TALLINNA TERVISHOIU KÕRGKOOL

APPROVED
Tallinn Health Care College
Rector's Order No 1-4/33 of
November 8, 2022

TALLINN HEALTH CARE COLLEGE'S PROCEDURES FOR VIDEO SURVEILLANCE AND THE USE OF ACCESS SYSTEM

1. GENERAL PROVISIONS

1.1. Current Procedures for Video Surveillance (hereinafter: *Procedures*) was established in accordance with General Data Protection Regulation of the European Parliament and of the Council (hereinafter: *GDPR*) („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"), and of guidelines of Data Protection Inspectorate.

1.2. Current Procedures provides principles of video surveillance and the use of access system at Tallinn Health Care College (hereinafter: *College*), rights of data subjects and obligations of the College and their members of staff regarding video surveillance.

1.3. Surveillance equipment is a set of technical equipment (transmits or records a picture or an electronic signal), which is intended to keep guard of a territory, person, item or process or to determine the location of a territory, person or item or the place at which a process is occurring; and which transfers, records the picture in real time by stationary security camera installed on outer walls of the College or indoors; it allows to edit and reproduce this image.

1.4. Access system is a set of technical equipment (transmits or records a picture or an electronic signal), which is installed in the rooms of the College to ensure safety, and to stop and regulate the access and movement of any unauthorised person at the territory of the College.

1.5. Recording is an electronic collection of a picture and other data.

1.6. Security camera is a device allowing observation and recording.

1.7. College is the responsible controller of the recordings.

1.8. Data subject is a person whose data are processed.

1.9. Processing of personal data is any action taken involving personal data of any person, incl. collecting, recording, organising, storing, changing, disclosure, allowing access to the data, carrying out automated searches and act of extraction, use of personal data, forwarding, cross-usage, combination, closure, deleting or destroying or several acts mentioned above regardless of the manner in which the operations are carried out or the means used.

2. AIM AND LEGAL BASIS OF TALLINN HEALTH CARE COLLEGE˙S VIDEO SURVEILLANCE AND ACCESS SYSTEM

2.1. Surveillance equipment, observed in real time, is used 24/7 at the territory and buildings of the College (hereinafter *video surveillance*).

2.2. Video surveillance and access system are used by the College to guard the buildings and rooms used by the College; also, to protect the property and people at the premises on the legitimate interest.

2.3. Video surveillance and access system are used as security measures by the College to prevent unauthorised persons from entering the workplace rooms without any reason; and to prevent situations threatening College´s staff members, learners and third parties; to ensure safety; to react in case of hazardous situations; and to protect College´s property.

2.4. Video surveillance is used to observe College´s outside areas, entrance areas, halls, lobbys and rooftop garden.

2.5. Access system is used to administer entrance to College´s buildings, halls and workplace rooms.

2.6. Corresponding signs inform about the use of video surveillance at College´s premises or rooms.

3. PRESERVATION OF RECORDINGS

3.1. Data processed by video surveillance are recorded in the corresponding server.

3.2. Data processed by access system are recorded in the computer administering access system, which is the subject to back-ups, using standard means.

3.3. Video surveillance operates on the principle of overwrite mode of the recordings. Storage capacity of the video surveillance was selected based on ability to preserve all recordings of every camera for 3 (three) months by using minimum size compression algorithm H.265and minimum size resolution 1920x1080 (HD) and minimum frame rate15 fps; if storage capacity is exceeded, old information will be overwritten by new information, after that older recordings will be inaccessible automatically.

3.4. Access system preserves the data for 30 (thirty) calendar days.

3.5. The College has a right to retain video recording for longer period in case it is necessary for investigation of some cases; however, not for longer period as set by legislation in the Security Act, and only in case the recording was available at the time of reporting the incident considering the principle of overwrite mode.

3.6. Security measures are implemented on video surveillance and Access system; these prevent the access of unauthorised persons to the components of the system and ensure the availability of the system and data integrity.

4. ENSURING SECURITY OF DATA PROCESSING

4.1. To ensure security of data processed by the College, unauthorised access to observation equipment and video surveillance is prevented to eliminate to option for unauthorised monitoring, copying, changing, transmission and deletion of the recordings.

4.2. Recordings of observation equipment and video surveillance are accessed by College´s head of administrative only. If necessary, recordings can be accessed by additional subjects authorised by the Rectorate.

4.3. Real-time monitoring of video surveillance is allowed by the College to the head of administrative and administrators, and if necessary, to additional subjects authorised by the Rector. Automatic notifications of anomalies are installed by College´s head of administrative.

4.4. Equipment used for monitoring used by the College are installed so that every user (incl. head of administrative) needs their personal username and a password to enter the system.

4.5. Use of the system is logged, it means it is possible to identify the use of the system afterwards; when and which data were looked at, recorded, changed, or deleted, and the person who performed these procedures. Corresponding logs are preserved in the volume derived from the capacity of the hard drive used.

4.6. A reasoned request by any means capable of producing a written record (e-mail) should be submitted to the head of administrative of the College to process the data collected by video surveillance.

4.7. The request must include the reason for necessity of data processing; the description of specific circumstances, case, or situation; the date; and if possible exact time of the situation or the happened event, which recordings are to be processed (watched).

4.8. Unauthorised and unwarranted watching or observation of data recorded by video surveillance or access system by the user is prohibited.

5. RIGHT TO ACCESS THE RECORDING

5.1. Every member of staff of the College, learner, visitor or other third party as the right to access the recording representing him or her.

5.2. The College is obliged to check in each specific case whether the person requesting to watch the recording is the person that is represented in the recording.

5.3. The request to inspect personal data is denied if it may have following consequences:

5.3.1. adversely affect the rights and freedoms of others;

5.3.2. interfere crime prevention or catching a criminal;

5.3.3. complicate the ascertainment of the truth in a criminal proceeding.

5.4. In case of issuing a copy of the recording or allowing to watch it the College is obliged to ensure the protection of personal data and privacy of third parties. It means that all third parties seen in the recording shall be deidentified considering that people can be identified by their clothes, walk etc., too.

5.5. Data subject should contact College´s data protection specialist to request the access to the recordings representing them by using the e-mail andmekaitsespetsialist@ttk.ee.

5.6. Data protection specialist shall forward the corresponding request to the College´s head of administrative having user rights of the video surveillance system.

5.7. In case of receiving the request, the College has a right to ask the person to add the details, which information or which actions of personal data processing is the request more specifically linked to.

6. TRANSFER OF DATA COLLECTED BY VIDEO SURVEILLANCE

6.1. The College has the right to transfer collected data to law enforcement institutions and other state or local government institutions.

6.2. The College shall transfer the video surveillance recordings in case of proceedings for the infringement of the law only following legislation rules if the institution proceeding submits a request and in case the recordings exist.

7. ACCESS SYSTEM AND USING IT

7.1. The College and the Student Hostel is equipped with access system and necessary access cards (chips) to use the access system are issued after concluding contracts with the College (employment contract, under the law of obligation, housing contract or other relevant contract); or in case of learner after their matriculation.

7.2. Access system allows its user the access to the areas determined to them individually by their contract.

7.3. Only the employee authorised by the College has the permission to access system and its logs; also, the person for maintenance of these systems who has the right to process personal data to the extent necessary to achieve the goals of processing personal data only.

7.4. The College has the right to transfer data collected by access system to law enforcement institutions only in case of proceedings for the infringement of the law following legislation rules if the institution proceeding submits a request and in case the logs exist.

8. IMPLEMENTING PROVISIONS

8.1. Current Procedures enter into force after its legal approval.

8.2. College´s data protection specialist administers current Procedures.