APPROVED
Vytautas Magnus University
Student Representation Parliament meeting
11 February 2021
PROTOCOL No. 210211

DESCRIPTION OF THE PROCEDURE FOR PROCESSING PERSONAL DATA AT THE STUDENT REPRESENTATIVE COUNCIL OF VYTAUTAS MAGNUS UNIVERSITY

CHAPTER I

GENERAL PROVISIONS

1. The Description of the Procedure for Processing Personal Data at the Student Representative Council of Vytautas Magnus University (hereinafter – the Description) establishes the requirements for the processing and protection of personal data, the purposes of personal data processing, the rights of data subjects and the procedure for their implementation, and the technical and organizational measures for data protection.

2. This Description applies to and is binding on the Data Controller – Vytautas Magnus University Student Representative Council (hereinafter – VMU SRC) – and all members of VMU SRC who process personal data or become aware of them in the course of their duties.

3. VMU SRC processes personal data of all current and former VMU SRC members and other people, which they have provided in accordance with the procedure established by law ibn the basis of contractual and other legal relations.

4. VMU SRC in the controller of all the data collected in the course of the VMU SRC's activities and internal administration processes, as well as the processor of personal data provided by data subjects and third parties.

5. This Schedule has been prepared in accordance with Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection on natural people with regard to the processing of personal data and the free movement of such data and repealing Directive 94/46/EC (General Data Protection Regulation) (hereinafter referred to as the "GDPR"), the Law of Legal Protection of Personal Data of the Republic of Lithuania (hereinafter referred to as the "LPPD"), and other legal acts.

6. VMU SRC undertakes to collect and process personal data only if and to the extend necessary for the fulfillment of a specific, defined and legitimate purpose.

7. For the purposes of this Schedule, the following key terms are used:

7.1. **Personal data** means any information relating to a natural person, i.e. the data subject, who is identified or can be identified, directly, indirectly, by reference, to data such as name, surname, address, e-mail address, personal identification number and other social characteristics.

7.2. **Data recipient** – the legal or natural person to whom the personal data are provided.

7.3. **Data subject** – a natural person whose personal data are processed by the controller or processor(s).

7.4. **Provision of data** means the disclosure of personal data by transmission or otherwise making the available (except for publication on the media).

7.5. **"Processing"** means nay operation performed on personal data, such as collection recording, accumulation, storage, classification, grouping, aggregation, modification (additional or alteration), disclosure, communication, use, logical and/or arithmetical operations, retrieval, dissemination, destruction, or any other operation or set of operations.

7.6. **Processing of data for statistical purposes** – carrying out statistical surveys, reporting and storing their results.

7.7. **Consent of the data subject** ("Consent") means the voluntary written indication of the data subject's will to have his or her personal data processed for a purpose known to him or her.

7.8. **Request** – an application of a person, not related to the violation of personal data protection rights or legitimate interests, to VMU SRC requesting, in accordance with the procedure established by VMU SRC, to provide him/her with information about personal data processed by VMU SRC and to obtain a copy thereof.

7.9. **Processing of a request** – an activity of the VMU SRC that includes receiving registering, determining the substance of the request, preparing a response and sending (serving) it to the person.

7.10. **Complaint** – a written appeal addressed by a person to the VMU SRC, stating that his/her personal data protection rights or legitimate interests have been violated, or informing about the violation of another person's personal data protection rights and legitimate interests and asking for their protection.

7.11. **Third party** – a legal or natural person other than the data subject, the controller, the processor and persons directly authorized by the controller or processor to process personal data.

CHAPTER II

THE PURPOSES, SCOPE AND DURATION OF THE PROCESSING OF PERSONAL DATA

8. Personal data is processed by VMU SRC for the following purposes:

8.1. For internal communication purposes, the following data of prospective, current and former VMU SRC members and candidates for VMU SRC membership are processed:

8.1.1. Name and surname;

8.1.2. Telephone number, address, and email address;

8.1.3. Date of birth;

8.1.4. Duties, period of office;

8.1.5. Visual material in which the person is filmed of photographed;

8.1.6. Information about the start of studies, end of studies (or expected end of studies), level of studies, study unit, study programme, study course.

8.2. For the purposes of student representation, the following data on student representatives in the various structural bodies of VMU and VMU SRC are processed:

8.2.1. Name;

8.2.2. Date of birth and personal identification number;

8.2.3. Telephone number and email address;

8.2.4. Duties, period of office;

8.2.5. Visual material in which the person is filmed of photographed;

8.2.6. Information about the start of studies, end of studies (or expected end of studies), level of studies, study unit, study programme, study course.

8.3. For the purposes of organizing events, the following data is processed on participants in events:

8.3.1. Name and surname;

8.3.2. Telephone number and email address;

8.3.3. Duties, period of office;

8.3.4. Study unit, study programme, study course;

8.3.5. Social network account address;

8.3.6. Dietary needs and other data provided by the data subject;

8.3.7. Visual material in which the person is filmed or photographed.

8.4. For the purposes of administering candidates for posts, the following candidate data is processed:

8.4.1. Name and surname;

8.4.2. Telephone number and email address;

8.4.3. Date of birth;

8.4.4. Information on the beginning of studies, the end of studies (or the expected end of studies), the level of studies, the unit of studies, the programme of studies, the course of studies;

8.4.5. Visual material in which a person is filmed or photographed;

8.4.6. Other details to be included in the candidate’s cover letter and CV.

9. In the cases and according to the procedure established by law, the personal data referred to in point 8 may be provided to the University.

10. Personal data is stored for as long as the person has the status of a student, VMU SRC member or event participant and for 2 years after the end of the study, membership event.

CHAPTER III

OBLOGATIONS OF DATA SUBJECTS INVOLVED IN THE PROCESSING

11. Data is collected by the VMU SRC in accordance with the procedure established by the legislation by obtaining it directly form the data subject, through formal requests to the entities processing the necessary information and entitled to provide it, or on the basis of contracts. As a general rule, the processing of personal data is subject to the consent of the data subject.

12. VMU SRC, as data controller.

12.1 . Ensure the exercise of the data subject's rights and fulfil the obligations of the controller laid down in the general requirements for organizational and technical measures for the security of personal data and in other legal acts regulating the processing of personal data;

12.2 . Designate the Audit Committee responsible for data protection and other persons responsible for the processing of personal data in VMU SRC;

12.3 . Ensure that the Audit Board is empowered to respond to requests and complaints from data subjects and is involved in an appropriate and timely manner in all matters relating to the protection of personal data;

12.4 . Ensure the development of the competence of its members in the field of personal data protection for the proper performance of their duties.

13. The following personal data processor functions shall be carried out by persons authorized by the President:

13.1. Ensure that personal data are processed by the VMU SRC only by those persons for whom it is necessary for the performance of the duties and functions of the VMU SRC, and only to the extent necessary to achieve the intended purposes;

13.2. Provides and implements technical measures for the protection of data processed by VMU SRC;

13.3. Ensure the lawful processing of personal data, the implementation of the rights of data subjects and the necessary technical data protection measures at the VMU SRC;

13.4. Ensure that technical measures are in place to enable personal data to be stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed;

13.5. Ensure that the members of the VMU SRC and persons processing personal data are familiarized with this Regulation;

13.6. Responsible for the preparation and approval, registration and submission to the Audit Board (in the exercise of the rights of data subjects) of the documents necessary for the processing of personal data (agreements, protocols, contracts, notifications, etc.);

13.7. Ensure that personal data are processed in accordance with this Description and that the data can be recovered in the event of their accidental loss;

13.8. Ensure the implementation of appropriate organizational measures to protect personal data processed by the relevant unit of the VMU SRC and/or the units coordinating the activities of the VMU SRC from accidental or unlawful destruction, alteration, disclosure, as well as from any other unlawful processing.

14. Audit Commission:

14.1. Ensure compliance with these processing principles:

14.1.1. Personal data is processed in accordance with the GDPR, the GDPR, The Hague Data Protection Act and other regulatory and VMU legislation governing data protection;

14.1.2. Personal data are collected for specified and legitimate purposes and are not further processed for purposes incompatible with those established before the personal data were collected;

14.1.3. Personal data are processed accurately, fairly and lawfully;

14.1.4. Personal data are accurate and, where necessary for the processing of personal data, kept up-to-date; inaccurate or incomplete data must be rectified, supplemented, erased or suspended;

14.1.5. The personal data are identifiable, adequate and limited to what is necessary for their collection and further processing;

14.1.6. Personal data are processed in such a way that the data subjects can be identified for no longer than is necessary for the purposes for which the data were collected and processed.

14.2. Ensure that personal data are processed in accordance with the organizational and technical data security measures specified in the documents drawn up by the President's delegates (agreements, protocols, contracts, communications, etc.);

14.3. Ensure that, after identifying data that are redundant, no longer used, or for which there is no longer a legal basis for processing, the possible non- compliance is immediately eliminated;

14.4. Ensure the destruction of electronic and/or paper documents containing personal data after the expiry of the retention periods laid down for personal data;

14.5. Ensure that confidentiality requirements are respected so that personal data are not disclosed to third parties.

14.6. Notify the President if it assesses and determines that the organizational and technical measures for the protection of personal data are not reliable.

VI CHAPTER
DATA SUBJECT RIGHTS

15. The data subject whose data is processed in the activities of the VMU SA has the following rights:

15.1. To know (be informed) about the processing of your data (right to know);

15.2. To know your data and how they are processed (right of access);

15.3. Require rectification or, taking into account the purposes of the processing of the personal data, completion of incomplete personal data (right of rectification);

15.4. To have your data erased or to stop the processing of your data (except for storage) (right to erasure and right to be forgotten);

16. Data subjects have the right to contact the Audit Commission directly on all issues related to the processing of personal data of data subjects and the rights of data subjects under the GDPR, the GDPR, The Hague Data Protection Act (GDPR) and other relevant legislation.

17. The response to a request or complaint from a data subject concerning the processing of his or her personal data must be provided free of charge within 30 calendar days from the date of the request, except in the cases and under the conditions provided for in the GDPR and other legislation, including Article 12(3) of the GDPR, where, depending on the complexity of the request and the number of other requests, that period may be extended by an additional 2 months.

18. If the data subject, having familiarized himself/herself with the personal data processed by VMU SRC in the response, finds that his/her personal data are being processed unlawfully or unfairly, and contacts the Audit Commission, the latter shall, within 5 working days at the latest, verify the accuracy, lawfulness and fairness of the processing of the personal data, and shall take measures to destroy without delay personal data which have been unlawfully and fraudulently collected or to suspend the processing of such personal data, except for storage, and shall inform the data subject of the action taken.

19. If the data subject, having read the personal data processed by the VMU SA contained in the response, determines that further processing of his or her personal data is inappropriate and withdraws his or her prior consent to the processing of the data and asks the VMU SA to forget about it, the Audit Board shall take measures to destroy the personal data processed on the basis of the consent, with the exception of the storage, and shall inform the data subject of the actions taken or shall inform him or her of the reasons why the data cannot be destroyed.

20. Where the VMU SRC has made publicly available personal data concerning a data subject, but is obliged to erase the personal data at the request of the data subject, the Audit Committee shall, taking into account the technology used by the VMU SA and the cost of implementation, take reasonable steps, including technical measures, to ensure that the personal data and/or copies or duplicates of the personal data are destroyed without delay.

21. The requirements to forget and erase personal data shall not apply where the reasons

set out in this Schedule cannot be substantiated and in the cases provided for in Article 17(3) of the GDPR, including where:

21.1. Legal obligations imposed by the VDU SRC that require the processing of data or for the performance of a task carried out in the public interest;

21.2. for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes in accordance with the GDPR and other legal requirements;

21.3. in other cases, provided for in the GDPR and other legal acts.

22. VMU SRC, having suspended the processing of personal data at the request of the data subject, shall store the personal data for which the processing has been suspended until they are rectified or destroyed (at the request of the data subject or after the expiration of the data storage period).

23. The data subject has the right to lodge a complaint with the State Data Protection Inspectorate regarding the activities of the VMU SRC.

24. The VMU SRC shall ensure that the rights of the data subject are properly implemented and that all information is provided to the data subject in a clear, intelligible and accessible form. The purposes of the processing of personal data set out in this Schedule, the rights of data subjects and the procedures for their implementation shall be set out in a simplified form in the Privacy Policy of the VMU SRC, which shall be published on the website of the VMU SRC.

VII CHAPTER

EXERCISING THE RIGHTS OF THE DATA SUBJECT

25. In order to exercise his/her rights, the data subject shall submit a free-form written request or complaint to the Audit Commission on the processing of personal data.

26. The data subject shall submit requests or complaints directly to the office of the VMU SRC or by e-mail.

27. The request must be legible, signed, contain the name, surname, address and other contact details of the data subject, in the form of the communication requested, and must indicate which of the data subject's rights, and to what extent, the data subject's rights are to be exercised.

28. The data subject may only exercise his/her rights after the possibility for the VMU SRC to verify his/her identity. The identity of the data subject shall be verified in one of the following ways: 26.1. by coming to the VMU SRC office and presenting an identity document together with the request rights; 26.2. by writing a request or complaint from a VMU provider email account.

29. The data subject may exercise his/her rights himself/herself or through a representative authorized by a notary.

30. If a representative of a person applies on behalf of the represented data subject, he/she shall indicate in his/her application his/her name, surname, place of residence, contact details, as well as the name, surname, place of residence of the represented person, the information on which of the data subject's rights specified in the Description, and the extent to which the data subject wishes to exercise the rights and shall enclose the document confirming the representation, or a copy of his/her document, certified in the manner prescribed by the legislation of the Republic of Lithuania. The request submitted by the representative shall comply with the same requirements as those of the principal.

31. Requests and complaints from individuals shall be responded to in the manner in which the request or complaint is made.

32. The President shall coordinate the drafting of the response to the request or complaint and shall advise the Audit Board and provide the response to the data subject. The response to the data subject shall be signed by the President.

33. The reply to the request or complaint shall be clear and reasoned, indicating all the circumstances relevant to the examination of the request or complaint and the specific provisions of the legislation relied on in assessing the content of the request or complaint.

34. The reply, stating the reasons for refusing to provide the service or information requested, shall inform the person or his representative of the procedure for appealing against such a reply, indicating the name(s) and address(s) of the institution(s) with which the appeal may be lodged, and the time-limit(s) within which an appeal may be lodged. When forwarding the application or complaint to another competent authority and informing the person or his representative thereof, the notification to the person need not specify the abovementioned appeals procedure.

35. Requests or complaints received shall be responded to within 30 (thirty) calendar days from the date of the data subject's request.

36. By decision of the Review Panel, in the cases provided for in the GDPR, the submission of the reply may be delayed by up to 60 days by informing the data subject.

VIII CHAPTER
PROCEDURES FOR MONITORING, IDENTIFICATION, ASSESMENT OF INCIDENTS

37. The controller shall ensure personal data breach incidents are adequately monitored, detected and evaluated. Risk factors for a personal data breach may include:

37.1. Unintentional, where the protection of personal data is breached for accidental reasons (data processing errors, deletion of information media, data records, destruction of data, establishment of incorrect data transmission routes (addresses), etc., or system failures due to power failure, computer virus, etc., breach of internal rules, lack of system maintenance, lack of system maintenance, software tests, inadequate maintenance of data media, inadequate capacity and protection of the lines, integration of the computers in the network, protection of the computer programs, inadequate provision of fax materials, etc.);

37.2. Deliberate, when the protection of personal data is violated deliberately (unauthorized intrusion into the premises of VMU SRC, personal data storage facilities, computer network, malicious violation of the established rules for processing personal data, deliberate spreading of a computer virus, theft of personal data, unauthorized use of another person's rights, etc.);

37.3. Unexpected accidental events (lightning, fire, flood, inundation, storms, burning of electrical wiring, exposure to temperature and/or humidity changes, influence of dirt, dust and magnetic fields, accidental technical breakdowns, other factors beyond the control and/or control of the insurance company etc.).

38. A data breach incident is an event that causes or is likely to cause, among other things:

38.1. Disclosure of personal data;

38.2. Leakage of personal data, i.e. when personal data are made available to persons who are not entitled to process them;

38.3. Malfunctions of the equipment used to process personal data, which may lead to the destruction of personal data;

38.4. Errors in personal data.

39. Any person processing personal data on behalf of VMU SRC who becomes aware of a data breach incident must immediately report it to the Audit Committee.

40. After an initial assessment of the data breach incident, the Review Panel shall inform the President of the data breach, who shall promptly take the following actions, taking into account the

seriousness of the data breach incident and the potential impact on the rights of the data subject:

40.1. Take all reasonable steps (within its technological and financial capabilities) to recover lost personal data and/or to mitigate the damage to personal data caused by the data breach incident;

40.2. If necessary, contact other public authorities (police, Communications Regulatory Authority, National Cyber Security Centre, etc.) (no later than 1 working day after the need to contact the relevant authority is identified);

40.3. Identify all groups of personal data likely to be affected by the same type of data breach incident (at the latest within 2 working days of becoming aware of the breach);

40.4. Decides on the need to report the incident to the State Data Protection Inspectorate (no notification is required if the breach is unlikely to endanger the rights and freedoms of natural persons);

40.5. Upon determining that a data breach is likely to result in a serious risk to the rights and freedoms of natural persons and that notification to the State Data Protection Inspectorate is therefore necessary, ensure that the breach is notified to the Inspectorate no later than 72 hours after becoming aware of the data breach. The notification shall include at least:

40.5.1. The nature of the data breach (including, where possible, the categories and approximate number of data subjects concerned, the approximate categories and approximate number of data records,

40.5.2. Describe the nature of the data breach and its possible consequences,

40.5.3. Recommendations for the individual concerned on how to remedy the data breach or its possible adverse effects and consequences (e.g. blocking emails sent to certain email addresses, etc.).

40.6. Assess whether the personal data breach is likely to result in a serious risk to the rights and freedoms of the natural person and whether the data subjects whose data have been compromised should be informed;

40.7. Initiate, as soon as possible, the notification of the data subjects whose data has been compromised, if it is established that the data breach may result in a serious risk to the rights and freedoms of the data subjects and that notification of the data subjects is therefore necessary (except in cases provided for in the Regulation, where notification of the breach to the data subjects is not required or is allowed to be public). The notification must contain at least:

40.7.1. Contact details of the VMU SRC representative,

40.7.2. Describe the nature of the data breach and its possible consequences,

40.7.3. Recommendations for the individual concerned on how to remedy the data breach or its possible adverse effects and consequences (e.g. blocking emails sent to certain email addresses, etc.);

40.8. If necessary, immediately contact third parties that can help manage the consequences of a data breach incident (IT companies, security companies, premises and technical repair companies, etc.).

41. The President's delegate must register each incident involving personal data in the Personal Data Incident Register (Annex 1).

IX CHAPTER

OTHER ORGANIZATIONAL MEASURES TO PROTECT PERSONAL DATA

42. Personal data (documents containing personal data or copies thereof) must not be kept in a visible place accessible to all, where persons who are not entitled to access them without hindrance.

43. The President's delegates shall ensure protection against unauthorized physical access to personal data by the following means: locked premises, a functioning personal access control systems, restricted access to the premises concerned on the measures appropriate to the risk.

44. Data stored on online platforms is accessible only to the persons whose functions require it. Electronic documents containing personal data shall only be created using accounts and platforms belonging to VMU SRC.

45. The President or the President's delegates may, if necessary, provide for additional organizational measures for the protection of personal data.

X CHAPTER

FINAL PROVISIONS

46. The description shall be reviewed periodically (at least once every two years) and updated as necessary.

47. The President shall ensure that the persons processing personal data in the VMU SRC are informed about updates to the Description.

48. Persons who violate the GDPR, the GDPR, the ADTAI, other legal acts, these Regulations and other legal acts of the VMU SRC in respect of the processing and protection of personal data shall be subject to the liability provided for in the legal acts of the Republic of Lithuania.

49. The description is published on the VMU SRC website.

50. The Schedule shall be approved by a resolution of Parliament.

Processing of personal data at Vytautas Magnus University Description of the procedures for student representation in the Students' Union

Annex 1

PERSONAL DATA INCIDENT LOG FORM

Date on which the incident was recorded	Likely causes of the incident	Incident type	Final list of data related to the incident	List of data subjects involved in the incident. If possible, finite	Date of Incident clearance	Measures taken to reduce effect of the incident	Name, surname, title, signature of the person who made the entry	Data Processor(s)	Is there an obligation to notify the IDAI and, if applicable, how/when this was done	Is there an obligation to notify the data subject and, if so, how/when? made