APPROVED BY
Order No. R-316 as of 25 May 2018
of the Rector of the Vilnius University

DESCRIPTION OF THE PROCEDURE OF PERSONAL DATA PROCESSING AT THE VILNIUS UNIVERSITY

CHAPTER I
GENERAL PROVISIONS

1. The Description of the procedure for personal data processing at the Vilnius University (hereinafter – the Description) sets out the requirements for personal data processing and protection, purposes of personal data processing, data subjects' rights and their implementation, technical and organisational measures of data protection.

2. This Description is prepared 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 – GDPR), the Republic of Lithuania Law on Legal Protection of Personal Data (hereinafter – LPPDL), the Labour Code of the Republic of Lithuania and other legal acts.

3. This Description is necessary for all University employees, students to accept internships at the University, trainees and other persons performing functions or activities at the University.

4. The terms used in this Description shall be understood as they are defined in the GDPR, LPPDL and other legal acts.

5. Personal data of data subjects are processed by the data controller – Vilnius University, legal entity code – 211950810, registered office address – Universiteto g. 3, LT-01513 Vilnius.

6. The provisions of this Description may not expand or narrow the scope of the LPPDL and the GDPR and may not conflict with the requirements for the processing of personal data established by the LPPDL and the GDPR and other legal acts regulating the processing of personal data.

CHAPTER II
PURPOSES OF PERSONAL DATA PROCESSING

7. Personal data at the University are processed for the following purposes:

7.1. For the administration of the study process (registration of the students admitted to the University, concluding study agreements, organisation and implementation of the study process, issuance of study completion documents, student records) the following data are processed: name, surname, personal code, date of birth, number of the identity document (optional), sex, address, telephone number, email address, citizenship, marital status, work experience, social status (belonging to a socially disadvantaged group), military service, education data (name, type and code of the school graduated, year of graduation, country), data related to studies (study cycle, form, faculty, programme, year, semester, group, type of student, nature of funding, amount and year of the State-supported grant for studies, student card number, completed course units, form of assessment, date, evaluation of learning outcomes), other data in the diploma document, student identification numbers, bank account number, payments made and/or received, their amounts and dates, type of document issued to the student, its serial number and expiration (issuance) date, video and (or) sound recordings of distance learning and assessment activities.

7.2. For the administration of the research process (determining the authorship of the research output, recording and evaluating the results of employee and student research (and artistic) activity, carrying out study completion procedures at the University, filing and providing documents) the following data are processed: data subject's name, surname, personal code, personal telephone numbers, personal email address, workplace, date of birth, (work or study) institution, division of (work or study) institution, type of studies (for students), academic group (for students), study commencement date (for students, students-residents, doctoral students), study completion date (for

students, students-residents, doctoral students), personnel group (for employees), job position, academic degree (for employees), date of research work commencement and completion and/or date of defence, language of the final paper or thesis, topic of the final paper or thesis, topic of the final paper or thesis in English, summary of the final paper or thesis in Lithuanian and English, positions of the participants of the thesis defence process and their identification data, access status of the final paper or thesis on the internet, time limit, date of publication, indication of the text-matching check of the final paper or thesis, significance of the text-matching check of the final paper or thesis, data used to identify the person who carried out the text-matching check, documents of the final research paper, video and (or) audio recording of the defense committee meeting.

7.3. For internal administration (management of structure, management of information about current and former employees, document management, management of available material and financial resources) the following data are processed: name, surname, citizenship, address, personal code, date of birth, sex, photograph, signature, marital status, contacts in case of emergency (optional), names and surnames of family members and dependents and their personal codes, personal social insurance certificate number, sums of wages and social insurance contributions, data about voluntary insurance contracts, dates of state insurance, data about participation in pension schemes, current account number, telephone number, email address, curriculum vitae, job position, data about recruitment (transfer) and dismissal, work experience, position the person desires to be appointed or transferred to, employees' time-card identification number, data about education and qualifications, academic titles, identification code in the Educators Register, date of data input (modification), data about vacations, data about business trips, data about individual work schedule, data about wages, benefits, compensations, allowances, information about work periods, information about incentives and penalties, official misconduct and breach of work duty, data about employees' performance evaluation, data about declaration of public and private interests, , passport and (or) identity card number (s), date of issue, date of validity, the institution that issued the document, the date and number of registration of documents, previous place of work and position, former surname, numbers of acquired scientific certificates, car registration number (if applying for a parking permit at the University car parks) and other personal data provided by the person. Special categories of personal data related to health, criminal record (for certain positions) and other personal data provided by the person himself/herself and (or) required to be processed by laws and other legal acts may also be processed. The data are processed in the information system for the entire period of the employment relationship and for 10 years after the end of the contractual relationship. Personnel administration orders are kept for 50 years.

7.4. For ensuring the security of Library readers and visitors, the security of property on the basis of legal obligations, contracts, consent and / or legitimate interest, the following data are processed: name, surname, residence address, telephone number, e-mail number and personal identification number. The data are processed in the information system for the entire period of service provision and for 3 years after full fulfillment of mutual obligations.

7.5. For administering the user account and identity check the following personal data are processed: name, surname, personal identification number, biometric data of the data subject (with separate information and consent of the data subject), personal telephone numbers, degree, student card number (for students), tabular employee identification number (for employees), electronic identity number (username), e-mail address, institution (work or study), password reminder data, computer IP and MAC address, date and time of connection to the system or website, cookies, sessions and other activity record information that may also be used to investigate potential information, cyber and personal data protection incidents. In the event of termination of the contractual or other legal relationship with the data subject, the use of the account shall be suspended as soon as it becomes known, but not later than within 14 calendar days.

7.6. For the purpose of monitoring and surveillance of electronic communications flows, on the basis of a legal obligation, users' actions in information systems and networks are automatically recorded in action logs. The data specified in Annex 1 to this Law shall be processed on the basis of the requirements of the Law on Electronic Communications in order to ensure the availability of data for the investigation, detection and prosecution of serious and very serious crimes as defined in the Criminal Code of the Republic of Lithuania. Unless otherwise specified by law enforcement

authorities, these data shall be processed for 6 months, except for the categories of data specified in the law, and shall be destroyed upon expiry of the established term.

7.7. For organising conferences and other events the following data are processed: name, surname, personal identification number, personal telephone numbers, current account number (for natural persons transferring paymets), personal e-mail address, place of work, date of birth, institution (work or study), department of the institution (work or study), position, pedagogical and academic names, degree, e-mail address, data of identity documents used for identification of the conference participant, video and audio recordings of the conference, data of provided services.

7.8. For accommodation purposes the following data are processed: name, surname, personal identification code, telephone numbers, other data for financial settlement purposes, e-mail address, degree, home address, e-mail address, used for personal identification identity document data, place of accommodation, dates of the period, car number and model, if the car will be parked, data on the related accommodation services provided. The data is stored for 5 years after the provision of services.

7.9. For financial settlements the following data are processed: data subject's name, surname, personal identification number, telephone numbers, current account number (for natural persons-beneficiaries), credit card number and validity period, e-mail address, organization or institution represented, position, degree, e-mail address, identity the data of identity documents used, the data of the provided services are determined. The data is stored for 10 years.

7.10. For the administration of candidates the following data are processed: photo, personal telephone numbers, e-mail address, address of residence, current and former place of employment, date of birth, institution of study (current or former), position, degree and other personal data voluntarily provided by the candidate. These data shall be processed throughout the selection process, but no later than 1 year after the end of the selection and at the end of the period, if the entity is not employed and has not given its consent to the processing for other positions. The data of the selected candidates shall be processed throughout the period of employment and shall be processed in accordance with the procedures and within the time limits laid down for the data processed for internal administrative purposes.

7.11. For the investigation of personal complaints, requests and applications the following data are processed: data subject's name, surname, personal code, address, telephone number, email address, signature, date and number (number of registration in the University Document Management System) of the complaint, request or application, information (including specific personal data) provided in the complaint, request or application, outcome of the investigation of the complaint, request or application, information obtained during the process of investigation of the complaint, request or application, date and number of the University's reply to the complaints, requests or applications. The data are processed throughout the administration of the complaint or request and for 1 year after the decision (response) has been taken.

7.12. For the purpose of public order and passage control (to ensure the security of employees, students and other visitors to the University and the property of the University) the following data are processed: name, signature, employee identity number, time of arrival and departure from the building/auditorium/parking lot, date, vehicle registration number, security video surveillance camera records and photos. Video surveillance and access control at the University are carried out to ensure the safety of persons, property, visitors, public order in the University premises and territory. Security cameras are filmed in the yards of the University, at the entrances to the University buildings, common areas, network or engineering system equipment concentration points (server rooms, communication nodes, building management system control panels, etc.). Video data is recorded and stored for a maximum of 60 days and is destroyed at the end of this period. If the video data is used as evidence in civil, administrative or criminal proceedings or in other cases provided for by law, the video data may be stored for as long as is necessary for these purposes of data processing and destroyed immediately when they are no longer needed.

7.13. For communication with the community the following data are processed: contact person's name, surname, academic, pedagogical names, scientific degrees, telephone number (s), date of birth, address of residence, e-mail address (es), social network contacts (when provided), represented company, position, address correspondence, data on membership in University societies

and collectives, communication choices and consents. These data are processed for the duration of the contractual relationship.

7.14. For ensuring the operation of the Mobile University applications on the basis of user consent, agreements and the University's legitimate interest: user account data (contact name, unique identifier), user-selected language (LT, EN), notifications and news subscription consents, reminders order details and related arrears data, consent for anonymous gadget usage statistics. These data are processed in the information system as long as the application is used, but not less than until the full fulfillment of the obligations of the parties. After fulfilling all obligations and refusing to use the mobile application, the data is stored in the information system for 3 years.

7.15. For marketing purposes, on the basis of the data subject's consent and the legitimate interest of the University to inform members of the community and the public about University events, services and goods offered (University academic and other expert services, paid University events, museums, botanical gardens and other tickets, University advertising on social networks and etc.), contact details are collected and processed: e-mail. email address, social networking contacts (when provided), name, phone number (s), address, videos to market the event and publicize the results. Contact details are retained until consent is revoked.

7.16. Data confirming the disability, working capacity, health disorders and individual needs of students and listeners with disabilities are processed on the basis of the individualisation of studies and the adaptation of the environment to individual needs arising from the purpose of disability, consent and legal requirements. Documents containing health data of students and listeners with disabilities are stored in the information system and personal files for the entire study period and for 5 years after the fulfillment or termination of obligations under the study contract. When the deadline expires, the data is deleted in the prescribed manner.

7.17. For the purpose of public procurement, on the basis of legal requirements, data of service providers, their representatives and other persons specified in public procurement documents (name, surname, position, individual activity certificate or business certificate number, business address, telephone number, e-mail address and current account data, contract revenue, data or copies of documents proving education and qualifications (certificates, licenses, etc.) as well as other personal data of an economic or social nature provided by the person himself/herself shall be processed for the purpose of execution and administration of public procurement contracts. The data is stored for 5 years after the end of the procurement.

7.18. For the purpose of administration of the University's art groups, on the basis of agreements and consent, personal data, name, e-mail, telephone, date of birth, study program, course, faculty, photos, audio and video recordings are collected and processed. The data is processed throughout the period of participation in the activities of the art collective.

7.19. The University uses cookies to make the use of websites faster and more convenient. Cookies are collected about the use of services and website traffic statistics. Cookies on the website are used with the consent of the person, which the person can cancel at any time by changing the settings of their web browser. The list of cookies used and the duration of their storage is specified in the University's privacy policy.

7.20. Personal data contained in documents held in the University archives are processed in the public interest, as well as for scientific or historical research or statistical purposes.

8. All personal data is stored at the University for no longer than required by the purposes of personal data processing. The time limits for the storage of personal data and the actions to be taken after this time limit shall be determined by the legislation governing the processing of the personal data concerned. Specific terms of storage of documents related to studies, research processes and internal administration are set in the Index of Terms of Storage of Vilnius University Activity Documents approved by the Order No. R-481 as of 9 August 2019 of the Chancellor of Vilnius University "On the Approval of the Index of Terms of Storage of Vilnius University Activity Documents and the Order No. R-545 as of 30 October 2013 of the Rector of Vilnius University "On the Recognition of the Approval of the Index of Terms of Storage of Vilnius University Special Activity Documents", in the annual documentation plans of the University and in other legal acts of the University.

9. At the end of the retention period of a document containing personal data, a decision shall be made on its destruction or extension of the retention period. Upon the decision to destroy the document, the document shall be destroyed in accordance with the procedure established by the Law on Documents and Archives of the Republic of Lithuania, except for those which must be transferred to the archives and are stored in accordance with the law.

CHAPTER III
DUTIES OF SUBJECTS PARTICIPATING IN DATA PROCESSING

10. The University as a data controller shall:

10.1. ensure the implementation of data subject's rights and carry out the duties of personal data controller specified in general requirements for organisational and technical personal data protection means and other legal acts regulating personal data processing;

10.2. appoint a data protection officer and other persons responsible for personal data processing at the University;

10.3. ensure the data protection officer's authorisation to reply to the data subjects' complaints and requests and his/her appropriate and timely involvement in the examination of all issues related to personal data protection;

10.4. provide the necessary resources for the data protection officer to carry out his/her tasks;

10.5. provide the opportunity for the data protection officer to maintain his/her expertise in the area of personal data protection;

10.6. ensure that the data protection officer receives no instructions concerning the execution of assigned personal data processing tasks, and assign no tasks or duties likely to cause a conflict of interests;

10.7. approve legal acts regulating personal data protection and processing;

10.8. establish a procedure of the disclosure of data to data subjects for a fee;

10.9. ensure training and qualification upgrading for employees in the area of legal protection of personal data.

11. The University divisions involved in personal data processing shall:

11.1. ensure compliance with the principles of personal data processing:

11.1.1. personal data processing shall be in compliance with GDPR, LPPDL and other normative and University legal acts regulating data protection;

11.1.2. personal data shall be collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

11.1.3. personal data shall be processed accurately, fairly and lawfully;

11.1.4. personal data shall be accurate and, where necessary, kept up to date; data that are inaccurate or incomplete must be rectified, supplemented, erased or their processing must be suspended;

11.1.5. personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

11.1.6. personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are collected and processed;

11.2. ensure that personal data are processed in accordance with the organisational and technical data protection measures specified in the documents of the managed information systems (regulations, data security regulations, rules of secure processing of electronic information, user administration rules);

11.3. familiarise the employees of the division with the Description by means of University Document Management System or any other means providing verifiability of access;

11.4. be responsible for the preparation of documents (orders, agreements, protocols, contracts, reports, etc.) necessary for personal data processing, their registration and submission to the data protection officer at the University in accordance with the procedure established by law (for the implementation of data subjects'rights);

11.5. ensure the destruction of electronic and (or) paper documents containing personal data upon expiration of the set term for personal data safekeeping;

11.6. in consultation with the data protection officer, carry out a data protection impact assessment of the Order no. 1T-35 (1.12.E) as of 14 March 2019 of the and the Director of the State Data Protection Inspectorate of the State Data Protection Inspectorate "List of data processing operations subject to a data protection impact assessment" and General Data Protection Regulation;

11.7. consult the Data Protection Officer when processing personal data for new purposes or changing the scope of previous processing;

11.8. keep records of the data processing activities of the unit and ensure their accuracy;

11.9. ensure the implementation of appropriate organisational measures, including protection of personal data processed by the division against accidental loss or unlawful destruction, damage, disclosure as well as against unlawful processing.

CHAPTER IV
DATA PROTECTION OFFICER

12. The data protection officer shall be responsible within his/her competence for the data processing operations at the University.

13. The data protection officer shall:

13.1. monitor compliance with this Description in relation to the performance of personal data processing duties by staff and other processors of personal data controlled by the University involved in processing operations;

13.2. in accordance with the established procedure make public the information about the data processing operations carried out by the data controller;

13.3. inform and advise the University management concerning data protection and data processing measures, monitor the implementation and use of these measures;

13.4. give direct instructions to staff to eliminate any violations in the processing of personal data;

13.5. familiarise the employees authorised to process personal data with the provisions of legal acts regulating personal data protection;

13.6. initiate and organise assessment of the data processing impact;

13.7. assist data subjects in exercising their rights;

13.8. consult personal data processors on personal data processing and protection issues;

13.9. be responsible for the preparation of records of data processing operations;

13.10. decide as regards the need for the data protection impact assessment and carry out the assessment. When necessary, the data protection officer shall apply to the State Data Protection Inspectorate for advance consultations;

13.11. in case of accidental destruction of personal data take possible measures to recover the lost personal data and/or to reduce the damage to personal data caused by the incident;

13.12. in specified cases notify the data subject and the State Data Protection Inspectorate about the incident related to personal data;

13.13. ensure secrecy or confidentiality in relation to the execution of his/her tasks in accordance with the requirements laid down in the legal acts of the European Union and the Republic of Lithuania;

13.14. notify the State Data Protection Inspectorate in writing upon establishing that personal data are processed in violation of the provisions of legal acts regulating data protection or direct instructions to rectify these violations are ignored;

13.15. carry out other tasks and duties assigned by legal acts.

CHAPTER V
PERSONAL DATA PROCESSING

14. At the University personal data are processed by automated means or by using personal data processing means installed in the filing systems.

15. At the University personal data are collected in accordance with the procedure established by legal acts by receiving them directly from the data subject, by officially requesting the necessary information from authorised subjects or on the basis of contracts. In some cases personal data at the University are processed upon receipt of the data subject's consent.

16. When personal data are collected directly from the data subject, the following information must be provided (unless the data subject already has such information at his/her disposal):

16.1. the data controller's address, telephone number, email address;

16.2. the purposes for which the processing of the data subject's personal data is intended;

16.3. the type of the data subject's personal data to be collected;

16.4. the consequences of the failure to provide personal data;

16.5. the recipients of the data subject's personal data and the purposes of disclosure;

16.6. the data subject's right to have access to his/her personal data and the right to request rectification of incorrect, incomplete or inaccurate personal data.

17. When personal data about the data subject are obtained not directly from the data subject or when personal data are intended to be disclosed to the third parties, the data subject must be informed not later than before the moment of the first disclosure of data, unless the data subject already has such information at his/her disposal or the disclosure of data is regulated by other legal acts. The data subject must be provided with the following information:

17.1. the address, telephone number, email address of the University and data recipient;

17.2. the purposes of the processing or intended processing of the data subject's personal data;

17.3. the sources and the type of data subject's personal data which are or will be collected;

17.4. the recipients of the data subject's personal data and the purposes of disclosure;

17.5. the data subject's right to have access to his/her personal data and the right to request rectification of incorrect, incomplete or inaccurate personal data.

18. Information to the data subject shall be provided in writing (directly, by registered post or via the National information system for delivery of electronic messages and electronic documents eDelivery) and request aknowledgement of information receipt providing verifiability of access.

19. In cases specified by the GDPR the data subject has the right to withhold consent to the processing of his/her data by a third party and inform the data protection officer about his/her decision.

20. When information cannot be provided to the data subject owing to a large number of data recipients, the outdated character of the data and excessively large expenses, the data subject must be notified.

21. In the cases and in accordance with the procedure established by legal acts personal data processed by the University shall be disclosed to the Ministry of Education and Science of the Republic of Lithuania, Ombudsman for Academic Ethics and Procedure of the Republic of Lithuania, State Tax Inspectorate of the Republic of Lithuania, Special Investigation Service of the Republic of Lithuania, State Security Department of the Republic of Lithuania, State Social Insurance Fund, National Cybersecurity Centre of the Republic of Lithuania**,** Communications Regulatory Authority of the Republic of Lithuania and other third parties upon request (in case of single collection of personal data) or according to personal data disclosure contract (in case of multiple collection of personal data).

22. Personal data to data recipients located in the European Union Member states or in other states of the European Economic Area are disclosed under the same conditions and in accordance with the same procedure as to data recipients located in the Republic of Lithuania.

23. Personal data processed or intended to be processed after disclosing them to a third country or international organisation shall be disclosed only in case the data controller and the data processor comply with the provisions of the GDPR.

24. When the University concludes a written data disclosure contract with the data processor, the contract must specify the following information:

24.1. to identity the purpose of personal data use and the legal basis for data transfer and disclosure;

24.2. to establish that a personal data processor may act only on instruction from the data controller;

24.3. to determine legal acts and standards regulating personal data processing;

24.4. to set purposes and manner of personal data processing;

24.5. to provide the final list of the personal data to be processed;

24.6. to define what personal data processing acts the data processor must or may perform on behalf of the data controller;

24.7. to define in what manner and in what cases personal data are to be rectified or updated, how the altered data are to be processed, etc.;

24.8. to determine the procedure of implementation of the data subject's rights;

24.9. to envisage time limits for personal data safekeeping (including active and passive data base) and actions performed after the expiration of the period;

24.10. to ensure adherence to the confidentiality requirement;

24.11. to determine the application of organisational and technical measures for ensuring the security of personal data;

24.12. to determine liability for the breach of contract.

25. The data recipient shall ensure the implementation of appropriate organisational and technical measures for the protection of personal data against accidental or unlawful destruction, alteration, disclosure as well as against any illegal processing.

26. The personal data protection measures of the data processor shall be in compliance with the requirements established in the University security documents.

27. In accordance with the provisions of GDPR, the University may process the collected personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

28. The University shall process the data no longer than is necessary for the purposes of data processing.

29. In accordance with the University legal acts, the divisions shall destroy the unnecessary data (documents containing personal data or their copies) collected by non-automated means in such a manner that the data become unidentifiable, and the data collected by automated means shall be destroyed by erasing personal data files from storage in such a manner that makes their recovery impossible.

CHAPTER VI
RIGHTS OF THE DATA SUBJECT

30. The data subject whose data are processed during University activities shall have the following rights:

30.1. to know (be informed) about the processing of his/her personal data (the right to be informed);

30.2. to have access to his/her personal data and to be informed of how they are processed (the right of access to the information);

30.3. to request rectification or, with regard to the purposes of personal data processing, completion of incomplete data (the right to rectification);

30.4. to destroy his/her personal data or to suspend further processing of his/her personal data (with the exception of storage) (the right to erase and the right to be forgotten);

30.5. to demand that the data controller restricted personal data processing (the right to restrict processing);

30.6. to request the transfer of data (the right to transfer).

31. The data controller shall not provide the data subject with the conditions for exercising the above rights in the cases laid down in laws when it is necessary to ensure prevention, investigation and detection of criminal offences, violations of official or professional ethics as well as protection of the rights and freedoms of the data subject or other persons.

32. A data subject has the right to appeal directly to the stem divisions of the University or the data protection officer concerning all issues relating to the processing of the data subject's personal data and the rights of the data subject set out in GDPR, LPPDL and other related legal acts.

33. A data subject has the right to obtain information on the sources and type of his/her personal data which have been collected, the purpose of their processing and the data recipients to whom the data are disclosed or were disclosed at least during the past year.

34. A data subject has the right to request that the University should erase his/her personal data without delay if the request may be justified by one of the following reasons:

34.1. personal data are no longer necessary to achieve the purposes the data were collected or processed for;

34.2. the data subject withholds his/her consent to data processing referred to in paragraph A part 1 of Article 6 or paragraph A part 2 of Article 9 of GDPR and there is no other legal basis for data processing;

34.3. the data subject objects to data processing referred to in part 1 of Article 21 of GDPR and there are no superior legal reasons to process data or the data subject objects to data processing referred to in part 2 of Article 21;

34.4. personal data have been processed unlawfully;

34.5. personal data shall be erased in compliance with legal requirements set for the data controller in the law of the EU or a Member State;

34.6. personal data have been collected in the context of the tender of information society services defined in part 1 of Article 8 of GDPR.

35. A reply to the data subject's request or complaint concerning their personal data processing shall be provided free of charge not later than within 30 calendar days from submission of the request, except in the cases and circumstances defined by GDPR and other legal acts, in particular in part 3 of Article 12 of GDPR when with regard to the complexity of the request and the number of other requests this period may be extended for 2 more months.

36. The University shall disclose such data to the data subject free of charge once per calendar year. In other cases data are disclosed according to the service charges and payment procedure determined by the University.

37. Where a data subject, after familiarising with his/her personal data processed by the University disclosed in the reply, finds that his/her personal data are incorrect, incomplete or inaccurate and applies to the University concerning their rectification, the data protection officer must suspend the processing operations of such personal data, except storage, check the personal data concerned no later than within 5 working days and take measures to rectify the incorrect, incomplete and inaccurate personal data, and notify the data subject about the actions performed.

38. Where a data subject, after familiarising with his/her personal data processed by the University disclosed in the reply, finds that his/her personal data are processed unlawfully or unfairly and applies to the University, the data protection officer must check the accuracy, lawfulness and fairness of the processing of personal data no later than within 5 working days and take measures to destroy the personal data collected unlawfully and unfairly or suspend processing of such personal data, except storage, without delay, and notify the data subject about the actions performed.

39. Where a data subject, after familiarising with his/her personal data processed by the University disclosed in the reply, finds that further processing of his/her personal data is no longer necessary, withdraws the previous consent to data processing and applies to the University with the request to be forgotten, the data protection officer shall take measures to destroy the personal data processed upon previous consent, except storage, and shall notify the data subject about the actions performed or inform him/her why the data cannot be destroyed.

40. Where the University has performed public disclosure of the data subject's personal data, but upon the data subject's request must erase his/her personal data, the data protection officer with regard to the technologies used by the University and the implementation costs shall take reasonable actions, including technical measures, to destroy such personal data and/or their copies or duplicates without delay.

41. Requirements to forget and to erase personal data are not applicable if reasons specified in the subparagraphs of paragraph 38 of this Description cannot be justified, and in the cases specified in part 3 of Article 17 of GDPR, including where:

41.1. legal obligations are imposed upon the University to process data or in order to perform a task in the public interest;

41.2. for archiving purposes in the public interest, for statistical, historical or scientific research purposes in compliance with the requirements set out in GDPR and other legal acts;

41.3. in other cases specified by GDPR and other legal acts.

42. When, at a data subject's request, the processing of his personal data is suspended, the University must store the personal data concerned until they are rectified or destroyed (either at the data subject's request or upon expiry of their storage period).

43. A data subject has the right to submit a complaint to the State Data Protection Inspectorate concerning the actions (inaction) of the University.

44. A data subject has the right to request compensation from the University for pecuniary and non-pecuniary damage sustained due to unlawful processing (inaction) of personal data.

45. The University must ensure the appropriate implementation of the data subject's rights and the provision of information in a clear, comprehensible and acceptable form. The purposes of personal data processing, the data subjects' rights and their implementation set out in this Description are laid down in a simplified form in the University Privacy Policy published on the University internet and intranet websites.

CHAPTER VII
EXERCISING OF DATA SUBJECTS' RIGHTS

46. In order to exercise his/her rights, a data subject submits a personal written request or complaint relating to the personal data processing issues addressed to the University data protection officer.

47. The University employees submit their requests or complaints via the University Data Management System.

48. Former University empoyees, current and former students, and other data subjects submit their requests or complaints at the University stem division processing the data subject's personal data, the Document Management subdivision of the Lawmaking division of the University Central Administration, User Services subdivision of the Information Technologies Assistance division of the Information Technology Service Centre, as well as by registered post or via the National information system for delivery of electronic messages and electronic documents eDelivery.

49. The request must be legible and signed, must contain the data subject's name, surname, address and other contact details to maintain communication of the preferred form, information specifying the data subject's right and the scope of its implementation.

50. A data subject may exercise his/her rights only after providing the University with an opportunity to check his/her identity. The data subject's identity shall be checked in one of the following ways:

50.1. by arriving at the University and submitting a document certifying his/her identity together with the request for exercisingg his/her rights;

50.2. in line with procedures established by legal acts or via electronic communication means which allow appropriate identification of an individual (e.g. electronic signature). When submitting his/her request or complaint at the University division, the data subject must show a document certifying his/her identity to the employee accepting the documents.

51. The employee accepting the documents must check the individual's identity.

52. When sending his/her request by registered post, the data subject must also submit a copy of the document certifying his/her identity approved by a notary public or by equivalent or simplified procedure as established in the Civil Code of the Republic of Lithuania and other legal acts.

53. Requests and complaints sent by unregistered post or lacking a return address are investigated in line with general procedures but not replied to in writing.

54. A data subject may exercise his/her rights personally or through a legally authorized representative.

55. If a representative applies on behalf of the represented data subject, he/she must provide his/her name, surname, place of residence, contact details for communication, as well as the represented individual's name, surname, place of residence, information specifying the data subject's right listed in the Description and the scope of exercising requested and attach a document confirming representation or a copy of the document approved in accordance with the procedures set by legal acts. The representative's request must satisfy the same requirements as set out for the request of the individual represented.

56. All data subjects' requests and complaints concerning personal data processing as well as replies must be recorded in a general file for individual requests and complaints on personal data issues and their investigation in the division registers of received documents in the University Document Management System.

57. A data subject's request or complaint submitted without regard to the requirements laid down in this Description shall not be investigated, except for cases where the data protection officer decides otherwise. The data protection officer notifies in writing the individual who has submitted the request or complaint about the motives for the refusal to investigate the request or complaint.

58. Replies to individuals' requests or complaints shall be in the state language using the same means of communication that was used to submit the request or complaint, if the individual has not specified another preference.

59. Where the request has been submitted by an institution of a foreign state, another foreign subject or an international organisation in accordance with international legal acts, the reply may be in a language other than the state language, if necessary.

60. The preparation of the reply to a request or complaint shall be coordinated, the divisions shall be consulted and the reply to the data subject shall be provided by the data protection officer or another person authorised by the Rector in accordance with the procedure established by the legal acts of the University.

61. The reply to the data subject shall be signed by the data protection officer or another person authorised by the Rector of the University.

61.1. Replies to the request shall be prepared with regard to its subject matter:

61.2. a reply to the request to obtain a document, its copy, transcript or excerpt shall be provided in the form of a requested service or the indication of reasons for refusal;

61.3. a reply to the complaint shall include information concerning the circumstances investigated or the indication of reasons for refusal;

61.4. a reply to the request for access to the information held by the University shall provide the requested information in accordance with the procedure established by the Law on the Right of Access to Information from State or Municipal Institutions and Organisations of the Republic of Lithuania or the indication of reasons for refusal;

61.5. a reply to the application expressing personal opinion on a certain issue, reporting on operational weaknesses of the University or its division, providing recommendations for improvement, drawing attention to a certain situation, informing about the misconduct and malpractice of the employees unrelated to the breach of lawful interests and rights of a specific person, or any other personal application shall be an written reply of a free form;

62. a reply to the request or complaint shall provide clear arguments indicating the circumstances that influenced the investigation and specific provisions of legal acts taken into account when assessing the subject matter of the request or complaint;

63. a reply which indicates reasons for the refusal to provide the requested service or information shall inform the individual or his/her representative of the procedure of making an appeal by indicating the name and address of the institution(s) to which the appeal may be lodged as well as the time period within which the appeal shoud be lodged. In the cases when the request or complaint is forwarded for investigation to another competent authority and the individual or his/her representative is informed, the reply shall not indicate the mentioned procedure for appeal.

64. Information on personal data processing issues that is missing in the information systems managed by the University shall be collected by the University divisions processing the data

subject's data and provided to the data protection officer not later than within 21 (twenty-one) calendar days from the date of the data subject's enquiry.

65. A reply to the request shall be provided within 30 (thirty) calendar days from the date of the data subject's enquiry.

66. Upon the decision of the data protection officer, in the cases specified in GDPR a reply to the request may be postponed up to 60 (sixty) days by notifying the data subject about the decision.

67. The University staff shall apply the principles of lawfulness, fairness, reasonableness and respect for human rights in their investigation of requests and complaints.

68. Investigation of requests or complaints may not be refused on the grounds of absence of the employee who performs that function. In the cases of the said employee's vacation, business trips or other absences from work the tasks to investigate requests and complaints shall be assigned to other employees.

69. The employee investigating a request or complaint shall withdraw from the investigation of the request or may be dismissed by the Rector or an authorised person in cases when:

69.1. the data subject submits a request or complaint in relation to the activities of the University employee processing personal data or some relevant circumstances arise;

69.2. the employee is a close relative (as defined in the Civil Code of the Republic of Lithuania), in-law or partner, who has registered the partnership in accordance with the procedure laid down by law, of the person who is the subject matter of the complaint investigation;

69.3. the employee and the person submitting a request or complaint are in a subordination relationship;

70. the impartiality of the employee raises reasonable doubt owing to certain reasons which may result in the conflict of public and private interests.

71. The copies of the documents received in relation to the data subject's request or complaint shall be destroyed within 6 (six) months from the end of the investigation of the complaint. Complaints, requests and the investigation documents shall be stored for 1 (one) year and destroyed after the specified safekeeping period in accordance with the procedure established by legal acts.

72. Documents containing personal data or copies of those documents in external data files or electronic mail shall be erased without delay after their use and/or transfer to storage but not later than within 5 (five) working days after the request or complaint has been acted upon.

73. Documents containing personal data or copies of those documents shall be destroyed in a manner preventing their recovery or content recognition.

CHAPTER VIII
ORGANISATIONAL PERSONAL DATA PROTECTION MEASURES

74. Personal data (documents containing personal data or copies of those documents) are kept safe on designated premises, areas of internal network, and hard discs of computers. Personal data (documents containing personal data or copies of those documents) shall not be kept in sight in publicly accessible area where unauthorized persons are able to access the data.

75. Upon the rotation of employees processing personal data (documents containing personal data or copies of those documents) or change of their authorisations, personal data (documents containing personal data or copies of those documents) shall be transferred to newly employed staff authorized to process personal data upon signing the acceptance of transfer document.

76. The employee processing personal data shall:

76.1. familiarise with this Description via the University Document Management System or any other means providing verifiability of access, sign the Commitment to Protect the Confidentiality of Personal Data (Appendix to the Description);

76.2. adhere to the provisions of this Description and the Commitment to Protect the Confidentiality of Personal Data;

76.3. adhere to confidentiality requirements and shall not disclose to the third parties any information related to personal data that he/she obtained by carrying out his/her functions, unless such data are considered public with regard to the provisions of existing laws and other legal acts; this obligation remains valid after the termination of employment or contractual relations;

76.4. notify the data protection officer and the head of the structural division without delay about any breach of personal data protection at the University;

76.5. notify without delay about any electronic information protection incidents in accordance with deadlines and means specified in the University procedure for the investigation of electronic information incidents;

76.6. change the password without delay if there is a threat of hacking into a computer with protected personal data or a suspicion that a password became known to the third parties, etc.;

76.7. avoid making excess copies of documents containing personal data or keeping those documents in sight in publicly accessible area and ensure proper protection;

76.8. ensure that documents containing personal data are protected in accordance with the requirements of legal acts;

76.9. notify the head of the structural division of the University and the data protection officer if the employee evaluates and determines the organisational and technical personal data protection measures to be unreliable.

77. The commitment to protect the confidentiality of personal data shall be signed in the presence of the head of the division, with the exception of cases when it is signed by electronic means ensuring non-repudiation.

78. The heads of the structural divisions of the University shall ensure protection against unlawful physical acces to personal data by the following means: locked premises, an operating (physical or electronic) entrance control system, restricted acces to certain premises or other risk reduction measures.

79. Personal data protection breaches at the University shall be investigated in accordance with the procedure established in the Description of the procedure for the investigation of electronic information protection incidents.

80. The protection of personal data processed in the University information systems shall be ensured in accordance with the requirements of the University information systems provisions and the documents implementing protection policy, including data protection provisions, rules for secure processing of electronic information, sustainability management plan, and user administration rules.

CHAPTER XII
FINAL PROVISIONS

81. The Description shall be periodically, at least once in 2 (two) years reviewed and updated, if necessary.

82. The heads of University divisions shall ensure that employees are notified about the updates of the Description.

83. Notification about the updates of the Description shall be iniciated by the data protection officer.

84. Persons who do not adhere to the requirements of personal data processing and protection established in GDPR, LPPDL, other legal acts, this Description and other legal acts of the University shall be liable for non-compliance in accordance with the rules of the University work procedure and other legal acts.

85. The data protection officer shall carry out the audit of organisational and technical protection means of personal data processing at least once in 2 (two) years.

86. The Description shall be published on the University internet and intranet websites.

87. Legal acts implementing the Description shall be approved by the order of the Rector or an authorised person.

_____

Appendix to the Description of the procedure of personal data processing at the Vilnius University for internal administration purposes

(the sample form of the Commitment to Protect the Confidentiality of Personal Data)

COMMITMENT TO PROTECT THE CONFIDENTIALITY OF PERSONAL DATA

_____
(date)

_____
(place)

I, _____ ,
(name, surname)

_____ ,
(position)

hereby **confirm** that I am acquainted 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), Law on Legal Protection of Personal Data of the Republic of Lithuania, the Description of the procedure of personal data processing at the University of Vilnius and other legal acts regulating personal data protection, and undertake:

1. to protect the confidentiality of personal data during the term of employment (contractual relations) and after the termination of employment (contractual) relations, unless these personal data are meant to be made public;
2. to process personal data only for lawful purposes;
3. to process accurate personal data and, where applicable, update them regularly, rectify or supplement incorrect or incomplete data and/or suspend the processing of such personal data;
4. to process personal data of such scope that is necessary for their processing and carrying out the necessary function (including not keeping the copies of the processed data, unless required by the existing legal acts);
5. to process personal data in a manner that allows the identification of data subjects no longer than is necessary for the purposes for which they are processed, and later to destroy those data;
6. to implement the provisions of legal acts regulating personal data protection envisaging ways of protecting personal data against unlawful processing or disclosure;
7. not to disclose or transfer the processed information nor create conditions by different means to access it by any person who is not authorised to use this information either in or outside the University;
8. to notify my immediate superior about any suspicious situation that can pose a threat to the security of personal data;
9. to ensure the implementation of the data subject's rights in accordance with the procedure laid down by legal acts;
10. to adhere to the provisions of other legal acts regulating personal data processing and protection.

Upon signing this commitment I confirm that I understand that I am liable for non-compliance in accordance with the procedure laid down in legal acts.

_____	_____	_____
(position)	(signature)	(name and surname)

The commitment was signed in the presence of*:

_____	_____	_____
(position of the head of the division)	(signature)	(name and surname)

* not completed when signed by electronic means ensuring non-repudiation.