APPROVED

on ____ May 2018

Acting Rector _____

Video Surveillance System Data Protection Regulations

I. General provisions

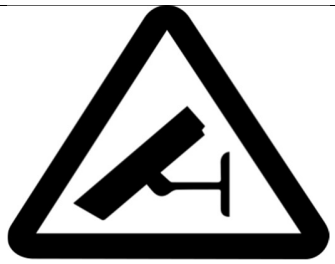
1. Video Surveillance System Data Protection Regulations of the JSC TRANSPORTA UN SAKARU INSTITŪTS (hereinafter the Institute), reg. No. 40003458903, Lomonosova 1, Riga, LV-1019 (hereinafter the Regulations) determine the processing, use and protection of the data obtained as a result of video surveillance as well as the procedure for the installation of video surveillance equipment.

2. The Regulations have been developed in accordance with 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 (General Data Protection Regulation) and other requirements set forth by laws and regulations of the Republic of Latvia pertaining to the use and safety of video surveillance systems.

3. The purpose of the video surveillance system is to protect the property of the Institute, to ensure the safety of employees and students, to prevent possible violations of law, to record the fact of committing a criminal offence as well as to identify the potential offender (ensuring the legality of evidence), in the detection and inspection of potentially dangerous objects, and potential finding of items.

4. The Regulations are binding upon all users of the personal data processed by the video surveillance system (persons that have been granted system user rights). The Regulations apply to all personal data recorded in video surveillance cameras (video surveillance recordings).

5. Video surveillance and the processing of the resulting personal data are carried out in the internal premises of the Institute, which is indicated by a special sign placed at the entrance to the video surveillance zone according to the sample. The sign contains information about the Controller of the system and its contact information.



VIDEO SURVEILLANCE
Objective: Prevention and detection of criminal offences related to the protection of property
The Controller: JSC TRANSPORTA UN SAKARU INSTITŪTS, reg. No. 40003458903
Registered address: Lomonosova 1, Riga, LV-1019

6. The security officer, Head of the Computer Technologies Division (hereinafter the User), is responsible for the security of processing of personal data resulting from video surveillance in the Institute.

II. Classification of information and allocation of user rights

7. Data recorded with the video surveillance cameras is qualified as restricted access information because it contains personal identification data. Only authorised, identified system users are entitled to access and process such data.

8. The user who is authorised to process personal data, access the video surveillance software and its records, is assigned by the person responsible for security, the Chairperson of the Board.

III. Duties, rights and liability of the user

9. Direct duties, rights and liability of the user are included in the job description of each user.

10. It is the duty of the user to research the Regulations, sign off and comply with such in the daily work. The user undertakes to retain and not unlawfully disclose any personal data.

11. The user is entitled to:

11.1. Use the appliances transferred for use to organise video surveillance image recording;

11.2. Require support in the event of malfunction of a computer or its software or where the user has sufficient reason to believe that there is a potential threat (danger);

11.3. Allow access to personal data obtained as a result of video surveillance to the relevant data subject (only about himself/herself); to other persons, if required for the performance of their work duties, in accordance with the authorisation specified in Paragraph 8 of the Regulations and only in accordance with the purpose of data processing specified in Paragraph 3 of the Regulations.

12. The user is prohibited to:

12.1. Disclose information about the structure and configuration of the video surveillance system network of the Institute and disclose classified information to unauthorised persons;

12.2. Allow access to personal data obtained as a result of video surveillance (video surveillance records) to other persons, if it is not related to the performance of direct work duties and if such authorisation has not been granted by the Board of the Institute (Paragraph 8);

12.3. Copy any files containing personal data on external media (floppy disks, USB and/or CD) if it is not related to the performance of direct work duties and if such authorisation has not been granted by the Board of the Institute (Paragraph 8).

13. The user is liable for:

13.1. Video surveillance appliances put at his/her disposal;

13.2. The actions taken with the video surveillance appliances transferred to him/her;

13.3. Data retention without allowing their unlawful processing, accidental loss, destruction or damaging of personal data and their unlawful transfer.

14. The video surveillance system maintenance staff are obliged to change the video surveillance access codes (consisting of 8 symbols) once every three months. In the event that any another person has learnt the access code, it must be replaced immediately in order to provide for appropriate security measures.

15. The user undertakes to maintain the confidentiality of the information after the termination of the employment relationship as well.

16. The Board of the Institute is only entitled to disclose personal data resulting from video surveillance to law enforcement authorities in the procedure set forth by law, according to their request. In the events where the disclosure of personal

data is required, records should be kept of to whom (by identifying the person), when, for what purpose and what personal data have been disclosed. In the event of the release of video surveillance data to another person on a legal basis, the person who has received the data is responsible for the further processing of the personal data and its legality.

17. The Institute shall keep records of the persons involved in the processing of personal data from the video surveillance system.

IV. Installation of video surveillance appliances, use of the software and storage of information

18. The installation and administration of video surveillance appliances and their software in the procedure set forth by the Institute is ensured by the person responsible for security - the User (Head of the Computer Technologies Division).

19. When installing the video surveillance cameras, such camera placement should be chosen that is safe from unauthorised access and protects them from damage.

20. The servers processing personal data resulting from video surveillance must be located in a separate room or in a locked server rack with restricted access to ensure security against unauthorised access and to protect them from physical damage.

21. The following conditions shall be met during video surveillance:

21.1. The recorded or printed images as well as images on the live monitor must be of adequate quality. It must be ensured that no undesirable distortion of image details occurs during the recording process;

21.2. In digital recording systems, the appropriate amount of data compression must be chosen so as not to affect image quality;

21.3. Recorded images must feature the exact time and date when the record is or has been made;

21.4. Continuous maintenance of video surveillance cameras must be provided to ensure that video surveillance cameras continue to make records of appropriate quality for the purpose intended;

21.5. If wireless data transmission is used, appropriate security measures must be provided to ensure that there is no interruption in data transmission and that data is not intercepted.

22. It is forbidden for the user to change the configuration of the video surveillance equipment and software received for use in any way and to install any software.

23. The Institute is responsible for the technical condition of the video surveillance appliances, ensuring the quality of recordings and preventing undesired distortion of the image/data components during the process of recording or period of storage.

24. The duration of storage of information resulting from video surveillance is set at 31 days. After the end of this period, the Institute shall ensure the complete deletion of the data if the data have not been previously requested or criminal offences have been detected. If the data has been previously requested by competent state or municipal authorities or criminal offences have been detected, the data shall be stored as necessary.

25. The transmission of video surveillance images (on-line surveillance) and viewing of records must be provided in a separate room or in such a way that unauthorised persons cannot see the image monitors.

26. Video surveillance cameras should not be used to record conversations between people. Devices without audio recording functionality are selected for video surveillance, or it is disconnected.

27. Any unauthorised access to video surveillance appliances (cameras) and/or record data shall be reported immediately to the responsible person specified in Paragraph 18 of these Regulations, who shall document the fact of unlawful access accordingly and shall take the necessary security measures to prevent further security incidents.

V. Transfer of information to other public officials

28. The Institute shall disclose personal data to state and municipal officials in the cases specified by law. Personal data shall only be disclosed to those state and municipal officials who have been identified prior to disclosure.

29. The persons specified in Paragraph 28 of these Regulations shall be entitled to disclose personal data on the basis of a written application or agreement specifying the purpose of use of the data, unless otherwise provided by law. The personal data request shall contain information that enables identification of the person requesting data and the data subject as well as the volume of personal data requested.

VI. Action in the case of security incidents and accidents

30. The user shall immediately report all emergency situations (including fire, flood, accidents, etc.) to the responsible person specified in Paragraph 8 of these Regulations or to persons authorised by him/her.

31. The user shall immediately notify the responsible person specified in Paragraph 8 of these Regulations or a person authorised by him/her of the events where the video surveillance appliance access code has become known to a third party.

32. Upon the receipt of information about a potential security incident in the protection of personal data, the Institute shall immediately provide for the investigation of the security incident, the provision of information to the competent state authorities, if necessary, and the provision for taking the necessary preventive action to ensure the security of personal data in accordance with the requirements of laws and regulations.