ORDER
OF THE RECTOR OF VILNIUS
UNIVERSITY

ON THE APPROVAL OF THE DESCRIPTION OF THE PROCEDURE FOR THE PROCESSING OF VIDEO SURVEILLANCE DATA AT VILNIUS UNIVERSITY

No. R-530 of 2 October 2018
Vilnius

In accordance with Articles 43(1)(19) and 43(1)(42) of the Statute of Vilnius University, in order to implement 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 (General Data Protection Regulation), and taking into account the Description of the Procedure for the Processing of Personal Data at Vilnius University, approved by Order of the Rector of Vilnius University No. R-316 of 25 May 2018 "On the Approval of the Description of the Procedure for the Processing of Personal Data at Vilnius University":

1. I hereby a p p r o v e the accompanying Description of the Procedure for the Processing of Video Surveillance Data at Vilnius University (hereinafter the 'Description').
2. I hereby a s s i g n the heads of the units carrying out video surveillance to familiarise the employees of the unit carrying out the video surveillance with this Description.

Rector Prof. Artūras Žukauskas

Prepared by
Viktoras Bulavas, Information Security Officer of Vilnius University
Evaldas Raistenskis, Chief Specialist of Legal Issues, Property Management and Service Centre

APPROVED
by Order No. R-530 of 2 October 2018
of the Rector of Vilnius University

THE DESCRIPTION OF THE PROCEDURE FOR THE PROCESSING OF VIDEO SURVEILLANCE DATA AT VILNIUS UNIVERSITY

CHAPTER I
GENERAL PROVISIONS

1. The purpose of the Description of the Procedure for the Processing of Video Surveillance Data at Vilnius University (hereinafter the 'Description') is to regulate video surveillance at Vilnius University (hereinafter the 'University').

2. Video surveillance is performed and video data is processed 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, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter the 'GDPR'), the Republic of Lithuania Law on Legal Protection of Personal Data (hereinafter the 'ADTAĮ'), and other legal acts implementing it and regulating personal data protection at the University.

3. Terms used in the Description:

3.1. Personal Data – any information relating to a Data Subject who is known or identifiable, directly or indirectly.

3.2. Data User – a natural person who has been granted access to video surveillance equipment and personal data.

3.3. Data Subject – a natural person whose personal data is processed for the purposes set out in the Description.

3.4. Data Processor – a natural or legal person, public authority, agency or other body that installs and maintains video surveillance cameras and video data recorders on behalf of the Data Controller.

3.5. Data Controller – Vilnius University, code: 211950810, address: Universiteto g. 3, Vilnius

3.6. Video surveillance – the processing of video data relating to a natural person using automated video surveillance cameras.

3.7. Video surveillance system – video data recorders and video surveillance cameras.

3.8. Other terms are used as defined in the GDPR, the ADTAĮ, and the Description of the Procedure for the Processing of Personal Data at Vilnius University, approved by Order of the Rector of Vilnius University No. R-316 of 25 May 2018 "On the Approval of the Description of the Procedure for the Processing of Personal Data at Vilnius University".

4. Vilnius University has the right to engage data processors (legal or natural persons who are not employees of Vilnius University) to maintain video surveillance systems or to process video data in order to ensure the safety of persons, property, and the public, as well as to ensure public order on the premises and territory of the University.

CHAPTER II
PURPOSE AND SCOPE OF VIDEO SURVEILLANCE

5. The purpose of video surveillance at the University is to ensure the safety of the University's employees, students, other persons, and property as well as public order.

5.1. Video surveillance is carried out on the territory of the University (courtyards, near warehouses, garages, etc.), at the entrances to the premises of the University, and in the premises (lobbies, corridors, server rooms, entrances to certain internal premises, etc.);

5.2. Video surveillance of the University's territory is carried out 24/7.

6. The video surveillance area shall not include premises outside the University territory, residential premises and/or private grounds or entrances belonging to them.

7. Video surveillance is prohibited in premises where the Data Subject expects absolute data protection and where such surveillance would be degrading to human dignity (e.g. toilets, changing rooms, etc.).

8. Video surveillance in the workplace is prohibited, except where the nature of the work makes it necessary to ensure the safety of persons, property or public order, and in other cases where other methods or means are inadequate and/or inappropriate for the purposes set out.

9. Where video surveillance is carried out at an employee's workplace, such employees shall be informed of the processing of their video data by signature or by any other means proving that they have been informed.

10. In the event of a change in the scope of video surveillance, Data Subjects shall be informed in accordance with the procedure set out in this Description.

11. Video surveillance data may not be used for purposes other than those referred to in Item 5 of the Description.

CHAPTER III
FUNCTIONS, RIGHTS, AND OBLIGATIONS OF THE DATA CONTROLLER AND THE DATA PROCESSOR

12. The Data Controller has the following rights:

12.1. to draft and adopt internal legislation implementing and regulating video surveillance;

12.2. to decide on the provision of video data to Data Subjects and/or third parties;

12.3. to designate the persons and units responsible for the protection of video data;

12.4. to authorise Data Processors to process video data.

13. The Data Controller has the following duties:

13.1. to ensure compliance with the requirements for processing personal data set out in the GDPR and other legislation governing the processing of personal data;

13.2. to exercise the Data Subject's rights in accordance with the GDPR and this Description;

13.3. to ensure the security of personal data by implementing appropriate organisational and technical measures to protect the security of personal data;

13.4. to choose only a Data Processor that guarantees the necessary technical and organisational measures for the protection of personal data and ensures compliance with such measures, and to enter into contracts with Data Processors; to give instructions to the Data Processor regarding the processing of video data; to be aware of any intended contracts with ancillary Data Processors and give prior written consent for their appointment;

13.5. to ensure that Data Subjects are informed that video surveillance is being carried out on the University premises.

14. The Data Controller carries out the following functions:

14.1. determines the purpose and scope of the video surveillance;

14.2. organises the installation of the video surveillance system;

14.3. grants access rights and the authorisation to process video data;

14.4. analyses the technological, methodological, and organisational challenges in the processing of video data and takes the necessary decisions to ensure the proper execution of video surveillance;

14.5. provides Data Subjects with extracts of video data, where appropriate;

14.6. organises employee training on the legal protection of personal data;

14.7. cooperates with the Data Protection Officer of Vilnius University;

14.8. performs other functions necessary for the exercise of the rights and duties of the Data Controller.

15. The Data Processor has the following rights:

15.1. to require Data Users to comply with the data security requirements set out in the Description and with the requirements of other legislation regulating the security of personal data;

15.2. to make suggestions to the Data Controller on how to improve the hardware and software measures for processing data;

16. The Data Processor has the following duties:

16.1. to ensure that access to video surveillance equipment and personal data is limited to persons authorised according to the procedure established in the Description;

16.2. to ensure that personal data is processed in accordance with the GDPR and other legislation on the protection of personal data;

16.3. to ensure that the scope of the surveillance video does not exceed the limits set out in this Description;

16.4. to ensure that the data provided to Data Subjects is consistent with the data processed by the Data Processor;

16.5. to protect video data against accidental or unlawful destruction, alteration, or disclosure.

17. The Data Processor carries out the following functions:

17.1. coordinates video recording actions;

17.2. implements the necessary technical data security measures, which shall be determined taking into account the risks arising from the processing of the data, including measures to ensure that video data is only accessible from the University's internal computer network;

17.3. ensures that access rights to the video data are granted only to persons authorised by the Data Controller;

17.4. upon request by the Data Controller, provides surveillance data for incident investigations, as well as to public authorities and institutions responsible for ensuring public order.

CHAPTER IV
PROVISION OF VIDEO DATA TO THIRD PARTIES

18. Video data shall only be disclosed to third parties under the criterion of lawful processing pursuant to a contract for the provision of personal data (in the case of multiple disclosures), upon request (in the case of single disclosures), or upon the lawful request of public authorities or institutions responsible for the maintenance of public order.

19. Video data may be submitted to a pre-trial investigation agency, prosecutor or court in connection with administrative, civil, or criminal cases at their disposal as evidence or in any other case provided by law.

CHAPTER V
TECHNICAL AND ORGANISATIONAL MEASURES FOR THE SECURITY OF VIDEO DATA

20. The following organisational and technical measures for the security of personal data shall be implemented to ensure the security of video data:

20.1. protection, management, and control of access to personal and video data is ensured;

20.2. access to video equipment and video data is limited to the person who needs the data to carry out their functions;

20.3. only those actions that the Data User has been granted the right to perform may be performed on video data;

20.4. passwords for access to video data:

20.4.1. are provided, changed, and stored by ensuring their confidentiality;

20.4.2. meet the complexity requirements for administrators set by the Information Technology Service Center (hereinafter the 'ITPC') of Vilnius University;

20.4.3. are changed at least once every two months;

20.4.4. are subject to mandatory change by the Data User at the time of the first login (reuse of the manufacturer's original passwords is prohibited);

20.5. protection of video data against unauthorised access to the internal computer network by means of electronic communications is ensured;

20.6. the physical security of video equipment storing video data is ensured (restricting and controlling access by unauthorised persons to premises where video equipment is located, etc.);

20.7. protection of computer equipment from malicious software is ensured (anti-virus, updates, etc.).

21. Procedure for granting, deleting and modifying access rights and authorisations to process video data:

21.1. access rights and authorisation to process video data are granted, removed and changed by an order of the head of the University unit conducting video surveillance;

21.2. the interested unit is responsible for enforcing the order granting or removing access to video data.

21.3. access rights to video data shall be removed upon termination of the employee's employment relationship with the University, upon a change in job functions for which access to video data is not required, or upon termination or expiry of the agreement for the processing of Personal Data concluded with the Data Processor.

22. Video data shall be recorded and retained for no less than five days and no longer than 60 days, after which it shall be destroyed. Where video data is used as evidence in civil, administrative, or criminal proceedings or in other cases provided for by law, it may be kept for as long as necessary for those processing purposes and destroyed as soon as it is no longer needed.

CHAPTER VI
PROCEDURE FOR MANAGING AND RESPONDING TO VIDEO DATA SECURITY BREACHES

23. Employees of the University or the Data Processor who have access rights to video data, having noticed any video data security breaches (acts or omissions that may cause or are causing a threat to the security of personal data), shall immediately, no later than before the end of the on-duty shift of the responsible post, inform the head of the unit conducting video surveillance and the Data Protection Officer of the University.

24. After assessing the risk factors for a breach of security of video data, the degree of impact of the breach, the damage and the consequences, the head of the unit carrying out the video surveillance shall decide, on a case-by-case basis and in consultation with the Data Protection Officer of the University, on the necessary measures to remedy the video data security breach and its consequences.

25. The Data Protection Officer of the University, after assessing the video data security breach, shall, if necessary, immediately inform the State Data Protection Inspectorate and the Data Subjects involved in the incident.

26. The Data Subject or the head of the unit carrying out the video surveillance shall take the decision to inform public authorities and institutions ensuring public order.

CHAPTER VII
RIGHTS OF THE DATA SUBJECT AND PROCEDURE FOR EXERCISING THEM

27. The rights of the Data Subject are set out in the Description of the Procedure for the Processing of Personal Data at Vilnius University.

28. The Data Subject shall exercise their rights in accordance with the Description of the Procedure for the Processing of Personal Data at Vilnius University and with this Description.

29. The Data Subject’s right to know about the processing of their video data shall be exercised as follows:

29.1. persons who are not employees of the Data Controller and whose video data is processed in the context of video surveillance are informed about the video surveillance:

29.1.1. by posting security camera signs at the entrance to the premises or territory under video surveillance;

29.1.2. the signs shall indicate 'Video surveillance is carried out by Vilnius University, code: 211950810, address: Universiteto g. 3, Vilnius (phone: 8 5 236 6200). Video surveillance is carried out for the purpose of ensuring the security of persons and property, and public order';

29.2. University employees shall be informed about video surveillance on University premises or territory:

29.2.1. before the start of video surveillance on the territory or site, or on the employee's first working day, or on the first working day after the employee's leave, period of incapacity for work, etc., if video surveillance at the workplace was started during this period;

29.2.2. by means of the document management information system, either by making this Description available for familiarisation or by signing a log (for employees without computerised workplaces) having given this information:

29.2.2.1. when the University has a video data processing agreement with a third party – who the controller and processor of video data is;

29.2.2.2. the purpose of video surveillance;

29.2.2.3. information on who may be provided with the video data;

29.2.2.4. the procedure for exercising the Data Subject's rights.

29.2.3. The familiarisation log shall be kept for two years from the last entry.

30. The Data Subject's right of access to their video data shall be exercised as follows:

30.1. the Data Subject shall, upon presentation of a reasoned written request and identification document or after having provided proof of their identity according to the procedure established by legislation or by means of electronic communications allowing to properly identify a person, after having indicated the territory or site where the Data Subject's video data may have been processed, after having indicated the reason for the request and other information necessary for processing the request, as specified in the Description of the Procedure for the Processing of Personal Data at Vilnius University, shall have the right to receive information on which cameras and which of their video data have been collected, for what purpose they are processed, whether they have been disclosed to data recipients, and if so, to which recipients;

30.2. if the Data Subject sends the request by post or courier, a copy of the Data Subject's identity document certified by a notary public must be attached to the request;

30.3. when a person's representative applies for information on that person, they must provide proof of representation and their identity document;

30.4. if the Data Subject's right of access to their video data cannot be exercised through the Data Subject's representative without the provision of the Data Subject's identity document or a certified copy thereof, the Data Subject's representative shall be informed thereof at the latest within 30 calendar days of the request;

30.5. upon receipt of a Data Subject's request for access to video data, the Data Protection Officer of the University shall assess and, within ten working days, make a decision to grant or deny access to the video data;

30.6. requests that are inadequately drafted, technically difficult to comply with, disproportionate or unreasonable, or likely to infringe the rights of others or the security of the University's property may be refused by a decision of the Data Protection Officer of the University;

30.7. The Data Subject shall have the right to appeal against the decision of the Data Protection Officer of the University to the State Inspectorate of Personal Data (hereinafter the 'SIPD');

30.8. when informing the person of the decision taken, the date and time when the person may come to the University to familiarise with the video data must be indicated;

30.9. the Data Subject shall be allowed access to the video data at the latest within 30 calendar days from the date of notification of the decision to the Data Subject; if the Data Subject, within this period, after the request has been made, does not, without a valid reason, arrive to familiarise themselves with the data in person or through a legal representative, the University

reserves the right to destroy such data in accordance with the established procedure;

30.10. the Data Subject's right of access to their video data shall be implemented in a manner that ensures the right to privacy of third parties, i.e. when the Data Subject accesses a video, if the video shows other identifiable persons or other information that may violate the privacy of third parties (e.g. the registration number of a vehicle), the videos shall be retouched or otherwise de-identified. If there are no technical possibilities to retouch video surveillance records, they shall only be made available to law enforcement officials.

31. The Data Subject's right to object to the processing of video data shall be exercised as follows:

31.1. the Data Subject's right to object to the processing of video data shall be exercised where video data is provided or processed for purposes other than those set out in this Description or in breach of the restrictions set out in this Description or other legislation;

31.2. if the Data Subject expresses a legally justified objection within the prescribed time limit, the Data Controller shall not carry out the processing of the video data and shall, at the request of the Data Subject, notify them of the termination of the processing operations on their personal data or of the refusal to terminate the processing operations, indicating the grounds for the refusal.

32. The right to request the destruction of own video data or to suspend, except for retention, the processing of own video data where the processing is not in accordance with the provisions of this Description and other legal acts shall be exercised in accordance with the following procedure:

32.1. if the Data Subject, having accessed their video data, determines that their video data is being processed unlawfully and unfairly, and they or their authorised representative contacts the University, the University shall immediately, and at the latest within ten working days, check the lawfulness and fairness of the processing of the Data Subject's video data free of charge and shall immediately destroy the unlawfully and unfairly collected video data or suspend the processing of such personal data, except for retention;

32.2. the University, having suspended the processing of video data at the request of the Data Subject or their authorised representative, shall retain the video data for which the processing has been suspended until they are destroyed (at the request of the Data Subject or after the expiry of the data retention period). Other processing operations on such video data may only be carried out:

32.2.1. for the purpose of proving the circumstances that led to the suspension of data processing;

32.2.2. if the Data Subject, directly or through an authorised representative, consents to the further processing of their personal data;

32.2.3. where necessary to protect the rights and/or legitimate interests of third parties.

32.3. The University shall notify the Data Subject or their authorised representative without delay, and at the latest within ten working days, of the successful or failed destruction of the Data Subject's video data or of the suspension of the processing of the video data at their request;

32.4. the destruction or suspension of the processing of the video data of the Data Subject shall be carried out on the basis of documents confirming the identity of the Data Subject and their personal data, upon the request of the Data Subject or their authorised representative;

32.5. the University shall promptly inform data recipients (if any), at the latest within ten working days, of the destruction of the Data Subject's video data at the request of the Data Subject or their authorised representative, or the suspension of the processing of the personal data, unless it would be impossible or excessively burdensome to provide such information (due to the large number of data subjects, the length of the data period, or the unreasonable costs). In this case, the State Data Protection Inspectorate must be notified immediately.

33. The University shall have the right to refuse to exercise the Data Subject's rights on the grounds that the Data Subject's request is manifestly unfounded or disproportionate, where it is necessary for the security or defence of the state, public order, the prevention or investigation of criminal offences or in similar cases.

CHAPTER VIII
FINAL PROVISIONS

34. Employees who are authorised to process video data or who become aware of it in the course of their duties are obliged to sign the Commitment to Keep Personal Data Secret (Annex to the Description of the Procedure for the Processing of Personal Data at Vilnius University), to comply with the signed Commitment, the Description of the Procedure for the Processing of Personal Data at Vilnius University, the basic requirements for the processing of personal data, as well as the requirements for confidentiality and security as laid down by the GDPR, the ADTAĮ, this Description, and other legal acts of the University regulating the processing of data. Employees who violate the procedure set out in the Description and/or personal data protection legislation shall be held liable in accordance with the procedure laid down by law.

35. Once approved, the Description shall be made available to employees carrying out video surveillance in a manner that ensures its non-repudiation (by means of a document management system), and to those who do not have computerised workplaces, by signature.

36. When a new video surveillance employee is recruited, they must be familiarised with the Description on the first day of their employment. The employee's immediate superior shall be responsible for familiarising them with the Description.

37. This Description shall be reviewed at least once every two years.

38. In the event of changes in the legislation governing the processing of video data, the Description shall be updated within the time limits set out in the legislation.

_____