

APPROVED BY
Order No. A-394 of the Rector of
Kaunas University of Technology of
10 September 2020

PRIVACY POLICY FOR THE PERSONAL DATA PROCESSED AT KAUNAS UNIVERSITY OF TECHNOLOGY

CHAPTER I GENERAL PROVISION

1. The Privacy Policy for the Personal Data Processed at Kaunas University of Technology (hereinafter – Policy) provides information on the principles that Kaunas University of Technology applies to the processing of the data of the members of its community and partners, the rights of the data subjects and how they can be exercised.

2. The following concepts are used in the Policy:

Personal data – any information related to a natural person whose identity is or can be identified directly or indirectly by using such data as personal ID number, one or several physical, psychological, economic, cultural or social characteristics of a person.

General Data Protection Regulation (hereinafter – **GDPR**) – Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of individuals with regards to the processing of personal data and the free movement of such data for the protection of natural persons in the processing of personal data and repealing Directive 95/46/EC.

Data subject – any natural person whose identity is or can be identified and whose personal data are processed by Kaunas University of Technology.

Data processing – any action by automated or non-automated measures using the personal data: collection, recording, accumulation, storage, classification, organisation, merging with other data, creation (including creation based on other data), changing (adaptation, addition or correction), profiling, submission (transfer), publication, use, search, destruction, deletion, etc.

Data controller – a legal entity or natural person who, individually or in cooperation with others, establishes the purposes and measures of data processing.

Data processor – a legal entity or natural person authorised by the data controller to process personal data. While processing data, a data processor receives the instructions from the data controller and does not establish any purposes of the processing.

Joint data controllers – the legal entities or natural persons who jointly process personal data but each of them pursues individual purposes of the processing.

Special category personal data – information on the natural person's racial or ethnic origin, political, religious, philosophical or other beliefs, membership of trade unions, health, sexual orientation or criminal record.

Consent – specific and unambiguous expression of the properly informed data subject, given freely as a written or oral statement or by unambiguously understood actions expressing his/her consent for the processing of the related personal data.

Direct marketing – the activities of offering to the persons the services of Kaunas University of Technology and/or ask for their opinion on the provided services by mail, telephone or in another direct method. The personal data processing for the purposes of marketing requires s data subject's consent.

Kaunas University of Technology (hereinafter – University) – a legal entity code 111950581, registered office address K. Donelaičio str. 73, LT-44249 Kaunas, tel. +370 (37) 300

000, 300 421, fax +370 (37) 324 144, email ktu@ktu.lt, main website <https://ktu.edu>. In most cases, the University processes personal data as a data controller; however, depending on the situation, it can also act as a joint data controller or a data processor.

Other definitions used in the Policy have the same meaning as in the GDPR or other applicable legislation.

CHAPTER II PERSONAL DATA PROCESSING

3. The University's employees or other data processors duly authorised by the University process personal data according to the following principles:

3.1. Lawfulness, fairness and transparency – this principle obligates to process personal data only when there are legitimate grounds for processing and only in a manner making the processing operations known and understandable to a data subject;

3.2. Purpose limitation – this principle obligates to process the available personal data only for specific processing purposes. However, in some cases, the additional technical and organisational measures are implemented and the personal data are processed for the archiving purposes in the public interest or the purposes of historical or statistical research;

3.3. Data minimisation – this principle obligates to process only the amount of data required for the performance of the University's activities;

3.4. Accuracy – this principle obligates to process only the updated personal data; the inaccurate or outdated data have to be corrected or destroyed immediately;

3.5. Storage limitation – this principle prohibits to process personal data longer than it is required for the achievement of the data processing purposes unless the University has to store the personal data in the archive while performing its obligations under the law or in the public interest;

3.6. Integrity and confidentiality – this principle obligates to process personal data in the manner and using the measures ensuring that the data are protected against the unauthorised or illegal data processing, accidental loss, destruction or damage;

3.7. Accountability – this principle defines the University's obligation to provide the proof that the University follows any of the above-mentioned principles at any time.

4. The University processes the personal data based on the following legal grounds defined by the GDPR:

4.1. The University aims to make or has made and is executing a contract, agreement with a person or any other equivalent obligation;

4.2. A person has expressed his/her consent in writing or by an action;

4.3. The University has a legal obligation, i.e., the current national legislation obligates it to process personal data;

4.4. Personal data are processed in the public interest (for example, in the process of research) or for the performance of the functions assigned by the public authorities (for example, to provide information for the statistical reports prepared by the public authorities or to the law enforcement authorities, etc.);

4.5. In the University's legitimate interests if they are more important than the personal interests, for example, for a provision of high-quality and competitive services of studies, the University has to provide the teaching material to its students by electronic means, in advance making sure the recipients of this information are the University's students.

5. The University processes the data subjects' personal data for the following purposes:

5.1. Admission of students and unclassified students;

5.2. Making contracts with students and unclassified students;

- 5.3. Financing of studies, allocation of financial support, administration of taxes and insurance of the entitlement to benefits for students and unclassified students;
- 5.4. Accounting of academic employees, students and unclassified students;
- 5.5. Transfer of the data on students to the state registers and the authorities;
- 5.6. Organisation of studies and accounting of learning outcomes;
- 5.7. Organisation, performance and administration of research, experimental development and innovation activities;
- 5.8. Promotion of the results of the University's academic and research activities, dissemination of the information on the University;
- 5.9. Quality management in the University's activities;
- 5.10. Registration and administration of the members of the University's management bodies;
- 5.11. Organisation and administration of public competitions and selections for the candidates and applicants to job positions;
- 5.12. Making and termination of employment contracts, and administration of employment relationships;
- 5.13. Accounting, execution and control of remuneration, taxes and payments;
- 5.14. Accounting of the individual work planning and the implementation of scheduled activities of academic employees;
- 5.15. Organisation of the publishing process, administration and accounting of publications;
- 5.16. Performance of financial obligations and settlements, financial accounting and control;
- 5.17. Management of available material and financial resources;
- 5.18. Administration of the resources of the University's Library, control and accounting of its visitors and resources;
- 5.19. Making and administration of the contracts on accommodation services;
- 5.20. Organisation and performance of events and conferences;
- 5.21. Provision of the services of non-formal education;
- 5.22. Qualification improvement and competence development;
- 5.23. Organisation and implementation of the participation in the interinstitutional projects, exchange programmes and traineeships for academic employees and students;
- 5.24. Organisation and execution of teaching and training visits;
- 5.25. Communication with the University's employees, students, alumni, partners and other community members;
- 5.26. Authentication of a data subject in the information systems;
- 5.27. Authentication of the users of the information systems;
- 5.28. Administration of the user's accounts;
- 5.29. Handling of personal complaints, requests and other applications;
- 5.30. Video surveillance for personal security and protection of property;
- 5.31. Execution of public procurements;
- 5.32. Making, execution and administration of contracts with suppliers;
- 5.33. Making, performance and administration of partnership and cooperation;
- 5.34. Direct marketing aiming to inform about the University's services and receive reviews of the interested persons.

6. Depending on the purpose of processing, the University processes the personal data of the following categories:

- 6.1. Personal identity data, such as name, surname, personal ID number, date of birth, age, an image of the face, data of the personal identity document (title, number of the document, date of issue, expiry date), gender, citizenship, student's internal code, employee's time-card number, a country

from which he/she arrived (in the case of a student), curriculum vitae (in the case of admission), the status of an emigrant/foreigner of the Lithuanian descent (in the case of a student);

6.2. Contact data, such as the address of the place of residence, postal code, telephone number, email address, contact information of the student's or employee's close relative (if provided);

6.3. Data related to studies, such as study cycle and form, language of studies, faculty, programme and its alternatives, year of studies, semester, group, the status of studies, the period of studies, completed study modules, mobility data, form and date of assessments, evaluation of academic achievements, student's applications and supporting documents; data proving the participation in classes: attendance data, reports on systematic absence, copies of the documents justifying the absence; works of studies: answers to the written assessments, test results, written works, final degree projects, doctoral dissertations, dissertation abstracts, attestation documents, mobility documents, public presentations and defences of the students' works of studies, statements in the e-learning environment in writing, audio or video; learning activity logs: performed actions in the University's information systems, statistical data, etc.;

6.4. Data related to the planned activities of individual work and their implementation;

6.5. Data related to the obtained education and professional activities, such as education, scientific degree, pedagogical or honorary title, knowledge of foreign languages, obtained qualifications, workplace, job position, occupied part of FTE, science (artistic) fields and areas, study fields and groups of fields, history of previous employment; data of the previously obtained education that is the basis for the person's admission to studies: completed school, date of issue, code and serial number of the document proving the obtained education, date and number of the acknowledgement document of the education obtained abroad, entry competition score, results of maturity examinations; data of tuition fees: nature and sources of the financing of studies, price of the study programme, price of the study credit, payment receipts, bank account number (if provided by a student); data of the allocated financial support: application and supporting documents, type, amount of the scholarship/support, payment period, data of the loan, etc.;

6.6. Data about family, such as marital status, children/adopted children, number of supported persons;

6.7. Financial data, such as calculated remuneration and payable taxes, premiums and bonuses, income and its sources, nature of the financing of studies, amount and year of the student's basket, financial volume of the supervised projects and contracts, etc.;

6.8. Data required for the performance of financial obligations, such as bank account number and title of the financial institution, identification number of a social security payer and/or taxpayer;

6.9. Data justifying the data subjects' entitlement to benefits, such as date of birth, social status, health condition, information on the family composition, received income, need for social support, personal data of socially disadvantaged students and students with disabilities or special educational needs (if provided by a student), disability, etc.;

6.10. Data required for the insurance of the requirements of accounting and control of the migration of persons under the procedure stipulated by the legislation, such as citizenship, country of residence, place of birth;

6.11. Data required for the management of resources and assets, such as name, surname, address of the place of residence, telephone number, email address, number of the personal identity document;

6.12. Data that are created and/or received pursuant to a legal obligation, such as data received according to the inquiries by the courts, law enforcement authorities, notaries, bailiffs, lawyers, tax administrators with regards to the income, a job position at the University or the activities performed;

6.13. Video data recorded by the video surveillance equipment on the University's premises and in its territory;

6.14. Data that are submitted or generated by electronic means (information systems, email, websites, etc.), such as login to accounts, internet user's IP address, version of the operating system and parameters of the device used to access content or services; login and access information and information collected by any cookies of the websites;

6.15. For the purposes of research and statistical analysis, the University can also process the special category data. Before the processing of the special category data, the University makes sure the University's applied organisational and technical measures are sufficient and, if needed, takes additional measures for protection and insurance of the confidentiality of these data.

7. The University processes personal data in the terms required for the achievement of the set processing purpose. When the set purpose is achieved, personal data are deleted or otherwise irreversibly destroyed unless the current legislation obligates to store such personal data in the term stipulated by the legislation. After the end of the term, personal data are irreversibly deleted or destroyed. Specific terms for storage of personal data depend on the legal basis for the data processing.

8. In the processing of personal data, the University applies the organisational and technical measures of adequate level, it constantly updates and improves the systems and processes for personal data processing, regularly briefs the University's employees on the proper processing and protection of personal data.

9. The University's administrative and academic employees have the right to process personal data. The access rights to the University's information systems and personal data are granted under the procedure set out by the University and according to the functions stipulated by the job descriptions of the employees.

10. While processing personal data, the University's employees and other data processors duly authorised by the University guarantee that personal data:

10.1. Are processed according to the personal data processing policy of the University, the GDPR, the legal protection of personal data of the Republic of Lithuania, this Policy and other current legislation regulating the protection of personal data;

10.2. Are not processed for the purposes incompatible with the purposes for personal data processing set before the collection of personal data;

10.3. Are processed accurately, honestly and lawfully;

10.4. Are accurate, complete; inaccurate data have to be corrected or destroyed;

10.5. Are processed according to the organisational and technical measures of data security;

10.6. Are not transferred to the third parties unless it is stipulated by the legislation;

10.7. Are destroyed when the set storage terms of personal data end.

11. Usually, the University processes and stores personal data within the University's infrastructure. The selected data processors usually process them within the territory of the European Union (hereinafter – EU) and the European Economic Area (hereinafter – EEA); however, sometimes personal data have to be transferred to other countries outside the territory of the EU and EEA.

12. In the cases when the University transfers personal data for processing in the countries outside the territory of the EU and EEA, it applies one of the following security measures:

12.1. A contract based on the Standard Contractual Clauses approved by the European Commission is signed with the data recipient/processor;

12.2. It has to be ensured that the recipient of personal data is located in the country recognised as applying the adequate standards of personal data protection by the decision of the European Commission.

CHAPTER III PROTECTION OF THE RIGHTS OF THE DATA SUBJECTS

13. Data subjects have the following rights:

13.1. To know (be informed) about the fact that the University processes their personal data;

13.2. After the submission of a personal identity document or the use of electronic means allowing the University to properly identify a person, to get acquainted with personal data and their processing, for example, to receive the information on which personal data and from which sources are received, the purpose of their processing by the University, which data recipients the data are provided to and/or has been provided to within the last year, as well as receive the copies of the documents containing their personal data;

13.3. To demand to correct or delete personal data or limit the processing of data, except for the storage, if personal data are processed disregarding the requirements of the legislation;

13.4. To not give consent to the processing of their personal data if the University is not obligated to process personal data under the legislation;

13.5. To demand from the University to transfer the personal data submitted by the data subjects to another data controller or provide them directly to the data subjects in the form convenient to them;

13.6. If their personal data are processed based on the consent, to revoke the consent at any time;

13.7. To submit a complaint to the State Data Protection Inspectorate (address L. Sapiegos str. 17, 10312 Vilnius, tel. (8 5) 271 28 04, (8 5) 279 1445, fax (8 5) 261 9494, www.vdai.lrv.lt, email ada@ada.lt) if the data subjects think the University does not process personal data properly or does not guarantee the data subjects' rights.

14. In case of any questions regarding the privacy or personal data protection, or any concerns that the University might violate the requirements of the legislation regulating the data protection while processing personal data, apply to the following address: Kaunas University of Technology, K. Donelaičio str. 73, LT-44249 Kaunas, tel. +370 (37) 300 000, 300 421, fax +370 (37) 324 144, emails ktu@ktu.lt or duomenu.apsauga@ktu.lt.

15. If the University receives a person's request or inquiry, it responds in the manner and form preferred by the applicant within 30 (thirty) calendar days at the latest. In case an inquiry needs to be clarified, the University immediately contacts the person requesting to clarify the request or inquiry. In this case, the term for the University's response is calculated from the date of the submission of the clarified inquiry.

16. If the person gets acquainted with his/her personal data and identifies that the University has processed the data unlawfully, the University's employees or other data processors duly authorised by the University immediately inspect the lawfulness of the data processing; if the fact is confirmed, at the person's written request, destroys the unlawfully processed personal data or suspends the processing actions, except for the storage in electronic back-up copies of the data or printed copies of the documents under the procedure stipulated by the legislation.

17. If the actions of the personal data processing are suspended, the respective personal data are stored until they are corrected or destroyed (at the person's request or the end of the data storage term). Other processing actions can be performed with regards to such personal data only if:

17.1. The University aims to prove the circumstances that caused the suspension of the data processing actions;

17.2. The person gives consent regarding the further processing of his/her personal data;

17.3. The public interest, the University's rights or legitimate interests need to be protected.

18. The University immediately notifies the person specifying how the person's instruction regarding the further processing of personal data has been implemented: whether the data has/has not been corrected or destroyed, whether the data processing has been suspended. If the personal data has been processed by the data processor at the University's assignment, the University immediately

notifies the data processor regarding the data subject's instruction to correct or destroy his/her personal data or suspend the processing actions, except for the cases when submission of such an instruction to the data processor proves impossible or involves a disproportionate effort (due to a large number of the data subjects, period of data, unreasonably high costs).

19. The University carries out the inquiries of the data subjects free of charge. In some cases (if a data subject is obviously abusing his/her rights, unreasonably resubmits the requests to provide information, extracts, documents), the University has a right to require payment for the provision of such information and data to the data subject based on the principle of the coverage of demonstrable costs.

20. The University stores the data subject's inquiries and correspondence on the issues of exercising of the data subject's rights for 1 (one) year from the deadline for submission of any claims.

21. The University's data protection officer can be contacted by email duomenu.apsauga@ktu.lt.

CHAPTER IV FINAL PROVISIONS

22. This Privacy Policy can be reviewed at any time due to any new circumstances of personal data processing, changes in the legislation or detected errors.

23. The latest version of the Privacy Policy is available on the main website of the University <https://ktu.edu>.
