## Annex 1[[1]](#footnote-1)

**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:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**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[[2]](#footnote-2)[[3]](#footnote-3)

**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.

## Annex 3[[4]](#footnote-4)[[5]](#footnote-5)

**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 |  |

# Annex 4[[6]](#footnote-6)

***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:
5. protection of the assets of the University, the prevention of the related violations of law and the support of the proving thereof,
6. 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,
7. protection of the assets of the data subjects, the prevention of the related violations of law and the support of the proving thereof,
8. 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,
9. 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,
10. 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.
11. No camera can be installed for the following purposes:
12. 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.
13. 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.
14. If there is a camera at the entrance of the real estate, it cannot monitor the public area in front of the entrance.
15. 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:
4. 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,
5. Purpose of monitoring: security of property or the support of healthcare service. It is necessary to indicate whether employees are monitored,
6. Way of monitoring: monitoring or saving.
7. 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.
6. 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.
7. 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.
8. 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:
4. exact location of the cameras,
5. angle of vision of the cameras,
6. operator,
7. position of the person monitoring the live records,
8. place of monitoring,
9. 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:
   1. Recorder / server:

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

1. 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

1. 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:
2. 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

1. In case of recording systems:

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

1. Amended: on 01 May 2023 [↑](#footnote-ref-1)
2. Amended 01 April 2021 [↑](#footnote-ref-2)
3. Amended: on 01 May 2023 [↑](#footnote-ref-3)
4. Amended 01 April 2021 [↑](#footnote-ref-4)
5. Amended: on 01 May 2023 [↑](#footnote-ref-5)
6. Amended: on 01 May 2023 [↑](#footnote-ref-6)