APPROVED
by Order No. 319 of the Rector of
Vilnius Gediminas Technical
University of 2 April 2019

PERSONAL DATA PROCESSING RULES OF VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

CHAPTER I
GENERAL PROVISIONS

1. The purpose of the Personal Data Processing Rules of Vilnius Gediminas Technical University (hereinafter referred to as the Rules) is to regulate the processing of personal data, to provide for basic organizational measures for the processing of personal data and the protection of personal data.

2. The Rules were prepared according to General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as the General Data Protection Regulation), the Law of the Republic of Lithuania on the Legal Protection of Personal Data (hereinafter referred to as the Law on the Legal Protection of Personal Data), the relevant subordinate legal acts implementing these legal acts, the Personal Data Storage Policy and the Employees' Personal Data Storage Policy of Vilnius Gediminas Technical University.

3. These Rules apply and are binding on the data controller – all persons working for VGTU who process personal data or have access to it by virtue of their office.

4. The Rules are not intended to reiterate the relevant provisions of legal acts. These Rules also do not replace any other VGTU internal legal acts or procedures, but only complement them. The absence of any provision on personal data processing, which is mandatory under the General Data Protection Regulation, the Law on the Legal Protection of Personal Data or any other legal act, including VGTU internal legal acts, from these Rules does not release one from the duty to comply with and follow such provisions.

5. Terms used in the Rules:

Staff (Staff Member) shall mean a person who entered into an employment contract with VGTU, is responsible for the processing of specific personal data and/or performs individual personal data processing actions.

Data Subject shall mean a prospective, current or former employee, student or another person who submitted any personal data about himself/herself on the basis of contractual and any other legal relationships in the manner prescribed by law.

Data Protection Officer shall mean a VGTU employee or service provider hired by VGTU, performing duties imposed on the data protection officer by the General Data Protection Regulation and the Law on the Legal Protection of Personal Data with regard to data controlled and/or processed by VGTU.

Unit shall mean a higher education and research unit of VGTU of the university level (faculty, university-level higher education and/or research centre or institute), a non-academic unit.

6. Other terms used in the Rules shall be understood and interpreted as defined in the General Data Protection Regulation and in the Law on the Legal Protection of Personal Data.

CHAPTER II
PROCESSING OF PERSONAL DATA

7. Personal data shall be processed in VGTU by the Units which have been granted such a right by legal acts applicable in the Republic of Lithuania or whose work functions are related to the processing of personal data.

8. Staff of the Units performing personal data processing functions shall process the following personal data of Data Subjects under lawful grounds defined in the legal acts regulating the protection of personal data:

8.1. Basic data processed by the Staff of the Human Resources Directorate, the Admission and Information Centre, the Doctoral Studies Division, the International Studies Centre, all faculties: first name, surname, personal ID number, employee's/student's identification number, date of birth, copy of the personal identity document, telephone number, e-mail address, address and other contact details, documents confirming qualifications and experience, such as diplomas, certificates of qualification, certifications, extracts from work or learning history files, publications, data on marital status, health data.

8.2. Basic data processed by the Staff of the Finance Directorate: first name, surname, personal ID number, employee's/student's identification number, date of birth, bank account number, amount of the salary and other payments, data on scholarships, pension accumulation and other financial data.

8.3. Basic data processed by the Staff of the Occupational Safety and Health Division: first name, surname, personal ID number, date of birth, address, health data.

8.4. Basic data processed by the library Staff: first name, surname, personal ID number, employee's/student's identification number, date of birth, copy of the personal identity document, telephone number, e-mail address, address, publications, other institutional identification data.

8.5. Basic data processed by the Staff of the Studies Directorate: first name, surname, personal ID number, date of birth, e-mail address, address, documents confirming qualifications and experience, such as diplomas, certificates of qualification, certifications, extracts from work or learning history files.

8.6. Basic data processed by the Staff of the Public Procurement Division: first name, surname, personal ID number, date of birth, copy of the personal identity document, contact details, documents confirming qualifications and experience, such as diplomas, certificates of qualification, certifications.

8.7. Basic personal data processed by the Staff of the Public Communication Directorate, the Laboratory of Video and Audio Technical Instruments: first name, surname, e-mail address, image, including data from photos and/or video records, live video streaming which is collected during, but not limited to, public events.

8.8. Basic personal data processed by the Staff of the Security Service: image, including video surveillance and recording.

8.9. Basic personal data processed by the Staff of the Centre for Information Technologies and Systems: first name, surname, personal ID number, employee's/student's identification number, date of birth, telephone number, e-mail address, address, and other contact details, Internet Protocol (IP) addresses of computer hardware, and office phone data.

9. Image data processing in VGTU:

9.1. Video surveillance and recording in VGTU premises and territory shall be carried out on the basis of lawful interest to ensure the safety of all persons and property and to maintain public order.

9.2. More detailed processing of personal data by use of video surveillance and recording is defined in the Image Data Processing Rules of Vilnius Gediminas Technical University.

9.3. VGTU may involve data processors who would get access to personal data contained in a video data record, i.e. companies providing security services or companies servicing video surveillance equipment may access video data in VGTU during the provision of their services.

9.4. Public events are organized in VGTU premises and territory, during which Data Subjects can be photographed and/or filmed. This video data shall be processed for publicity purposes, taking into account the peculiarities of activities of VGTU, as a research and higher education institution, informing Data Subjects about the fact of video recording, broadcasting and photographing in the event information notice, informing additionally about it before the event starts.

9.5. Image data (including photos) of Data Subjects captured during public events organised by VGTU can be publicized in such places as social network account, website, mass media portals, and other mass media forms.

9.6. Image data captured during public events shall be stored for no longer than necessary for the purpose for which the data is processed.

10. Personal data may be processed in VGTU only for the purpose for which it is collected. Personal data shall be collected in accordance with the procedure established by legal acts, receiving it directly from the Data Subject, on the basis of an official request made to entities that process and have

the right to provide the necessary information, or on the basis of contracts. Where necessary, personal data shall be processed with the consent of the Data Subject.

11. If personal data is not necessary for a specific purpose, it cannot be processed. The amount of personal data processed to achieve a specific purpose must be as minimal as possible. Personal data that is inaccurate, having regard to the purposes for which it is processed, must be erased or rectified without delay.

12. Each Staff Member must assess, prior to each personal data processing operation (action), whether such processing of personal data complies with the data processing principles and lawfulness (reasonability) requirements established in the General Data Protection Regulation, and ensure that each data processing operation (action) complies with the said requirements, also assess whether such processing of personal data has at least one of the bases for the processing of personal data as laid down in the General Data Protection Regulation and ensure that personal data is not processed if there is none of the above-mentioned lawful bases.

13. No additional Data Subject identification data, such as personal ID number, shall be used in the VGTU internal documents unless it is necessary for identification of the Data Subject, for another lawful purpose or it is required by legal acts.

14. Personal data processed by VGTU is confidential information.

15. Each Staff Member of VGTU must:

15.1. process personal data he/she is given access to only for the purposes for which he/she is given access to such personal data;

15.2. protect personal data he/she accessed from intentional or unintentional disclosure to third parties, including colleagues, who do not have the right of access to that personal data. In performing this duty, every Staff Member must:

15.2.1. not leave any documents containing personal data in a freely accessible place unattended so that their content can be accessed by other persons (good practice is to close or cover documents so that another person who approaches during work with those documents would not be able to see personal data contained in those documents);

15.2.2. after finishing work with documents that contain personal data, put them in lockable drawers or cabinets, lock computers with password;

15.2.3. if a paper document containing personal data is sent through another person without the right of access to the personal data contained in that document, such a document must be sent in a sealed envelope;

15.2.4. if personal data is sent by e-mail, this can only be done after ascertaining that the data is sent to a known e-mail address of the addressee. The e-mail must contain a statement about the recipient's duty of confidentiality. Personal data transmitted by e-mail must be encrypted and password protected, and the password must be provided to the addressee separately from personal data;

15.2.5. before disclosing personal data to other persons, one must always make sure that there is a lawful basis for such disclosure, also must get informed about the purpose of the disclosure.

16. In case of non-standard situations regarding the processing of personal data (individual data processing actions) or the exercise of Data Subjects' rights, the Staff shall consult the VGTU Data Protection Officer (hereinafter referred to as the DPO).

17. The DPO shall keep records of VGTU data processing activities in accordance with the information provided by the heads of the Units as to which personal data is processed and transferred and for what purposes. Records of data related activities shall be kept in accordance with the legal acts in force in the Republic of Lithuania and the recommendations of the State Data Protection Inspectorate (hereinafter referred to as the SDPI).

CHAPTER III
INFORMING THE DATA SUBJECT

18. A Staff Member, before collecting personal data directly from the Data Subject, regardless of the way in which it is collected, shall ensure that the Data Subject is provided with the information

provided for in Article 13 of the General Data Protection Regulation regarding the intended processing of his/her personal data. Such information may be provided by familiarizing the Data Subject with the Personal Data Storage Policy, the Employees' Personal Data Storage Policy, or by a separate document.

19. All document forms of VGTU, which are intended for the collection of personal data of Data Subjects (questionnaires, curricula vitae, etc.), shall contain a reference to the Personal Data Storage Policy or to the Employees' Personal Data Storage Policy, specifying in addition which of his/her personal data the Data Subject must provide and which he/she does not have to provide, but can provide exclusively at his/her sole discretion, and what the consequences of not providing such data are.

20. The Staff Member must get ascertained (if necessary, also to ensure) that the Data Subject providing paper documents containing personal data (questionnaires, requests, certificates, copies of personal identity documents and other documents, etc.) is familiarized with the Personal Data Storage Policy, the Employees' Personal Data Storage Policy (or any other document containing information required by legal acts about the processing of his/her personal data) in accordance with the procedure set out in paragraph 14 of these Rules and understands it and data about such familiarization is stored in such a way that it can be presented as evidence at any time, if the need arises.

21. In cases where personal data is received not directly from the Data Subject, the Staff Member must get ascertained that such a Data Subject is provided with the information specified in Article 14 of the General Data Protection Regulation regarding the intended processing of his/her personal data. If, in the case referred to in this paragraph, the Data Subject is not provided with the necessary information on the processing of his/her personal data, the Staff Member shall provide such information to him/her no later than within one month, but in any case before contacting that Data Subject for the first time.

CHAPTER IV
KEEPING AND STORAGE OF PERSONAL DATA

22. Personal data (documents containing personal data or copies thereof) shall be stored in dedicated premises, information system, computer hard drives. Personal data (documents containing personal data or copies thereof) shall not be kept in a visible place accessible to everybody, where unauthorized persons could access them readily.

23. Documents containing personal data of Data Subjects and provided by Data Subjects to VGTU themselves (questionnaires, relevant requests, certificates, etc.) shall be stored in the personal files of the Data Subjects. A separate personal file shall be created for each Data Subject.

24. All personal files of Data Subjects, regardless of their form (paper or electronic in the information system), shall be stored in such a way as to be directly accessible only to the Staff of the Units responsible for the processing of personal data.

CHAPTER V
PROVISION OF PERSONAL DATA

25. Personal data of employees required for communication at work (office phone numbers and office e-mail addresses) shall be provided to all VGTU employees and external recipients. The data specified in this paragraph may be published on the website https://www.vgtu.lt/.

26. Relevant personal data from personal files (in paper or electronic form in the information system) shall be provided within VGTU as follows:

26.1. personal data of prospective employees – only to the Staff participating in the assessment of the suitability of the respective applicant for work and/or in taking of the employment decision;

26.2. employees' personal data – only to the Staff participating in the conclusion and/or performance of the employment contract of the relevant employee and/or in the performance of obligations related to the relevant employment contract;

26.3. students' personal data – only to the Staff participating in the conclusion and/or performance of the respective student's agreement on studies and/or in the performance of obligations related to the relevant agreement on studies.

27. In cases not specified in paragraph 26 of the Rules, personal data from personal files of the Data Subjects (in paper or electronic form in the information system) shall be provided to VGTU employees only after the head of the Human Resources Directorate or the head of a Unit assesses in a particular case and gets ascertained about the necessity, reasonability and lawfulness of providing data.

28. When providing personal data to VGTU employees, it must be ensured that personal data does not come into knowledge of unauthorised persons.

29. Relevant personal data of Data Subjects may be provided to external recipients or data processors only:

29.1. if the provision of such personal data is provided for by laws and other legal acts of the Republic of Lithuania (for example, the provision of data of an employed person to the State Social Insurance Fund Board, the provision of students' personal data to the national Register of Students administered by the higher education institutions of Lithuania and the Ministry of Education, Science and Sport of the Republic of Lithuania as the main institution processing register data, etc.);

29.2. personal data may be provided to external recipients or data processors with whom VGTU has signed relevant agreements on the provision of personal data and who ensure adequate protection of transmitted personal data by implementing appropriate organizational and technical measures intended to protect personal data from accidental or unlawful destruction, alteration, disclosure, as well as from any other unlawful processing.

30. In the case of a lawful basis, personal data must be provided to external recipients or data processors only to the minimum necessary.

CHAPTER VI
FULFILMENT OF DATA SUBJECTS' REQUESTS

31. The Staff must verify the identity of the applicant before fulfilling the Data Subject's request regarding the processing of his/her personal data by VGTU (to get access to the data processed about him/her, to rectify or delete his/her personal data, to restrict the processing of his/her personal data, etc.).

32. The Data Subject's request related to the processing of his/her personal data by VGTU shall be carried out in accordance with the General Data Protection Regulation. The Staff shall take a decision regarding the fulfilment of such requests, unless these Rules specify that in specific cases a decision regarding the fulfilment of a request may be taken by a VGTU Staff Member holding a particular office.

33. Unless these Rules specify that in specific cases the Data Subject's request regarding the processing of his/her personal data by VGTU must be submitted in writing, such a request may also be made orally. An oral request shall be fulfilled if the Staff Member gets duly satisfied about the identity of the applicant. A written request of the Data Subject may also be submitted in the electronic form by e-mail.

34. The personal data of the Data Subject may be provided to him/her also by e-mail, but only to an office e-mail address of VGTU or such an e-mail address as the Data Subject has personally indicated to VGTU and signed in confirmation of this (in a contract or signed questionnaire). Personal data is not provided by phone.

35. The Data Subject's request for rectification of his/her personal data must be made in writing, clearly indicating which of his/her personal data and how should be rectified. The request must be signed by the Data Subject. In fulfilling such a request, the Staff Member shall, if necessary, ask the Data Subject to prove the correctness of new personal data with relevant documents.

36. In the fulfilment the Data Subject's request for the destruction (deletion) of his/her personal data, only that data, processing of which is exclusively based on the consent of the Data Subject and when there is no other reason for processing of that personal data by VGTU, shall be destroyed (deleted). Decisions on the destruction of personal data may only be taken by the head of a relevant Unit (or by a Staff Member responsible for this by virtue of his/her office).

37. A decision on the Data Subject's request to restrict the processing of his/her personal data and/or regarding the transfer of his/her personal data may be taken only by the head of a Unit.

38. Upon fulfilment of the request of the Data Subject concerning the processing of his/her personal data, the Staff Member shall check whether the personal data that was deleted or altered had not been provided to data recipients (including data processors) and, if it had, must inform the data recipients of the alteration or deletion of the data provided to them.

CHAPTER VII
DESTRUCTION OF PERSONAL DATA

39. Personal data of prospective employees (all data or that part of data processing of which is based solely on the consent of the prospective employees) must be destroyed (deleted) without any undue delay (no later than within one working day) in any of the following cases:

39.1. upon receipt of a written request (including by e-mail) from a prospective employee or his /her withdrawal of his/her consent for data processing;

39.2. if it becomes apparent that VGTU will no longer need the personal data / when the personal data becomes unnecessary (after deciding not to employ an applicant);

39.3. at the end of the time limit for the storage of personal data, if any.

40. Employees' personal data must be destroyed (deleted) at the end of the time limits for storage of relevant documents containing employees' personal data.

41. Students' personal data must be destroyed (deleted) at the end of the time limits for storage of relevant documents containing students' personal data.

42. Personal data, the processing of which by VGTU is based solely on the consent of the Data Subject, must be destroyed (deleted) immediately upon request of the Data Subject or upon withdrawal of the Data Subject's consent.

43. If there are bases for destruction of personal data provided for in these Rules, the data shall be destroyed as follows: paper copies shall be destroyed by using a paper shredder; digital copies – by deleting them from the respective medium beyond recovery.

44. The destruction of personal data shall be communicated to all data recipients to whom the data that was subject to destruction was provided and such data recipients shall be required to immediately destroy the relevant personal data (documents, copies thereof) they have.

CHAPTER VIII
PERSONAL DATA PROTECTION MEASURES

45. Access to personal data must be restricted. Access to personal data shall be given only to the extent and only for the persons who need such data for the performance of their work functions.

46. Only those actions may be performed on personal data in information systems, for performance of which access rights are granted to a user of the information system.

47. VGTU Staff who get or may get access to personal data processed by VGTU must have assumed the undertaking to protect confidential information.

48. Personal data (documents, their copies, which contain personal data) must be stored in lockable premises which can independently be accessed only by persons entitled to access the personal data stored in those premises. If other persons can enter the premises on their own, personal data (documents, their copies, which contain personal data) must be stored in lockable cabinets or drawers, which can independently be unlocked only by persons entitled to access the relevant personal data.

49. Personal data in electronic form must be stored only on media located at VGTU premises, and access to personal data must be protected by passwords unique for each Staff Member.

50. In order to prevent unauthorized access to personal data in electronic form, including its unlawful destruction or alteration, effective, appropriate and adequately reliable software measures (passwords, firewalls, antivirus software) shall be used. The Centre for Information Technologies and Systems of VGTU shall be responsible for the installation and functioning of those measures.

CHAPTER IX
PERSONAL DATA BREACH

51. In the event of a personal data breach, a Staff Member who has become aware of it must notify the head of a Unit and the DPO about that immediately but in any case no later than within one hour.

52. The DPO and the head of a Unit, having received a notification or otherwise learned about a personal data breach, must immediately, but in any case no later than on the day, on which the fact of the personal data breach became apparent, inform the VGTU Rector. In such a case, VGTU must remedy the personal data breach as soon as possible, eliminate its consequences and take measures to reduce and eliminate the risk or potential damage to the rights and freedoms of the Data Subjects.

53. VGTU must, in accordance with the provisions of the General Data Protection Regulation, decide on notifying such a breach to the SDPI and the relevant Data Subjects. The decision referred to in this paragraph must be taken in such a way that the notification to the SDPI (if decided to notify) is given no later than within 72 hours after a personal data breach becomes apparent. A notification to the SDPI shall not be given when a personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

54. In case of a personal data breach in VGTU, following the provisions of Article 33 of the General Data Protection Regulation and the Description of the Procedure for Submission of the Notification on a Personal Data Breach to the State Data Protection Inspectorate approved by the Director of the SDPI on 27 July 2018 by Order No. 1T-72(1.12. E) “On approval of the Description of the Procedure for Submission of the Notification on a Personal Data Breach to the State Data Protection Inspectorate”, the head shall notify the State Data Protection Inspectorate by submitting a notification under the established procedure and conditions.