

Charles University, Faculty of Medicine in Hradec Králové

Dean's measure No 10/2019

Title: **The Operation of the Camera System at the Faculty of Medicine in Hradec Králové and the Protection and Processing of Personal Data during Camera System Operation**

Validity and effectiveness: on the date of the Dean's signature

**Article 1
Initial Provisions**

This Dean's measure lays down the conditions and rules for the operation of the camera system at buildings and premises of Charles University, Faculty of Medicine in Hradec Králové (hereinafter 'the Faculty'), the processing of personal data obtained during the operation of the camera system and the measures to protect them in accordance with generally applicable legislation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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, Act No. 110/2019 on the processing of personal data and national rules relating thereto (hereinafter 'the Regulation' or 'the Legislation'), Act No. 89/2012 Coll., Civil Code, as amended (hereinafter 'the Civil Code'), Act No. 262/2006 Coll., Labour Code, as amended (hereinafter 'the Labour Code'), and the Internal Regulations of Charles University and the Faculty.

**Article 2
Scope**

This Measure is binding to all staff members of the Faculty and persons in a similar relation to the Faculty to the extent of their duties, job classification and work content, and affects all staff and students at the Faculty and other persons entering the monitored premises of the Faculty.

**Article 3
Purpose of the Operation of the Camera System and Legal Grounds for Personal Data Processing**

1. The purpose of the operating of the camera system is to protect the buildings and property of the Faculty, the property of employees, students and others from damage, destruction and theft, and the safety, protection and health of employees, students and others. These include the preventive protection of buildings (buildings partly listed), intellectual property, facilities and high-value equipment of science and teaching departments and the protection of fundamental personal rights, which is a legitimate interest of the Faculty and other persons. With regard to the importance of the subject-matter of protection, the legitimate interests, the financial and organizational complexity of protection, the protection cannot be otherwise adequately ensured in the given extent.

2. The processing of personal data during the operation of the camera system is necessary for the legitimate interests of the Faculty and other persons, and is therefore, in accordance with the provisions of Article 6(1)(f) of the Regulation, legitimate, not subject to the consent of the data subject and is conducted with respect to minimizing the intervention of the chosen solution in the legitimate interests of the data subjects.

Article 4

The Camera System Operator and the Personal Data Controller

1. The operator of the camera system and the controller of personal data obtained from the operation of the camera system is Charles University, Faculty of Medicine in Hradec Králové (Operator, Faculty) and as such complies with the legal obligations of the data controller.
2. The person who is entrusted by the Faculty to carry out the operation of the camera system and to manage and process personal data obtained from the operation of the camera system is the Head of the Operational and Technical Department (hereinafter ‘the PTO’) of the Faculty (hereinafter also ‘the Head of the Authorized Employees’) who shall, during the performance of that role, directly report to the Secretary and Dean of the Faculty.
3. The person responsible for the processing and protection of personal data and the protection of the rights of the data subjects on behalf of the operator is the Dean.

Article 5

Camera System

1. The camera system is an automatically operated permanent technical system, allowing the capture and storing of visual records of the monitored area.
2. The camera system is operated at these Faculty premises:
 - a. Building at Šimkova 870, Hradec Králové,
 - b. Educational Centre (EC) building at the campus of the University Hospital Hradec Králové, Sokolská 581, Hradec Králové,
 - c. Teaching and Research Centre (VaVC) building, Zborovská 2089, Hradec Králové,
 - d. Building at Na Hradě 91, Hradec Králové.
3. The camera system operates continuously 24 hours a day, including Saturdays, Sundays and public holidays, with continuous video recording during camera operation.
4. Number identifiers of cameras, specific camera locations (building, space), monitoring area range, data transmission method, operating time, camera data processing control centres, data logging information, and data storage from the camera system (server room) are listed in Appendix 1 *Camera System Specifications*.
5. The camera system monitors specifically defined interior and exterior areas of the Faculty buildings with data transmission, virtually separate from the conventional network (network of camera system), cable routes to displaying and recording facilities at control centres and repositories (servers in server rooms).

6. From the control centres (Article 5(7)(a)), authorized employees shall manage the operation and control the functions of the camera system and the systems downstream and evaluate the data from the camera system using established processes and maintain operating books.
7. The control centres are:
 - a. the information desk and reception of the Faculty buildings,
 - b. the technical control room of the VaVC building,
 - c. other recording storage locations (server rooms).
8. The authorized employees shall be:
 - a. Head of the Authorized Employees
 - Head of the Operational and Technical Department (PTO) of the Faculty (see Article 4).
 - b. Management of the Authorized Employees
 - Deputy Head of the PTO,
 - Head of the Computer Technology Centre (OVT) of the Faculty and the Deputy,
 - administrators of the Faculty buildings and their deputies.
 - c. Authorized employees
 - employees at control centres (information desks),
 - OVT technicians with access to the control centres and camera system elements.

Article 6

Operation of the Camera System and Processing of Personal Data

1. By the operation of the camera system for the stated purpose, the operator acquires and processes personal data. The source of personal data is the video recording from the camera system, without audio recording. Personal data obtained from the operation of the camera system may only be processed for the purpose of the operation of the camera system.
2. Authorized employees at control centres (Article 5(7)(a))
 - a. perform random or continuous monitoring of monitored areas on imaging devices through the camera system, and evaluate current recorded events from the camera system,
 - b. operate the relevant part of the camera system, check the functionality of the camera system and the camera system recording mode,
 - c. exercise surveillance of objects, ensure protection of the camera system, data acquired and stored, and of the control centre against unauthorized persons entering and tampering, and data leaks and disruption of protection measures,
 - d. if a camera system recording, report, or other fact exhibits a harmful event (natural element, force majeure) or a malfunctioning event (intrusion or threat to premises, persons or property), a malfunction of the camera system, or the occurrence of a security incident (threat to, breach of or loss of personal data, or threat to or breach of protection measures), they shall notify of it without delay (depending on the nature of the breach) the authorities of the Police of the Czech Republic, the Fire Rescue Service and the nearest available competent supervisor of the authorized employees at the section, in the following order: the Building Manager (Deputy), the Head of the PTO (Deputy), the Secretary, the Dean,
 - e. to the extent possible, shall, without delay, take measures to remedy defects in the camera system, to prevent, remedy or eliminate harmful or malfunctioning event or

- security incident, prevent their continuation and occurrence of harmful consequences,
- f. shall make specific entries in the operating book.
3. The Head of the Authorized Employees and the Manager of the Authorized Employees in their areas of responsibility
 - a. manage their reports, instruct them about their activities and perform continuous, periodic and random checks on the performance of their roles and the operation of the camera system and camera system recording mode,
 - b. shall, without delay, take measures to remedy defects in the camera system, to prevent, remedy or eliminate a harmful or malfunctioning event or security incident, prevent their continuation and the occurrence of harmful consequences (or to ensure that they are rectified) and shall immediately notify the supervisor of the event,
 - c. when a harmful or malfunctioning event is reported or offense or criminal offense is suspected, ensure or, within the scope of their access authorizations, store the relevant documenting part of the camera system recording on the special storage or medium and report this fact to the supervisor,
 - d. carry out checks on the keeping of operating books and records and carry out specific entries in operating books.
 4. Authorized employees (OVT technicians with access to control centres, storage and camera system elements)
 - a. ensure and control the operation, functionality and security of the computer network, the transmission of data and the recording mode of the camera system and record-storing equipment, in particular, supervise the backup battery pack and provide active cooperation during system operation, maintenance, change of configuration or resolving of system crashes,
 - b. if a fault or other abnormal system behaviour is detected, or a security incident occurs, they shall immediately report this fact to the appropriate supervisor of the authorized employee at the section, in the following order of the Head of the OVT (Deputy), Head of the PTO (Deputy), the Secretary, the Dean,
 - c. to the extent possible, they shall without delay take measures to remedy a security incident, malfunction of the camera system or safety measures and to prevent their continuation and harmful consequences,
 - d. shall make specific entries in the operating book.
 5. The Head of the PTO shall report the occurrence of a harmful or malfunctioning event or suspected offense or criminal offense to the Secretary and the Dean in order for them to decide on the next step to be taken. The Head of the PTO shall immediately notify the Secretary and the Dean of the occurrence of the security incident in order for them to decide on the next procedure and, at their direction, they shall also notify the Data Protection Officer of the Charles University.
 6. The storage, transfer and disposal of recordings from the camera system (personal data) shall be carried out in accordance with Article 8.

7. Control centres shall administer operating books for the part of the camera system being operated. The relevant authorized employees shall record in the operating book, as appropriate, all facts relating to the operation of the camera system, including, but not limited to, malfunctions, repairs, inspections and changes to camera system settings, the occurrence of harmful or malfunctioning events and incidents, the export, saving and transfer of recordings from the camera system.
8. A readily visible, legible A4 size information table (Annex 2, *Information Table and Pictogram*) is displayed in every monitoring area with a camera pictogram and a warning that the space is monitored by a recording camera system and with information to data subjects.

Article 7

Technical and Organizational Measures to Protect Personal Data

1. The operation of the camera system, the processing and security of the personal data obtained from the operation of the camera system is the responsibility of the Head of the PTO.
2. Only authorized employees can access the control centres, camera system elements, recordings and data from the camera system, as well as the Dean, Secretary, Data Protection Officer of Charles University and persons accompanying them or designated by them.
3. Authorized employees must, before carrying out the duties of authorized employees, undergo an initial and, in the event of substantial changes to the legislation or camera system, further training, which consists of a legal part – legislation on the protection and processing of personal data – and a technical part – operation of the camera system, technical procedures for personal data processing and security measures to protect them. The training is organized by the Head of the PTO through their own Faculty instructors or external instructors. The Head of the PTO shall immediately inform the authorized employees of any changes to the legislation, operation or settings of the camera system and the processing of personal data. Authorized employees are, as part of their employment relationship or by other means, under the obligation of confidentiality.
4. Authorized employees shall, to the extent of their duties:
 - a. participate in mandatory trainings,
 - b. use the camera system only for the purpose for which it is intended and in accordance with this Dean's Measure, the general legislation in force and the operator's internal rules,
 - c. not make, leak or distribute recordings from the camera system or copies thereof and ensure that they are erased in a timely manner,
 - d. ensure the functionality of the camera system and recording mode, and properly evaluate the recordings made,
 - e. protect the camera system and the control centre from tampering and entry by unauthorized persons, and prevent data leakage from the camera system and compromise of the protection measures,
 - f. promptly report any identified incident, harmful or malfunctioning event, camera system defect, or security incident to their supervisor and take action to resolve and remove it themselves or as directed by a supervising authorized employee (e.g., service desk, help desk request),

- g. in the event of a detection or reporting of a harmful or malfunctioning event, a suspected offense or criminal offense, ensure that, within the scope of their access authorizations, the network of the camera system stores the relevant documentation part of the record on a special repository or on a medium, securely stored at the control centre,
 - h. protect personal data obtained from the camera system from leakage and unauthorized use, and observe safety measures to protect them,
 - i. maintain the confidentiality of the personal data processed and the security measures taken to protect them, even after the end of the role as an authorized employee or employment relationship with the camera system operator,
 - j. ensure that the system allows for the identification of personal data use, processing and security measures for their protection at any time,
 - k. make entries in the operating book.
5. Buildings that are the locations of the camera system are secured by lockable entries, an electronic security system and surveillance by the personnel of information desks and receptions. The control centres (information desks and receptions at buildings) are secured by entries from the interior of buildings, the supervision of the door guards, as well as the technical and operational capabilities of the various control centres by electronic security means, locks and key modes.
 6. The cameras are protected by positioning them out of the normal reach of persons, by cover and by the supervision of the authorized employees.
 7. The protection of the transmission routes is ensured by placing the network cables of the camera system under plaster, in skirting boards, in protectors/tubes, or in grooves. Ends are located in lockable cabinets.
 8. Recordings from the camera system are stored on servers at the recording storage locations (server rooms). The storage of recordings from the camera system is protected by their location in rooms with electronic security and restricted, conditional access by persons authorized by the OVT. Every network and all equipment of the camera system for recording, transmitting, displaying and storing of recordings from the camera system and data from the camera system shall be protected against unauthorized use, leakage or disposal of recordings and data by the means of restricted, conditional access of authorized persons to the camera system network under access-level passwords and other hardware and software resources of the Faculty (firewalls, network security configurations, etc.). Access to data, camera images, or camera system recordings is only possible from computers located on the network of the camera system, in control centre buildings of the Faculty. Only authorized employees can log on to computers on the camera system network using their valid credentials. The camera system interfaces have access levels for authorized employees for:
 - live stream monitoring without access to recordings,
 - access to recordings with an option of export to external storage and deletion of records,
 - management and configuration of the system.

Article 8
The Retention and Transfer of Personal Data

1. The recording from the camera system shall be retained for the purpose of evaluation for 5 calendar days. If not reported or if the recording does not show a harmful or malfunctioning event, suspected offense or criminal offense, the recording shall be irreversibly deleted from all media and storage facilities after the evaluation, at the latest within 5 calendar days of its acquisition (by automated erasure by a new recording).
2. In the event of capturing of a harmful or malfunctioning event or a suspected offense or criminal offense, the relevant documenting part of the recording from the camera system shall be stored for as long as is strictly necessary to resolve the recorded event.
3. After the end of the required storage period of the camera system recording, the recording must be discarded without delay, irreversibly deleted from all operator's media and storage facilities.
4. Recordings from the camera system may only be played and transferred in justified cases when a harmful or malfunctioning event or suspected offense or criminal offense has been committed, for the purpose of resolving the recorded event, and only to law enforcement authorities, administrative authorities or other duly authorized bodies (e.g. insurance company) for fulfilling the purpose of the operation of the camera system.
5. The recordings from the camera system shall be transmitted in such cases upon written and reasoned request from the authorized body, on the basis of the Protocol for Transfer of Camera System Recoding (Annex No. 3 *Protocol for Transfer of Camera System Recoding*). Part of the Protocol for Transfer of the Recoding is the obligation of the receiving party to use and process the personal data on the recording only for the purpose for which it was transferred and irreversibly dispose of the recording immediately after the purpose of its use and processing has ceased, except for legal obligations (archiving, etc.). Playing and transferring of the recording from the camera system is decided by the Dean.

Article 9
Information to Personal Data Subjects, Notice

1. The camera system is operated in accordance with Article 316 of the Labour Code and the relevant provisions of the Civil Code for the protection of personality and other generally applicable data protection legislation.
2. The camera system does not monitor individual workplace premises and the premises used for private activities. Monitoring shall be performed in such a way that the right to the protection of private and personal life and the protection of the rights of data subjects against their breach is respected to the maximum extent while fulfilling the purpose of the operation of the camera system. The operation of the camera system results in a simple video recording without the use of means for comparing biometric characteristics and without audio recording.
3. Subjects of the personal data acquired and processed during the operation of the camera system are employees and students at the Faculty and other persons entering the monitored

buildings and premises. Personal data collected and processed during camera system operation are sensitive personal data.

4. The information tables in the monitored areas shall inform the operator's employees and other personal data subjects of the operation of the camera system and of the monitoring of the space, of the camera system operator and of the controllers of personal data obtained from its operation, of the person responsible for the operation of the camera system and of the performance of the management of personal data obtained from its operation, and of publicly available sources of information and notice to personal data subjects.
5. This Dean's measure on the camera system operation and information on the processing of personal data, on the rights of data subjects and on the possibilities for their application and on the right to lodge a complaint with the supervisory authority and the contact details of the Data Protection Officer of the Charles University are publicly available on the website of Charles University, Faculty of Medicine in Hradec Králové, www.lfhk.cuni.cz. Additional information is provided by the responsible person in charge of the implementation and performance of the administration of the camera system – Head of the PTO Department of the Faculty (Head of the Authorized Employees).

Article 10

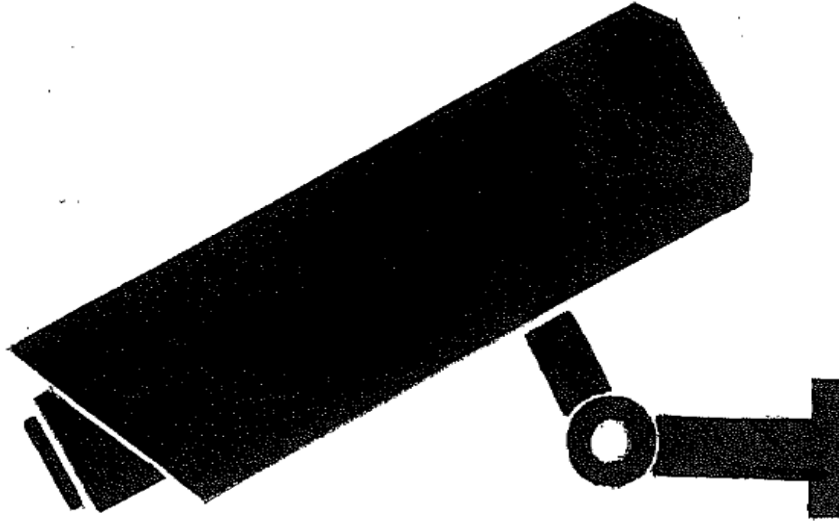
Final Provisions

1. This Dean's measure and Annexes 2 and 3 are public. Annex 1 is non-public and is deposited with the Secretary of the Faculty and with the Head of the PTO (Head of the Authorized Employees).
2. With regard to the importance of protected interests, a breach of the employee's obligations under this Dean's measure will be considered as a serious breach of the employee's obligations under the legislation applicable to the work performed or breach of the employee's obligations under the legislation applicable to the work performed in a particularly gross manner.
3. In other cases, the rights and obligations of the persons concerned are governed by the relevant generally applicable laws of the Czech Republic, in particular Act No. 89/2012 Coll., the Civil Code, as amended, Act No. 262/2006 Coll., Labour Code, as amended, Act No. 40/2009 Coll., Criminal Code, as amended, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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, Act No 110/2019 Coll., on the processing of personal data and national rules subsequent to it and internal rules of the Charles University and the Faculty.

Annexes: No. 1 Camera System Specifications
No. 2 Information Table and Pictogram
No. 3 Protocol for Transfer of Camera System Recoding

In Hradec Králové on 20th August 2019

prof. MUDr. Jiří Mandřák, Ph.D.
Dean of the Faculty



THIS SPACE IS MONITORED BY A RECORDING CAMERA SYSTEM

The operator of the camera system, the controller and the processor of personal data obtained from the operation of the camera system is Charles University, Faculty of Medicine in Hradec Králové, Šimkova 870, Hradec Králové.

The person in charge of the camera system operation, the management and processing of personal data obtained from the operation of the camera system and the provision of information to the data subjects to which they are entitled is the Head of the Operational and Technical Department of the operator, telephone: , email:

Dean's measure No. 10/2019 The Operation of the Camera System at the Faculty of Medicine in Hradec Králové and the Protection and Processing of Personal Data during Camera System Operation, information and notices on the rights of data subjects and the possibilities of their application and contact details of the Data Protection Officer of Charles University are publicly available on the website of Charles University, Faculty of Medicine in Hradec Králové, at www.lfhk.cuni.cz.



UNIVERZITA KARLOVA
Lékařská fakulta
v Hradci Králové

Charles University, Faculty of Medicine in Hradec Králové

PROTOCOL FOR TRANSFER OF CAMERA SYSTEM RECORDING

I request the transfer of a camera system recording for the purpose of use and processing for:

.....

In Hradec Králové on

.....
 Applicant (Authority/Body, First Name, Last Name, Role, Personal Number, Signature)

On the basis of the application submitted, I hereby transfer to the applicant the visual recording of a space from the LFHK camera system recorded on in the time range on the medium for the purposes set out in the application.

The receiving party is aware of its legal obligations during the processing of personal data on the recording. The receiving party undertakes to use and process the personal data on the recording only for the purpose for which it was transferred and irreversibly dispose of the recording (including all copies) immediately after the purpose of its use and processing has ceased, except for legal obligations (archiving, etc.).

Transferred in Hradec Králové on

Transferred, on the behalf of the LFHK, by:

.....
 (Function, First Name, Last Name, Signature)

Received by:

.....
 (Authority/Entity, First Name, Surname, Role, Personal Number, Signature)