

Approved by Rector's directive No 27 of 10 July 2026

In force from: 10.07.2026

Regulation on the Use of Artificial Intelligence

1. General provisions

1.1. Purpose

1.1.1. The purpose of this Regulation is to regulate the use of artificial intelligence at Tallinn University of Technology.

1.1.2. The Regulation lays down the principles, conditions, restrictions and general requirements governing the use of artificial intelligence, as well as the circumstances in which additional assessment or a risk analysis is required, in order to ensure the lawful, secure, appropriate and ethical use of artificial intelligence.

1.1.3. The Regulation constitutes the general framework for the use of artificial intelligence, which serves as the basis for more detailed guidelines, rules for use and assessment procedures.

1.2. Scope of application

1.2.1. This Regulation applies to the university's employees, students and other persons acting on behalf of the university who use artificial intelligence solutions in the course of the university's work, teaching, research or support activities.

1.2.2. The Regulation applies to all artificial intelligence solutions and use cases, irrespective of whether the solution has been centrally procured, managed or provided by the university, or has been deployed at the initiative of the user. The Regulation also applies where artificial intelligence forms part of other software, services or tools.

1.3. Other university regulations and guidelines

1.3.1. The conditions governing the use of artificial intelligence may be further specified in other university regulations, rules, procedures, guidelines, codes of good practice and other relevant rules. They must be consistent with the general principles laid down in this Regulation.

1.3.2. Other university regulations and guidelines may establish additional or more stringent requirements governing the use of artificial intelligence in teaching, assessment, academic work, and research and development activities, including the acknowledgement of AI use, permitted methods of use, data processing, the use of AI-generated outputs, and other relevant conditions, taking into account the specific characteristics of the respective field.

2. Definitions

2.1. For the purposes of this Regulation, the terms defined in the Information Security Policy and the Procedure for the Processing and Protection of Personal Data shall apply. In addition, the following terms have the following meanings:

2.1.1. "**AI solution**" means a specific tool, application, service or functionality that uses artificial intelligence. An AI solution may include one or more AI systems or other automated functions.

2.1.2. "**Centrally managed AI solution**" means an AI solution procured, managed or made available for use by the university, the suitability of which has been assessed by the university and for which terms of use have been established.

2.1.3. "**Non-centrally managed AI solution**" means an AI solution that is not centrally managed, provided or made available for use by the university.

2.1.4. "**AI system**" means a machine-based system within the meaning of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) that is designed to operate with varying levels of autonomy and to infer from the input it receives outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments.

2.1.5. "**High-risk AI system**" means an AI system the use of which falls within the category of high-risk AI systems under Article 6 of the European Union Artificial Intelligence Act because it may significantly

affect a person's rights, obligations, opportunities or status, in particular in the use cases referred to in Article 6 and Annex III.

2.1.6. "**AI use case**" means a specific context in which an AI solution is used for work, teaching or research, including the purpose of its use, the data processed, the user roles and the expected outcome.

2.1.7. "**Special categories of personal data**" means personal data the processing of which is subject to enhanced requirements under applicable legislation.

2.1.8. "**Security-critical information**" means information the disclosure, alteration or misuse of which may significantly compromise the security of the university's information systems, services or data, including passwords, cryptographic keys, authentication data, certificates, security settings and other similar information.

2.1.9. "**Employee**" means a natural person who performs work at the university under an employment contract, provides services to the university under another valid contract, or acts under the authority of the university.

2.1.10. "**Student**" means a student within the meaning of subsection 4 (1) of the Academic Policies and a doctoral student within the meaning of subsection 4 (1) of the Regulations for Doctoral Studies.

2.1.11. "**User**" means an employee, student or other person acting on behalf of the university who uses an AI solution in the course of the university's work, teaching or research activities.

3. Principles for the use of artificial intelligence

3.1. General principle

3.1.1. Artificial intelligence is used at the university as a tool supporting work, teaching and research activities. Artificial intelligence shall be used lawfully, appropriately and securely, and under the control of the employee, student or other person using the AI solution.

3.1.2. When using an AI solution, the user must maintain meaningful control, be able to intervene in the generation of the output and, where necessary, stop, modify or reject the output.

3.2. Lawfulness and security

3.2.1. When planning and implementing an AI use case, the confidentiality, integrity and availability of the university's information, information systems and tools shall be ensured, and data protection requirements must be complied with. An AI use case shall not be planned or implemented in a manner that unjustifiably increases the risk of data leakage, unauthorised modification, misuse or any other security incident.

3.3. Human oversight and transparency

3.3.1. The person responsible for the AI use case shall review the output before it is used and, where necessary, correct, supplement or reject it.

3.3.2. For a high-risk AI use case, sufficient transparency shall be ensured to enable the user to correctly interpret the output of the AI solution. Where appropriate, it shall also be clearly indicated that the content has been generated or modified using artificial intelligence.

3.4. Use of artificial Intelligence for assessment and decision-making

3.4.1. An AI use case shall not involve the use of an AI solution as the sole basis for decisions in academic assessment, admission, candidate selection, suitability assessment, ranking or other decision-making processes that may affect a person's rights, obligations, opportunities or status.

3.4.2. In such processes artificial intelligence may be used only as a preparatory tool, provided that its use is appropriate for its intended purpose, remains under meaningful human control, and the final decision is made by a human.

3.4.3. Where a proposed AI use case may constitute a prohibited AI practice or involve the use of a high-risk AI system within the meaning of the Artificial Intelligence Act, a documented preliminary assessment shall be carried out before its use in accordance with Chapter 6 of this Regulation. The use of AI is permitted only after the required approval has been obtained.

3.4.4. The use of AI shall not create the misleading impression that a decision or assessment has been made solely by automated means. Content generated or modified using AI shall be clearly identified whenever this is not otherwise readily apparent to the recipient or user.

3.5. Prohibited AI practices

3.5.1. Artificial intelligence shall not be used in a manner that is unlawful or constitutes a prohibited AI practice referred to in Article 5 of the EU Artificial Intelligence Act. Prohibited uses include, for example, the use of artificial intelligence for subliminal, manipulative or deceptive techniques, exploiting the vulnerabilities of persons, social scoring, assessing the risk of criminal offending based solely on profiling or personal characteristics, the untargeted scraping of facial images to create or expand facial

recognition databases, emotion recognition in workplaces and educational institutions, biometric categorisation, and real-time remote biometric identification in publicly accessible spaces, unless a limited exception is provided for by law.

4. Principles for the use of AI solutions

4.1. Centrally managed AI solutions

4.1.1. AI solutions centrally managed by the university may, by default, be used by the university's employees, students and other persons acting on behalf of the university, provided that they are used in accordance with the applicable terms of use and restrictions. The list of centrally managed AI solutions, the applicable terms of use, restrictions and, where necessary, additional guidelines shall be published on the website ai.taltech.ee.

4.2. Non-centrally managed AI solutions

4.2.1. Where an employee, student or other person acting on behalf of the university intends to use a non-centrally managed AI solution, he or she shall, before implementing the specific AI use case, ensure that the use is appropriate for its intended purpose, lawful, and complies with this Regulation, data protection requirements, information security requirements and any other applicable university guidelines.

4.2.2. A non-centrally managed AI solution may be used only if such use is not contrary to this Regulation or applicable law and complies with the applicable terms of use and restrictions.

4.2.3. Where a specific AI use case falls within the scope of Chapter 6 of this Regulation, the preliminary assessment and approval procedure laid down in that Chapter shall be completed before the AI use case is implemented.

4.2.4. The university may publish recommendations, terms of use and other relevant materials relating to AI solutions on the university's website ai.taltech.ee. Such materials are intended to assist users in selecting AI solutions but do not replace the assessment of a specific AI use case or relieve users of their obligation to comply with the applicable requirements.

4.3. AI solutions used by students

4.3.1. A student may use AI solutions of his or her choice for learning, independent study, supporting his or her studies and other routine academic activities, including when using the university's learning materials and other study-related information, provided that such use is not restricted by legislation governing studies or other applicable university requirements.

4.3.2. Students are not required to carry out a separate risk assessment when processing public information, anonymised data, synthetic or sample data, or other low-risk information.

4.3.3. Where a student intends to use an AI solution in academic work to process personal data, non-public information or other restricted datasets, the student shall comply with the applicable university guidelines and requirements and obtain the prior approval of the lecturer, supervisor or other appropriate responsible person for the specific AI use case.

5. Principles for the use of data in AI solutions

5.1. General rule

5.1.1. Only data that are necessary, lawful and permitted for the relevant work, teaching or research activity may be entered into or processed using an AI solution.

5.1.2. University data shall not be used for training, fine-tuning or developing AI solutions unless such use has been separately assessed, authorised and organised by the university, including as part of a research or development project.

5.1.3. When selecting and using an AI solution, users shall consider the type of data, the purpose and legal basis of the processing, the suitability of the AI solution for the intended use, and the associated risks.

5.2. Use of data in centrally managed AI solutions

5.2.1. A centrally managed AI solution may be used to enter and process information required for carrying out a work, teaching or research task, including personal data, information designated for internal use and other work-related information, provided that the processing is appropriate for its intended purpose and necessary for carrying out that task.

5.2.2. When processing personal data, the applicable legal bases for processing and the principles of data minimisation and necessity shall be observed, and particular attention shall be paid to the processing of data relating to students.

5.2.3. Where the lawfulness of the processing is unclear or the AI use case falls within the scope of Chapter 6 of this Regulation, a preliminary assessment shall be carried out before processing.

5.2.4. When processing the data referred to in this clause, the prohibitions and exceptions set out in clause 5.4 shall be observed.

5.3. Use of data in non-centrally managed AI solutions

5.3.1. Only public, anonymised or synthetic information, and other low-risk information, may be entered into or processed in a non-centrally managed AI solution.

5.3.2. Personal data, security-critical information, information designated for internal use, other information subject to access restrictions, and any other information subject to legal, contractual or risk-based restrictions may be processed in a non-centrally managed AI solution only on the basis of a preliminary assessment and the required approval in accordance with Chapter 6 of this Regulation.

5.4. Restricted and prohibited data

5.4.1. Passwords, cryptographic keys, authentication data, private keys used with digital certificates, access tokens and other access credentials shall not be processed in any AI solution.

5.4.2. State secrets, classified foreign information or other information subject to an equivalent level of protection may be processed in an AI solution only where this is expressly permitted by law and takes place in an environment specifically designated for that purpose, in accordance with the prescribed procedures and conditions.

6. Preliminary assessment, risk assessment and approval

6.1. General principle

6.1.1. Where a proposed AI use case may constitute a prohibited AI practice or involve the use of a high-risk AI system within the meaning of the Artificial Intelligence Act, or where the use case involves restricted data, significant risks associated with the processing, or any other unusual or high-risk use, a documented preliminary assessment shall be carried out before the AI use case is implemented.

6.1.2. The purpose of the preliminary assessment is to determine whether the AI use case is permitted, permitted subject to conditions, or prohibited, and to identify any additional measures, restrictions or approvals that may be required.

6.2. Cases requiring a preliminary assessment

6.2.1. A preliminary assessment is required in particular where:

6.2.1.1. the AI use case may constitute a prohibited AI practice;

6.2.1.2. the AI use case may involve the use of a high-risk AI system;

6.2.1.3. the AI use case may affect a person's rights, obligations, opportunities or status;

6.2.1.4. the AI use case may give rise to significant information security, data protection or legal risks;

6.2.1.5. a non-centrally managed AI solution is used to process information other than public, anonymised or synthetic information;

6.2.1.6. a non-centrally managed AI solution is used to process information designated for internal use, information subject to access restrictions, or other restricted information; or

6.2.1.7. the terms of use, the type of data, the service provider, the location of the data processing, or any other material circumstance changes.

6.3. Procedure for the preliminary assessment

6.3.1. The Information Security Division shall be responsible for the preliminary assessment, risk assessment and approval process.

6.3.2. Where necessary, the data protection officer, legal officer, area director, process owner or another person with the appropriate competence shall be involved.

6.3.3. Requests and any supporting information shall be submitted by e-mail to cybersecurity@taltech.ee.

6.4. Outcome of the preliminary assessment

6.4.1. The preliminary assessment shall determine whether the AI use case is permitted, permitted subject to conditions, or prohibited.

6.4.2. Where the AI use case is permitted subject to conditions or only after the required approval has been obtained, the necessary restrictions, safeguards and responsibilities shall be specified.

6.5. Documentation and reassessment

6.5.1. The preliminary assessment, risk assessment, approval, any exceptions, restrictions and any reassessment shall be documented in a manner that enables subsequent review and audit. Where the circumstances of the AI use case change, the preliminary assessment shall be carried out again where necessary.

7. Responsibility

7.1. The person responsible for the AI use case shall, within the scope of his or her role and responsibilities, be responsible for the use of the AI solution, the lawfulness and permissibility of the data entered into the AI solution, and the use of outputs generated or processed using AI. Responsibility cannot be transferred to an AI solution or its service provider.

7.2. Where the AI use case falls within the scope of Chapter 6 of this Regulation, the responsible person shall ensure that the preliminary assessment, risk assessment and any required approval have been completed before the AI use case is implemented.

7.3. The Information Security Office shall be notified immediately of any suspected information security, data protection or other incident related to the use of an AI solution by e-mail at cybersecurity@taltech.ee.

7.4. The university shall ensure that guidance relevant to users' roles and the intended use of AI solutions is available and that training is provided where necessary. More detailed guidance and information on the approval process shall be published on the website ai.taltech.ee.

8. Review and updating

8.1. This Regulation shall be reviewed at least once a year or whenever significant legal, technological or organisational changes occur.

8.2. The necessity, adequacy and relevance of this Regulation shall be assessed against the requirements of the Artificial Intelligence Act, data protection legislation, information security requirements, contractual obligations, and the university's internal regulations and guidelines.