DECISION OF THE SENATE

RTU Senate meeting of September 28, 2018 (protocol No. 622)

On the approval of the personal data protection policy of Riga Technical University in a new version

Taking into account Regulation (EU) 2016/679 of the European Parliament and Council of April 27, 2016 "On the protection of data of natural persons with regard to the processing of personal data and the free circulation of such data", the Senate decides:

1. to approve the data protection policy of the Riga Technical University of natural persons (hereinafter - the Policy) in a new version.
2. to recognize as invalid the decision of the Senate of May 21, 2018 (protocol No. 620) "On the approval of the data protection policy of natural persons of Riga Technical University".

Personal data protection policy of Riga Technical University

Issued in accordance with the State Administration of Equipment Article 72, Part One, Clause 2 of the Law and, in accordance with the first part of Article 15 of the University Law

I. General questions

1. The personal data protection policy of Riga Technical University (hereinafter - RTU) (hereinafter - the Policy) defines the guidelines for the collection, storage and processing of personal data, which ensures the protection of personal data by implementing and maintaining a sufficient set of measures to reduce or prevent potential or caused damage, and compliance with the applicable personal data protection legislation, including Regulation (EU) 2016/679 of April 27, 2016 "On the protection of personal data with regard to the processing of personal data and the free movement of such data" .
2. The policy is applicable to RTU staff, students and other authorized third parties who have access to any data of RTU natural persons, subject to RTU the security policy of information and communication technology systems and other related internal regulations, which provide instructions on the correct processing of personal data.
3. The policy applies to any type of information, which includes personal data stored by RTU (in computer systems, mobile devices, telephones, paper records, etc.), written, verbally expressed and electronic data.

II. Terms used in politics

4. Data of natural persons (hereinafter - personal data) - is any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be directly or indirectly identified, in particular by reference to an identifier such as the said person's name, surname, identification number, location data, online identifier or one or more physical, physiological, genetic, spiritual, economic, cultural or social identity factors;

5. Special categories of personal data – sensitive personal data revealing race or ethnicity, political opinions, religious or philosophical beliefs or trade union membership, and genetic data, biometric data for the unique identification of a natural person, health data or data about a natural person's sex life or sexual orientation;
6. Processing - any operation or set of operations performed on personal data or sets of personal data, with or without automated means, such as collection, registration, organization, structuring, storage, adaptation or transformation, retrieval, viewing, use, disclosure, transmission, sharing or otherwise making them available, matching or combining, limiting, erasing or destroying;
7. RTU staff - persons who have an employment contract with RTU for an indefinite or fixed period, company, copyright contract or contract for volunteer work or practice;
8. Data subject – an identified or identifiable natural person;
9. Manager – RTU, which determines the purposes and means of personal data processing;
10. Processor – natural person (including RTU staff) or legal entity, public institution (including RTU), agency or other body, on behalf of the controller, processing personal data;
11. Third party – a natural or legal person, public institution, agency or structure that is not the data subject, manager, processor and persons who are authorized to process personal data under the direct authority of the manager or processor;
12. Data protection specialist – a specialist appointed by the controller who has special knowledge in the field of data protection law and practice and who is able to inform and advise the controller or the processor and the employees who perform the processing on their obligations in accordance with the regulatory enactments regulating data protection; monitor compliance with data protection laws and the controller's or processor's policy regarding personal data protection, including division of responsibilities, informing and training employees involved in processing operations, and related audits; provide advice on data protection impact assessment upon request and monitor its implementation; cooperate with the Data State Inspectorate; to be the contact point of the Data State Inspectorate in matters related to processing and advise on any other matter as appropriate;
13. Privacy notice – notice to the data subject about confidentiality to provide the data subject with an insight into how the processor collects, uses, stores and shares the data subject's personal data (indicating the purposes and legal basis of the processing of personal data), as well as what measures the processor takes to protect the data subject's personal data, additionally informing the data subject that the data subject can request: access to or change the personal data of the data subject held by the processor; withdraw consent previously given to the processor; not to send certain notifications to the data subject and to answer questions that the data subject may have regarding the processor's privacy practices;
14. Pseudonymization – processing of personal data carried out in such a way that it is no longer possible to associate personal data with a specific data subject without the use of additional information, provided that such additional information is kept separately and technical and organizational measures are applied to it to ensure that individuals the data is not linked to an identified or identifiable natural person;
15. Phishing - also phishing *(English: phishing)* in computer science is an illegal way of trying to fraudulently obtain confidential information from an Internet user, such as usernames, passwords, credit card numbers.

III. Personal data protection principles

16. When processing personal data, the following principles of personal data protection must be observed:
    16.1. legal, fair and transparent processing of personal data;
    16.2. collecting personal data only for specific, clear and legitimate purposes and processing it in a way that is compatible with those legitimate purposes;
    16.3. only the processing of personal data that is appropriate and necessary for the respective purposes;
    16.4. maintaining accurate and up-to-date personal data and taking steps to ensure that inappropriate personal data is promptly deleted or corrected;
    16.5. retention of personal data in a form that allows identification of data subjects for no longer than is necessary for the purposes for which the data is processed;
    16.6. taking appropriate technical and organizational measures to ensure that personal data is stored securely and protected against unauthorized or unlawful processing, as well as against accidental loss, destruction or damage.
17. RTU is also responsible for demonstrating compliance with the aforementioned data protection principles.

IV. Basis of personal data processing

18. In relation to any processing operation involving personal data, before the processing starts and then regularly during the processing, you must ensure that:
    18.1. the purposes of the specific processing activity have been reviewed and the most appropriate legal basis for this processing has been found, ie:
        18.1.1. that the data subject has consented to the processing;
        18.1.2. the processing is necessary for the performance of a contract to which the data subject is a contracting party, or to take measures at the data subject's request prior to the conclusion of the contract;
        18.1.3. processing is necessary to fulfill a legal obligation applicable to RTU;
        18.1.4. the processing is necessary for the protection of the essential interests (including physical health or life) of the data subject or another natural person;
        18.1.5. processing is necessary to fulfill a task carried out in the public interest, or in the implementation of the obligations set out in the regulatory acts of the RTU;
        18.1.6. processing is necessary to comply with the legitimate interests of RTU or a third party, except in cases where the interests of the data subject or the fundamental rights and fundamental freedoms that require the protection of personal data are more important than such interests.
    18.2. the processing is necessary for the relevant legitimate purpose (in cases where the processing is based on consent only and there is no other basis for the processing);
    18.3. the legal basis applied to specific processing is documented to demonstrate compliance with data protection principles;
    18.4. the data subject has the opportunity to familiarize himself with the privacy statement (Policy 10);
    18.5. a legal condition to process the special category of personal data is established and documented.

V. Special categories of personal data

19. Special category or sensitive personal data can be processed if:

    19.1. there is a legitimate basis, and
    19.2. one of the special conditions applies to the processing of sensitive personal data:
        19.2.1. the data subject has given explicit consent to the processing of this personal data ;
        19.2.2. processing is necessary for the implementation of RTU or the data subject's employment legal relationship;
        19.2.3. the processing is necessary to protect the important (including health and life) interests of the data subject or another natural person, and the data subject is physically or legally unable to give consent;
        19.2.4. processing refers to personal data that the data subject has deliberately made public;
        19.2.5. processing is necessary for the establishment, exercise or defense of legal claims, or whenever the courts carry out their tasks; or
        19.2.6. processing is necessary due to significant public interests that are proportionate to the stated purpose, respects the essence of the right to data protection and provides for appropriate and specific measures to protect the fundamental rights and interests of the data subject.

VI. Data privacy impact assessment

20. If the processing may pose a high risk to the rights and freedoms of natural persons (for example, if the RTU plans to use a new technological way to process personal data), before starting the processing, a data privacy impact assessment must be carried out to assess:

    20.1. whether the processing is necessary and proportionate to the stated purpose of the processing;
    20.2. whether there is a risk to the rights and freedoms of natural persons;
    20.3. what additional security measures can be implemented to prevent risks and protect personal data.

VII. Documentation

21. Personal data processing must be registered in the RTU personal data processing register. For each processing of personal data, the purpose, legal basis of processing, categories of data subjects, categories of recipients, intended storage terms of personal data, as well as the responsible structural unit, which is responsible for both the personal data processing process and the updating of related information in the register, are identified.
22. RTU regularly renews the documentation related to the processing of personal data, which may include:
    22.1. conducting information audits to find out what personal data is stored in RTU systems;
    22.2. distribution of survey sheets and conversations with employees throughout the RTU to obtain a more complete picture of processing activities; and
    22.3. Reviewing policies, procedures, contracts to ensure data security.

VIII. Privacy notices

23. The Administrative Department ensures the publication of a general privacy statement on the RTU website, as well as information on where the data subject can find out about the processing of his data and its legal basis.
24. In cases where the processing of personal data is initiated, RTU ensures the provision of a privacy notice to the data subject in a short, transparent, understandable and easily accessible manner using clear language.

IX. Data subject rights

25. Data subjects have the following rights regarding their personal data:
    25.1. to be informed about how, why and on what basis the data is processed;
    25.2. obtain confirmation as to whether the data subject's data is being processed and, in case of confirmation, obtain access to them by submitting an appropriate request;
    25.3. to have the data rectified if it is inaccurate or incomplete;
    25.4. have the data deleted if it is no longer necessary for the purpose for which it was originally collected and processed, or if there is no longer a legitimate basis for this processing (also known as the “right to be forgotten”);
    25.5. achieve restriction of personal data processing if the accuracy of the information is disputed, or the processing is illegal (but the data subject does not want his data to be deleted) or if the RTU no longer needs the personal data, but the data subject requests to leave them to defend himself in court ;
    25.6. achieve a temporary limitation of personal data processing if the data subject believes that they are inaccurate (and RTU conducts a data accuracy check), or if the data subject has objected to data processing (and RTU conducts an assessment , whether RTU's legal justification prevails over the data subject's interests).
26. RTU's privacy notices provide information that the data subject has the right to contact RTU's data protection specialist about the possibilities of exercising their rights.

X. Individual responsibilities

27. The data subject is obliged to inform the RTU about any changes in his personal data transferred to the RTU.
28. RTU expects from the processor, who, in the performance of his official duties, has access to the personal data of RTU staff, students and other data subjects, to treat this data in good

faith in order to fulfill the assumed obligations to ensure the confidentiality and integrity of personal data.

29. Processor who has access to RTU personal data:
    29.1. accesses only the personal data to which the processor has the right to access, and only to the appropriate extent and for the permitted purpose (it is not permitted to be interested in the data for no purpose);
    29.2. allows third parties to access personal data only if they have been given appropriate permission;
    29.3. protects personal data (including following the security policy of RTU's information and communication technology systems and related regulations on access to premises, computer access, password protection and secure file storage and destruction, as well as observes other precautions when processing personal data);
    29.4. do not carry away (home) data or devices that contain (or can be used to access) personal data, unless appropriate security measures (such as pseudonymization , encryption with appropriate password protection) have been taken to ensure the confidentiality of the information on the device.
30. The manager, processor or data subject informs the RTU data protection specialist if one of the following cases has occurred (or is occurring or could occur with a very high probability):
    30.1. processing of personal data takes place without a legal justification, or with respect to sensitive personal data, at least one of the conditions mentioned in Clause 12 of the Policy is not met;
    30.2. access to personal data is provided without proper authorization;
    30.3. personal data is not securely stored or deleted;
    30.4. personal data or devices containing personal data (or which can be used to access them) are taken out of the RTU without taking appropriate security measures;
31. there is any other violation of these internal rules or any violation of the data protection principle specified in clause 16.

XI. Information security

32. RTU uses appropriate technical and organizational measures in accordance with RTU's information and communication technology systems security policy and other related internal regulatory enactments to maintain the security of personal data and, in particular, to protect them against unauthorized or illegal data processing and/or accidental loss, destruction or damage. These may include:
    32.1. assurance that, where possible, personal data is pseudonymised or encrypted;
    32.2. confidence in the confidentiality, integrity, availability and durability of the data in the processing systems;
    32.3. confidence that in the event of a physical or technical incident, personal data can be restored in time and access to them provided; and
    32.4. processes are established that regularly check and evaluate the effectiveness of technical and organizational measures to ensure the security of data processing.
33. In the event that RTU uses third parties to process personal data on its behalf, it is necessary to incorporate additional security measures regarding data confidentiality and integrity into contracts. In particular, contracts with third parties must ensure that:
    33.1. the third party can act only in accordance with the written instructions of RTU;
    33.2. the third party processing the data is reliable;

33.3. appropriate measures are taken to ensure the security of processing;
33.4. subcontractors are involved only with the prior consent of RTU and in accordance with a written agreement;
33.5. a third party will help RTU ensure the rights of the data subject in the field of personal data;
33.6. the third party will assist RTU in fulfilling its obligations regarding data processing security, data breach notifications and data protection impact assessment;
33.7. upon termination of the contract, the third party will delete or transfer to RTU all personal data transferred to it on the basis of the contract;
33.8. the third party will provide RTU with the information necessary to ensure the fulfillment of data protection obligations.

34. Before a new contract is concluded (or an existing contract is amended), which includes the processing of personal data by a third party, the employee responsible for concluding the contract receives an acceptance from the data protection specialist of RTU.

XII. Storage of personal data

35. Personal data and sensitive personal data will be securely stored in accordance with RTU's information and communication technology systems security policy.
36. Personal data and sensitive personal data may not be stored longer than necessary for the relevant purpose. The duration of data retention depends on the circumstances, including the purposes for which the personal data was obtained.
37. Personal data and sensitive personal data that are no longer needed will be permanently deleted from RTU's information systems. Data from backup copies will be deleted as soon as the backup storage time expires.

XIII. Data protection violations

38. A breach of data protection can be different, for example:
38.1. loss or theft of data or equipment on which personal data is stored;
38.2. unauthorized access to personal data;
38.3. loss of data resulting from equipment or systems (including hardware and software) errors;
38.4. the result of human error, such as accidental deletion or alteration of data;
38.5. unforeseen circumstances such as fire or flood;
38.6. deliberate attacks on IT systems, such as system hacking, virus or phishing attacks.
39. If there is a suspicion that the personal data held by RTU has been compromised in any way, the personal data protection specialist of RTU must be notified immediately.
40. RTU commits to:
40.1. investigate any reported actual or potential data security breaches;
40.2. in the event that it may threaten the rights and freedoms of a person, without delay and, if possible, within 72 hours from the moment the violation becomes known, provides the necessary information about the data violation to the Data State Inspectorate;
40.3. to notify affected individuals if the loss of data could pose a major risk to their rights and freedoms, and if such notification is required by law.

XIV. International data transfer

41. RTU may transfer personal data outside the European Economic Area (which includes the countries of the European Union (EU) and Iceland, Liechtenstein and Norway) and to other countries on the basis that the protection requirements established in these countries are in line with EU requirements or that the receiving organization information, has provided sufficient guarantees (for example, using binding company regulations or standard data protection clauses) or if RTU obtains the explicit consent of the relevant data subjects for such data transfer.
42. The processor is obliged to inform the data subject of all intended international transfers of personal data in the relevant privacy statement.

XV. Training

43. RTU provides adequate training of RTU personnel in the field of data protection. For the processor (who needs regular access to personal data, or who is responsible for responding to the relevant requests of data subjects), RTU provides additional training to help the processor understand his duties and their correct performance.

XVI. Closing questions

44. RTU takes the protection of personal data very seriously. Disregarding the protection of personal data:
    44.1. persons whose personal data are processed are at risk;
    44.2. criminal sanctions for the processor and controller is increased .
45. Taking into account the importance of personal data protection, non-compliance with requirements regarding personal data protection may lead to disciplinary measures in accordance with RTU's internal regulations, and these actions, as a result of a serious violation, may lead to the termination of the employment contract. If the person who violates the requirements regarding the protection of personal data is not an employee of RTU, the contract with this person can be terminated immediately.
46. RTU's data protection specialist is responsible for informing and advising RTU and its employees about data protection obligations of natural persons, as well as monitoring the implementation of RTU's Policy (e-mail: datuaisardziba@rtu.lv, phone: 67089833).
47. The order in which personal data processing and protection is organized at RTU is determined by internal regulations approved by the rector.

President of the Senate E. Gaile-Sarkane

Prepared by the Administrative Department .