DEBRECENI EGYETEM

CHANCELLOR'S ORDER

ON THE OPERATION OF VIDEO SURVEILLANCE SYSTEM

IN THE TERRITORY OF THE UNIVERSITY OF DEBRECEN

Entry into force: 01 May 2023

Contents

CHAPTER I *3*
PURPOSE AND SCOPE OF THE ORDER, BASIC DEFINITIONS *3*
Purpose of the Order *3*
Material scope of the Order *3*
Personal scope of this Order *3*
Definitions *4*
CHAPTER II *4*
FUNDAMENTAL REQUIREMENTS OF THE LAWFULNESS OF DATA PROCESSING *4*
Purpose of the operation of the camera surveillance system *4*
Legal basis of the operation of the camera surveillance system *5*
Duration of the storage of the records *5*
Scope of people having access to the records *5*
Procedure of the review and the use of records *6*
CHAPTER III *8*
RIGTHS OF DATA SUBJECTS AND THEIR EXERCISE OF SUCH RIGHTS *8*
Obligation to inform in advance *8*
Rights of data subjects regarding data processing *8*
Procedure based on the exercising of rights of the data subject *9*
CHAPTER IV *9*
FURTHER OBLIGATIONS REGARDING DATA PROCESSING *9*
Information technology and organisational security measures *9*
Data protection impact assessment *10*
Management and reporting of personal data breaches *11*
Use of a processor *11*
CHAPTER V *12*
MISCELLANEOUS *12*
Annex 1 ..... *13*
Annex 2 ..... *15*
Annex 3 ..... *16*
Annex 4 ..... *17*

In order to operate the camera surveillance system in the real estates owned and used with any legal title[1] by the University of Debrecen in a legal, fair and transparent manner for the data subjects, the Chancellor of the University of Debrecen issues the following order on the basis of the 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 (hereinafter referred to as GDPR), the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information, the Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators and other legal regulations:

CHAPTER I

PURPOSE AND SCOPE OF THE ORDER, BASIC DEFINITIONS

Purpose of the Order[2]

Section 1

(1) The purpose of the Order is to ensure that data processing during the use of the camera surveillance systems located in the territory of real estates owned and used with any legal title by the University of Debrecen (hereinafter referred to as University) is in compliance with related legal regulations and data protection requirements.

Material scope of the Order[3]

Section 2

(1) The scope of this Order shall cover:

a) the camera surveillance systems operated in the real estates determined in the paragraph (1) of the section 1 hereof (i.e. in the territory of the real estate, installed on or inside the buildings),

b) any camera surveillance system installed by the University after the acceptance hereof.

Personal scope of this Order

Section 3

(1) The personal scope of this Order shall cover every natural person entering the area monitored by camera surveillance system.

(2) The regulations hereof shall be applied by

a) anyone having access to camera surveillance system based on their job description or contractual obligation,

[1] Amended: on 01 May 2023

[2] Amended: on 01 May 2023

[3] Amended: on 01 May 2023

b) anyone instructed by the person exercising employer's rights (employer's instruction) to proceed as described herein,

c) anyone subject to any regulations hereof.

Definitions[4]

Section 4

(1) Except paragraphs (2)-(7) hereunder, the definitions herein shall be governed by the related regulations of the Internal Privacy Policy accepted by the decision no. 21/2022 (28 April) of the Senate of the University of Debrecen on 28 April 2022 (hereinafter referred to as Internal Privacy Policy).

(2) **Data subject**: any natural person entering the area monitored by camera surveillance system.

(3) **Personal data**: image of the data subject, his/her act seen in the camera record and his/her other personal data seen in the camera record, such as his/her clothing and external characteristics.

(4) **Employee**: a person employed by the University (employee, public servant or a person having a relationship with the aim of providing work or services).

(5) **University citizen**: employee or student of the University or a person taking part without student status in a training organised by any organisational unit of the University.

(6) **Access to records**: inspection or review of the records of the camera surveillance system, saving these records to external data carrier, forwarding these records, any IT operation performed with the stored records and physical access right to the servers storing these records.

(7) **Assets**:

a) any movable property owned or exclusively used by the University based on any legal regulation or agreement - independently of the value thereof -, such as vehicles, equipment, devices, working materials;

b) any movable property owned or used by the data subject - independently of the value thereof - such as vehicle or other means of traffic, bag, wallet, IT device, clothes, key to a flat.

CHAPTER II

FUNDAMENTAL REQUIREMENTS OF THE LAWFULNESS OF DATA PROCESSING

Purpose of the operation of the camera surveillance system

Section 5

(1) Purpose of the operation of the camera surveillance system:

[4]Amended: on 01 May 2023

a) protection of the assets of the University, the prevention of the related violations of law and the support of the proving thereof,

b) protection of the buildings on the real estates owned by the University and the natural environment, the prevention of the related violations of law and the support of the proving thereof,

c) protection of the assets of the data subjects, the prevention of the related violations of law and the support of the proving thereof,

d) clarification of the circumstances of accidents, work accidents or damage events in the area monitored by the camera surveillance system and the support of the proving thereof,

e) clarification of the circumstances of the acts committed by the university citizens and violating the regulations of the Code of Ethics accepted by the decision no. 16/2007 (15 November) brought by the Senate of the University of Debrecen on 15 November 2007 and the support of the proving thereof,

f) clarification of the circumstances of any acts committed by the employee and violating law based on which the University may impose an adverse legal consequence on the employee, and the support of the proving thereof.

(2) If the University intends to use the records of the camera surveillance system for a purpose other than described in the paragraph (1) hereof, it shall be qualified as a new data processing, and the University shall proceed according to the related regulations of the Internal Privacy Policy.

Legal basis of the operation of the camera surveillance system

Section 6

(1) The legal basis of the operation of the camera surveillance system shall be the legitimate interest of the University [item f) of the paragraph (1) of the article 6 of the GDPR].

(2) The interest assessment test necessary for the application of the legal basis of legitimate interest shall be performed according to the related regulations of the Internal Privacy Policy.

Duration of the storage of the records[5]

Section 7

(1) The University stores the record for 10 days. Afterwards, the IT system automatically, irrevocably and permanently erases the record by overwriting.

Scope of people having access to the records[6]

Section 8

[5]Amended 01 April 2021

[6]Amended: on 01 May 2023

(1) The review and the saving of the records of the camera surveillance system can be ordered by the Chancellor, the data protection officer, the security director general and the deputy security director general. Requests shall be submitted to the data protection officer to the e-mail address adatvedelmi.tisztviselo@unideb.hu who shall, together with his/her point of view, notify the deputy security director general of the request received.

(2) The people determined in the paragraph (1) above may be present during the review of the records, and in justified cases, they may watch the records even later. Furthermore, based on the paragraph (2) of the section 9 hereof, the people determined in the paragraph (1) above may order the presence of the following people during the review or during the later inspection of the records in justified cases:

a) the legal representative of the University,

b) the Information Security Officer (ISO) of the University,

c) the head or the representative of the affected organisational unit,

d) the general manager, property protection branch manager and competent area manager of the contractor operating a part of the camera system, and the general manager and security technology specialist engineer of the company supporting the operation of the camera surveillance system.

(3) The employees of the contractor of the University, who perform property protection and facility security tasks can monitor the live video broadcast of the camera surveillance system.

(4) In the extent necessary for performing their work, the administrative employees may get access to the records or the report made during the review of the report.

(5) If regarding the treatment or the use of the camera records or the operation of the camera surveillance system any special task arises, which cannot be performed by the employees of the University, the University may assign a sole entrepreneur or a company to perform such task. During this, the employees of the company or the sole entrepreneur may have access to the camera surveillance system or the records in an extent necessary for the performance of their work.

(6) The general manager of the company contracted by the University and performing the operation support of the security systems and the employees assigned by such manager may have the highest level of authorisation necessary for the operation of the systems, however, they shall not be entitled to review or save records or to inspect live video broadcast unless unambiguously authorised in writing by the people determined in the paragraph (1) of the section 8 hereof.

Procedure of the review and the use of records[7]

Section 9

(1) Records can be reviewed if the person entitled to order review becomes aware of any circumstance based on which it can be reasonably assumed that the review of the records may be necessary:

a) to clarify the circumstances of an unlawful activity affecting the assets, buildings of the University or the natural environment and to identify the perpetrator,

[7]Amended: on 01 May 2023

b) to clarify the circumstances of an unlawful activity affecting the assets of the data subject and to identify the perpetrator,

c) to clarify the circumstances of an accident, work accident or damage event,

d) to clarify the circumstances of an unlawful activity violating the regulations of the Code of Ethics and to identify the perpetrator,

e) to clarify the circumstances of an assumed unlawful activity of any employee based on which the University may impose an adverse legal consequence on such employee, and the identification of the perpetrator

f) to reach another aim of data processing as determined in the paragraph (2) of the section 5 hereof,

g) in cases ordered by the police and the authorities.

(2) Upon ordering the review of records, it shall be determined who out of the entitled people should be present during the review of the records of the camera surveillance system.

(3) If the review of the camera records is necessary due to an unlawful act, damage or accident by a university citizen, this data subject may be present during the review of the records. If the assumed perpetrator is an employee of the University, it shall be ensured to let him/her be present during the review of the records, unless this is excluded by the circumstances of the review.

(4). The information technology tasks accompanying with the review of the records or with the saving of these record to external data carrier shall be performed by the people determined in the items c) and d) of the paragraph (2) of the section 8 hereof.

(5) In case of the review of the future use of the records, the report described in the Annex 1 hereof shall be made.

(6) Based on the report, the person having ordered the review of the records shall bring a decision on the future use of the records. The records of the camera surveillance system can be used for:

a) the initiation of a criminal procedure,

b) the initiation of an infringement procedure,

c) the submission of a statement of claim or for the submission of the record as evidence during the lawsuit,

d) the procedure performed by the University in case of a work accident or for the procedure of the labour authority,

e) the procedure launched based on the Code of Ethics,

f) to reach another aim of data processing as determined in the paragraph (2) of the section 5 hereof.

(7) If any authority (court, prosecution office police) calls the University to forward the records to them, the University shall be entitled to forward the record, if the call of the authority (court, prosecution office, police) clearly includes the legal reference based on which the authority is entitled to process the records.

(8) Storage of the saved (blocked) records

a) the company contracted by the University and performing the operation support of the security systems shall be entitled to store the records.

b) The records shall be safely stored and guarded until use or erasure in a lockable cabinet, separated from other data carriers in a way that only the person entitled to storage can have access to them. Storage can be performed either by a designated physical data carrier or by means of software, i.e. a logical device of suitable accessibility.

c) The records, if not used, can be stored for at most 3 months from blockage. Before final erasure, the person having ordered the saving of the records shall be requested to make a statement on the need for further storage.

d) The person having ordered the use or the erasure of the records and the data protection officer shall be notified of the use or the erasure of the records.

CHAPTER III

RIGTHS OF DATA SUBJECTS AND THEIR EXERCISE OF SUCH RIGHTS[8]

Obligation to inform in advance

Section 10

(1) The company contracted by the University and performing the operation support of the security systems shall ensure:

a) the display of warning sign (pictogram) of camera surveillance system

b) and the display of the privacy policy according to the Annex 2 hereof,

which shall be provided by the Security Directorate.

(2) The warning sign and the privacy policy shall be displayed at the right vicinity of the point of entry into the territory of the real estate.

(3) The privacy policy according to the Annex 2 hereof shall be published on the central website of the University.

(4) The heads of the organisational units of the University shall cooperate with the organisation determined in the paragraph (1) to perform the obligations in such paragraph.

Rights of data subjects regarding data processing

Section 11

(1) The rights of the data subjects to be exercised regarding the camera surveillance system - except the paragraphs (2) - (4) - shall be governed by the related regulations of the Internal Privacy Policy.

(2) If the data subject exercises the right of access or the right to request copy related to the records, the University - even in case of compliance with such request - shall provide information about:

[8]Amended: on 01 May 2023

a) the aim and the legal basis of the operation of the camera surveillance system,

b) the duration of the storage of the records,

c) to whom the University has forwarded the records (if the University has forwarded the records containing the personal data of the data subject to another controller),

d) the rights of data subjects regarding data processing,

e) the right to submit a complaint to the Hungarian National Authority for Data Protection and Freedom of Information.

(3) Considering the characteristics of data processing accompanying with the operation of the camera surveillance system, the data subject cannot request the rectification of the records. The request of rectification of the data subject can relate only to the report in the Annex 1 hereof.

(4) In case of camera surveillance system, the right to data portability is not applicable, since the legal basis of the data processing is not the consent of the data subject or a contract.

Procedure based on the exercising of rights of the data subject

Section 12

(1) During the exercising of rights of the data subject, the distribution of tasks, the identification of the data subject, the execution or the denial of the request and the deadline of execution shall be governed by the regulations of the Internal Privacy Policy.

CHAPTER IV

FURTHER OBLIGATIONS REGARDING DATA PROCESSING

Information technology and organisational security measures[9][10]

Section 13

(1) In case of an information technology system operating the camera surveillance system and storing the records:

a) the access to or the login into these systems by unauthorised people shall be prevented,

b) appropriate access rights shall be set, and user name and password shall be set for each user with access rights,

c) password requirements shall be regulated (minimum length of password, characters to use, periodical mandatory change of password, number of incorrect password entries before the blocking of account),

[9]Amended 01 April 2021

[10]Amended: on 01 May 2023

d) it shall be ensured that people with access rights can access the records only within the framework of their access permit,

e) by logging it shall be ensured that it can be checked and established which user entered the IT system and when,

f) it shall be ensured that it can be checked and established which user reviewed or copied the records or performed another data processing operation (such as forwarding) with the records,

g) it shall be ensured that only authorised people have access from an external network, in a controlled way,

h) it shall be ensured that the records are stored separately from other personal data and that the backup of the records within the period determined in the paragraph (1) of the section 7 hereof,

i) the automatic erasure of the records over the period determined in the paragraph (1) of the section 7 hereof, even from the archives of backups.

(2) By keeping a record according to the Annex 3 hereof, the IT Security Centre of the Security Directorate shall document that the camera surveillance systems of the University meet the requirements of the paragraph (1).

(3) people having access to the camera surveillance system can use exclusively the IT devices provided by the University to store the records and the backups. people having access may not store the records on an own IT device or an IT device owned by another person.

(4) During the operation of the camera surveillance system it shall be ensured that

a) only people having access to the records can enter the room where the records and the backups are stored,

b) in the room where the live video shown by the camera surveillance system is monitored, unauthorised person is allowed to stay only in exceptional cases and only for the necessary time,

c) the monitors showing the live video of the camera surveillance system cannot be watched by unauthorised person.

(5) People with access right shall keep confidential the personal data they became aware of during the review or the saving of the records and during the writing and the handling of reports, they shall not publish such data or disclose them to any third person. This obligation of confidentiality shall survive even after the termination of the legal relationship.

Data protection impact assessment

Section 14

(1) The University shall perform a data protection impact assessment related to the camera surveillance system if

a) it is mandatory based on GDPR,

b) it is reasonable based on the guidelines of the European Data Protection Board and the Hungarian National Authority for Data Protection and Freedom of Information.

(2) Data protection impact assessment shall be performed according to the related regulations of the Internal Privacy Policy.

Management and reporting of personal data breaches

Section 15

(1) The management and reporting of personal data breaches related to the camera surveillance system shall be governed by the related regulations of the Internal Privacy Policy.

Use of a processor

Section 16

(1) During its activity regarding the records of the camera surveillance system, the company or sole proprietor determined in the paragraphs (3) and (5) of the section 8 hereunder shall be qualified as the processor of the University.

(2) The use of a processor shall be governed by the related regulations of the Internal Privacy Policy.

Installation of a new camera[11]

Section 17

(1) A new camera can be installed after the procedure determined in the Annex 4 hereof.

(2) Before commissioning, the new camera shall be recorded in the register determined in the section 18 hereunder.

(3) Prior notification according to the section 10 hereof shall be ensured before the commissioning of the new camera. The organisation determined in the paragraph (1) of the section 10 shall ensure the display of notifications.

Register

Section 18

(1) The University shall keep a register about the cameras subject hereto.

(2) This register shall include the exact location of the cameras, their angles or vision, the operator of the cameras, the position of the person monitoring the live records, the place of observation, the fact and the duration of saving the records and the place of storage of the records.

(3) The register of cameras shall be kept by the Security Directorate.

(4) The data protection officer shall register the requests on review and blockage, together with the report according to the paragraph (5) of the section 9 and the report on seizure by the authority. The data and documents necessary for keeping a register shall be sent by the Security Directorate to the data protection officer.

[11]Amended: on 01 May 2023

CHAPTER V

MISCELLANEOUS

Section 17

(1) Any data protection questions not regulated herein shall be governed by the regulations of the Internal Privacy Policy.

(2) This order entered into force on 15 January 2021, and it shall be valid until withdrawal. Modifications are indicated by footnotes.

Debrecen, 01 May 2023

Prof. Dr. Bács Zoltán

chancellor

Annex 1[12]

Report

on the review or further use of the records saved by the camera surveillance system

Name and position of the person ordering the review or forwarding of records	
Name of the person (organisation) initiating review or forwarding	
Reason of ordering review or forwarding	
Place and time of the review of the records *(hour, minute)*	

Names and positions of the people taking part in the review of the record: *(in case of the presence of the data subject, the position shall be "data subject")*

Name	Position

Description of the findings during the review of the records:

_____

_____

_____

[12]Amended: on 01 May 2023

_____

_____

_____

_____

_____

_____

Other circumstances: (especially the events during the review of the record, or if the data subject is present, the remarks or the complaint of the data subject)

_____

_____

_____

Dated in _____*(city)* _____*(day)* _____*(month)* _____*(year)*

Signatures:

Name	Signature

Annex 2[13][14]

Privacy policy

on the data processing accompanying the operation of the camera surveillance system

Controller and the operator of the camera system

The controller is the **University of Debrecen** (hereinafter referred to as **University**):

Postal address: H-4032 Debrecen, Egyetem tér 1.

Contacts of data protection officer:

E-mail: adatvedelmi.tisztviselo@unideb.hu

For the operation of the camera surveillance system, the University of Debrecen uses a processor.

Regulatory background of the camera system

The camera system shall be primarily subject to the order of the Chancellor of the University and the Regulation 679/2018 (EU) of the European Parliament and the Council (GDPR).

Purpose of the operation of the camera system

The University uses the camera surveillance system for the purposes below:

- protection of the assets, building and real estates of the University,
- protection of the assets of the data subjects,
- clarification of the circumstances of accidents or damage events,
- investigation of other unlawful acts.

Processed set of personal data

The camera system records the image of the person entering the monitored area and the acts of the data subjects seen in the records.

Legal basis of making a record

The legal basis of data processing shall be the legitimate interest of the University [item f) of the paragraph (1) of the article 6 of the GDPR]. The primary legitimate interests of the University are the clarification of the circumstances of an infringement of law, an accident or a damage event, the identification of the perpetrator and the launch and the performance of the necessary procedure.

Place and duration of the storage of the records

The University stores the records in the servers located in the territory of the University. The University stores the records for 10 days.

Scope of people having access

The review of the records can be ordered by the chancellor, the data protection officer of the University, the security director general and the deputy security director general. Only people allowed by the order on camera surveillance system can be present during the review of the records.

Fundamental data security measures

The University shall store the records in an own physical or logical data storage, which shall ensure the access and security logging according to requirements.

Rights of data subject and the possibilities of the exercise of rights

Right of access. The data subject can get information what the records show about him/her and how the University handles the records. The data subject can inspect the records of the camera system, and can request a copy of such records. Data subject can get further details thereabout via the contact data indicated in the privacy policy.

Right to restriction of processing. The data subject can request the blockage of records, e.g. if he/she intends to use the records as evidence in a legal procedure launched by him/her.

Right to object. The data subject shall be entitled to object against data processing.

If the data subject thinks that the data processing is not in compliance with legal regulations, he/she may initiate a procedure in the Hungarian National Authority for Data Protection and Freedom of Information or may request judicial remedy.

[13] Amended 01 April 2021

[14] Amended: on 01 May 2023

Annex 3[15][16]

Information technology safety measures

Information technology safety measure	Solution applied
Prevention of unauthorised people to get access to or to log into information technology systems	
Appropriate setting of access rights by setting a separate user name and password for each access right	
Regulation of password requirements (minimum length of password, characters to use, validity period, number of incorrect password entries before the blocking of account),	
Ensuring that people with access rights can access the records only within the framework of their access permit,	
By logging it shall be ensured that it can be checked and established which user entered the IT system and when	
Ensuring that it can be checked afterwards which user reviewed or copied the records or performed another data processing operation (such as forwarding) with the records,	
Ensuring that only authorised people have access from an external network, in a controlled way,	
Ensuring that records are stored separately from other personal data	
Ensuring the backup of records within 10 days	
Ensuring that records older than 10 days are automatically erased from the archives of backups	

[15]Amended 01 April 2021

[16]Amended: on 01 May 2023

Annex 4[17]

Procedure of the installation of a new camera surveillance system in the territory of the University of Debrecen

Introduction

(1) This is to ensure that data processing during the use of the camera surveillance systems located in the territory of real estates owned by the University of Debrecen (hereinafter referred to as University) is in compliance with related legal regulations and data protection requirements. Before the installation of the camera system, the controller shall assess whether this measure is on the one hand suitable to reach the set purpose and on the other whether it is appropriate and necessary for reaching this purpose.

(2) Video camera monitoring measures can be decided only if the purpose of data processing cannot be reasonably achieved by another tool impairing less the fundamental rights and freedoms of the data subject.

(3) The installation process of the new electronic monitoring systems shall be subject to this unified procedure, which makes possible the achievement of the purposes set in the paragraph (1) hereof.

Installation of a new camera surveillance system

Section 1

(1) New cameras can be installed and commissioned in possession of a separate dedicated permit.

(2) Before the installation and the commissioning of the new camera surveillance system, the head of the organisational unit intending to install the camera or the agent thereof shall submit an application for the installation of a new camera surveillance system via a designated electronic application interface.

(3) In case of a new investment or restoration, the Chief Engineer's Department shall submit the application for the installation of the new camera.

(4) A camera surveillance system can be installed for the following purposes determined in the paragraph (1) of the section 5 of the Chancellor's order on the camera surveillance system operating in the territory of the University of Debrecen:

a) protection of the assets of the University, the prevention of the related violations of law and the support of the proving thereof,

b) protection of the buildings on the real estates owned by the University and the natural environment, the prevention of the related violations of law and the support of the proving thereof,

[17]Amended: on 01 May 2023

c) protection of the assets of the data subjects, the prevention of the related violations of law and the support of the proving thereof,

d) clarification of the circumstances of accidents, work accidents or damage events in the area monitored by the camera surveillance system and the support of the proving thereof,

e) clarification of the circumstances of the acts committed by the university citizens and violating the regulations of the Code of Ethics accepted by the decision no. 16/2007 (15 November) brought by the Senate of the University of Debrecen on 15 November 2007 and the support of the proving thereof,

f) clarification of the circumstances of any acts committed by the employee and violating law based on which the University may impose an adverse legal consequence on the employee, and the support of the proving thereof.

(5) No camera can be installed for the following purposes:

a) No camera surveillance system can be used on locations where monitoring would violate human dignity, especially in changing rooms, fitting rooms, lavatory, toilet, dining room for employees. If in any of these rooms there is an asset to be protected (such as a vending machine) where an employer's interest can be justified (e.g. the device has been damaged several times), the use of electronic surveillance system is justified.

b) In case of the monitoring of devices or raw materials of significant value, which are stored in the workplace, the rooms having importance regarding protection - mostly warehouses - and the corridors leading to them can be monitored.

c) If there is a camera at the entrance of the real estate, it cannot monitor the public area in front of the entrance.

d) Cameras cannot be operated for the permanent monitoring of the employees and their activities without an expressed purpose.

Submission of application by using the electronic application interface

Section 2

(1) Electronic application interface is available at: https://forms.it.unideb.hu/kamera-felszereles-igenyles

(2) Application for installation of a camera shall be submitted separately for each camera. If multiple cameras are installed within the same building, the application shall be completed separately for each camera.

(3) After the completion of the data of the applicant, the following monitoring-related data shall be given for each camera:

a) Area to monitor: name of the site or building, exact location of the camera to be installed, determination what the camera is going to monitor,

b) Purpose of monitoring: security of property or the support of healthcare service. It is necessary to indicate whether employees are monitored,

c) Way of monitoring: monitoring or saving.

(4) If out of the purposes determined in the item b) of the paragraph (3), the security of property is selected, it is necessary to select the purpose of the electronic monitoring system - as intended by the applicant organisation - out of the purposes determined in the paragraph (4) of the section 1 of this procedure.

Adjudication of the received applications

Section 3

(1) The applications received via https://forms.it.unideb.hu/kamera-felszereles-igenyles shall be available for the Security Directorate, the data protection officer, the healthcare data protection officer and the Chief Engineer's Department.

(2) The received applications shall be considered first by the data protection officer of the University of Debrecen and the applications from the Clinical Centre by the healthcare data protection officer in terms of compliance with data protection regulations.

(3) If applications need specification or amendment, or if the data protection officer or the healthcare data protection officer considers the on-site survey reasonable, he/she shall immediately contact the representative of the organisation having submitted the application.

(4) After the specification or the amendment of the application or in reasonable cases after the on-site survey, the people determined in the paragraph (3) and being entitled to adjudicate the applications shall adjudicate the application in writing, at most within 5 working days.

(5) If the application is not in compliance with data protection aspects, the data protection officer and the healthcare data protection officer shall be entitled to reject the received application, and shall justify such rejection.

(1) In the justification, he/she shall call the attention to the data protection aspects he/she considers necessary to comply with for the lawful operation, and he/she shall call the applicant to submit a new application for the installation of an electronic surveillance system, which observes the requirements given.

(2) The complete applications which are in compliance with the data protection requirements shall be approved by the data protection officer in writing. He/she shall forward the approval to the Security Directorate.

(3) The approval shall be forwarded by the Security Directorate to the employees of the Chief Engineer's Department assigned to perform planning and construction, who shall contact the applicant organisation.

Register

Section 4

(1) The register shall be managed and kept up to date by the Security Directorate.

(2) After the installation and the delivery of the electronic surveillance system, the applicant organisation shall send the data of the cameras - as indicated in the paragraph (3) herein - to the Security Directorate for registration.

(3) Register shall include the following data of the electronic surveillance system:

a) exact location of the cameras,

b) angle of vision of the cameras,

c) operator,

d) position of the person monitoring the live records,

e) place of monitoring,

f) the fact and the duration of saving the records and the place of storage of the records.

System requirements in case of the installation of new property security camera system

Section 5

(1) The system shall connect to the intranet network of the University by a cable.

(2) Minimum requirements for the design of the IP surveillance system:

a) Recorder / server:

- • handling of at least 2 HDDs (raid handling)
- • design to install in rack (in the absence thereof, a rack tray)

b) Cameras

- • resolution of at least 4 megapixels
- • at least 25 fps
- • angle of vision: 2.8 mm (wide angle, outdoors and in larger areas – 105 degrees) – deviation is possible if reasonable
- • infra illumination: at least 25 m
- • accepted manufacturers: HikVision, Dahua, Intellio, Vivotek
- • design: indoors: dome, outdoors: tube (in case of low installation height (< 2.5 m) dome design outdoors as well)
- • ONVIF compatibility
- • h264 or h265 compression
- • PoE support is necessary

- • at least IP67 protection

(3) For the precise registration and the compliance with legal regulations, the installer of the IP monitoring system shall send the followings to the Security Directorate:

a) In case of a camera:

- installation location of the camera,
- area monitored by the camera
- whether the camera records or only shows live video
- IP address
- MAC address
- make and unique identifier (SN) of the device
- name and password of admin user

b) In case of recording systems:

- IP address
- MAC address
- make and unique identifier (SN) of the device
- name and password of admin user