration of the camera system
Annex No. 9Declaration of the contractor ASEC-elektrosystémy s.r.o.