Approved by Rector's directive No 147 of 20 May 2013
Amended by Rector's directive No 83 of 25 May 2016
Amended by Rector's directive No 15 of 31 March (entry into force 01.04.2021)
Amended by Rector's directive No 9 of 3 February 2022 (entry into force 01.02.2022)

In force from: 01.02.2022

Procedure for Processing and Protection of Personal Data

1. General provisions

1.1 The Procedure for Processing and Protection of Personal Data (hereinafter Procedure) applies to processing and protection of personal data at Tallinn University of Technology (hereinafter TTÜ).

1.2 The Procedure has been drawn up in compliance with the requirements established in the Personal Data Protection Act (hereinafter Act) and other legislation regulating processing and protection of personal data.
1.3 The Procedure has been drawn up on the basis of the advisory guidelines on processing and protection of personal data provided by the Data Protection Inspectorate for the implementation of the Act.

2. Definitions used in the Procedure

2.1 **Personal data** – any data concerning an identified or identifiable natural person, regardless of the form or format in which such data have been submitted.

2.2 **Sensitive personal data –** the following data concerning a natural person:
2.2.1 data revealing political opinions (except data relating to being a member of a political party);
2.2.2 data revealing religious or philosophical beliefs;
2.2.3 data revealing ethnic or racial origin;
2.2.4 data on the state of health or disability;
2.2.5 data on genetic information (genetic data);
2.2.6 biometric data (above all fingerprints, palm prints, eye iris images);
2.2.7 information on sex life;
2.2.8 information on trade union membership;
2.2.9 information concerning commission of an offence or falling victim to an offence before a public court hearing, or making of a decision in the matter of the offence or termination of the court proceeding in the matter.

2.3 **Private personal data** – personal data the disclosure of which may materially breach the inviolability of the private life of a natural person.

2.4 **Data subject –** a natural person whose personal data are processed.

2.5 **Data carrier containing personal data** – any object whereto personal data have been recorded.

2.6 **Processing of personal data –** any act performed with personal data, including collection, recording, organisation, storage, alteration, disclosure, granting access to personal data, consultation and retrieval, use of personal data, communication, cross-usage, combination, closure, erasure or destruction of personal data or several of the aforementioned operations, regardless of the manner in which the operations are carried out or the means used.

2.7 **Processor of personal data** – TTÜ as a legal person in public law who processes personal data or on whose assignment personal data are processed.

2.8 **Employee processing personal data** – an employee, who processes personal data.

2.9 **Head of the structural unit processing personal data** – the head of the structural unit, where personal data are processed.

2.10 **Protection of personal data** – application of organisational, physical, technical and electronic information security measures upon processing of personal data.

2.11 **Organisation of protection of personal data** – ensuring compliance with the requirements for processing and protection of personal data.

2.12 **Coordinator for protection of personal data** – an employee, whose official duty is to organise protection of personal data.

2.13 **Personal data information system** – an information system, including technical equipment, used for electronic processing of personal data.

2.14 **Main user of the personal data information system** – an employee, whose official duty is to administer the personal data information system.

2.15 **Rooms for personal data processing** – the rooms, where personal data are processed.

2.16 **Unauthorised person** – a person, including a TTÜ employee, who does not have the right of access to personal data.

2.17 **Person with need for access** – a natural or legal person, a state or local government agency or a branch of a foreign company, who needs to access personal data.

3. Persons responsible for compliance with the requirements for processing and protection of personal data

3.1 At TTÜ, persons shall be responsible for compliance with the requirements for processing and protection of personal data as follows:
3.1.1 the Rector shall be responsible for compliance with the requirements for processing and protection of personal data;
3.1.2 the coordinator for protection of personal data shall be responsible for the organisation of protection of personal data;
3.1.3 the head of the structural unit processing personal data (hereinafter head of the structural unit) shall be responsible for compliance with the requirements for processing and protection of personal data in the structural unit;
3.1.4 an employee processing personal data (hereinafter employee) shall be responsible for compliance with the requirements for processing and protection of personal data upon processing of a data carrier containing personal data;
3.1.5 the main user of the personal data information system shall be responsible for compliance with the requirements for processing and protection of personal data in the personal data information system administered by the main user.

4. Coordinator for protection of personal data

4.1 The Rector shall appoint a coordinator for organising protection of personal data who shall:
4.1.1 audit and verify on a regular basis that TTÜ processes and protects personal data in compliance with the Act and this Procedure and any other legislation;
4.1.2 take appropriate measures at TTÜ for bringing into compliance with the requirements for processing and protection of personal data;
4.1.3 maintain a data processing register of the data processor;
4.1.4 advise the employees on a daily basis in the issues of processing and protection of personal data;
4.1.5 conduct training for employees on a regular basis in the issues of processing and protection of personal data.

4.2 The Personnel Office shall notify the Data Protection Inspectorate of appointment of a coordinator for protection of personal data by providing his or her name and contact details.

4.3 A coordinator for protection of personal data is functionally independent of the processor of personal data.

4.4 A coordinator for protection of personal data shall consult the Data Protection Inspectorate in the issues concerning the application of organisational, physical, technical and electronic information security measures upon processing and protection of personal data.

5. Head of structural unit

5.1 The head of a structural unit shall coordinate processing and protection of personal data in the structural unit pursuant to the requirements of this Procedure.

5.2 The head of a structural unit shall determine, in cooperation with the coordinator for protection of personal data, the purposes of processing of personal data and the categories of personal data to be processed.

5.3 The head of a structural unit shall decide on granting access to data carriers containing personal data of the structural unit and communication of personal data in compliance with the Act and other legislation by consulting the coordinator for protection of personal data.

5.4 The head of a structural unit shall make sure that personal data are not disclosed to unauthorised persons.

5.5 The head of a structural unit shall determine, in cooperation with the coordinator for personal data protection, the rooms for processing personal data of the structural unit and the persons' rights of access to the locked room, where personal data of the structural unit are processed.

5.6 The head of a structural unit has the right to grant permission to an employee to process data carriers containing private personal data outside TTÜ premises with prior approval of the coordinator for protection of personal data.

5.7 The head of a structural unit is required to contact the coordinator for protection of personal data in matters concerning the requirements for processing and protection of personal data.

5.8 The head of a structural unit shall coordinate the organisational, physical, technical and electronic information security measures applied for protection of personal data with the coordinator for protection of personal data.

5.9 The head of a structural unit is required to notify:
5.9.1 the head of the Internal Audit Office and the coordinator for protection of personal data in case the protective measures for communication, storage, preservation and destruction of data carriers containing personal data prove to be insufficient; [entry into force 01.02.2022]
5.9.2 the head of the Real Estate Office and the coordinator for protection of personal data in case the measures for protection of personal data in the room for processing of personal data prove to be insufficient; [entry into force 25.05.2016]
5.9.3 the main user of the personal data information system and the coordinator for protection of personal data, in case the measures for protection of personal data in the personal data information system prove to be insufficient.

5.10 The head of a structural unit shall submit information on compliance with the requirements of this Procedure in accordance with the established format to the coordinator for protection of personal data by 30 November each year.

5.11 In case of violation of the requirements for processing and protection of personal data of the structural unit, the head of a structural unit is required to contact immediately the coordinator for protection of personal data in order to eliminate the violation.

6. Employee

6.1 An employee shall process the data carriers containing personal data pursuant to the requirements of this Procedure.

6.2 An employee shall apply organisational, physical, technical and electronic information security measures upon processing of personal data in order to prevent unauthorised processing of personal data.

6.3 An employee shall make sure that the following is prevented in the room for processing personal data:
6.3.1 unauthorised access to personal data;
6.3.2 unauthorised transfer of data carriers containing personal data.

6.4 An employee shall make sure that personal data are not disclosed to unauthorised persons in the course of data transfer.

6.5 An employee shall, when taking a data carrier containing personal data out of TTÜ premises, apply information security measures to prevent unauthorised access to personal data.

6.6 An employee, who transfers or transports personal data, shall make sure that unauthorised reading, copying or destruction is prevented upon transfer or transportation.

6.7 In case of an electronic data carrier containing personal data, an employee shall make sure that after disposal the data are securely erased from the electronic data carrier or overwritten, if possible. Disposed electronic data carriers, from which data cannot be erased electronically, must be destroyed physically.

6.8 An employee is required to participate in a training on processing and protection of personal data once in every two years.

6.9 An employee is required to contact the coordinator for protection of personal data in matters concerning the requirements for processing and protection of personal data.

6.10 In case an employee becomes aware of violation of the requirements for processing and protection of personal data, the employee is required to notify immediately the head of the structural unit and the coordinator for protection of personal data.

6.11 An employee is required to maintain confidentiality of the personal data which become known to the employee in the performance of his or her duties even after performance of his or her duties relating to processing of the personal data, or after termination of his or her employment in accordance to the deadlines set out in legislation.

7. Main user of the personal data information system

7.1 The main user of the personal data information system shall coordinate processing and protection of personal data in the information system pursuant to the requirements of this Procedure.

7.2 The main user of the personal data information system shall make sure that in the personal data information system:
7.2.1 it would be subsequently possible to ascertain the details related to access to personal data and communication, storage, modification or deletion of personal data;
7.2.2 each user of the personal data information system has access only to personal data permitted to be processed by him or her and to the data processing to which the user is authorised;
7.2.3 unauthorised reading, copying and modification or deletion of personal data is prevented upon communication of personal data.

7.3 The main user of the personal data information system shall make sure that security rules are prepared and established for administration of the personal data information system.

7.4 The main user of the personal data information system shall, in cooperation with the head of a structural unit and the coordinator for protection of personal data, determine the rights of access of the users of the personal data information system and other authorisations in the personal data information system.

7.5 The main user of the personal data information system shall obtain approval of the coordinator for protection of personal data in order to introduce a new personal data information system.

7.6 The main user of the personal data information system is required to submit to the coordinator for protection of personal data the following data concerning the administered equipment and software :
7.6.1 the name, type, location and name of the producer of the equipment;
7.6.2 the name, version and name of the producer of the software, and the contact details of the producer.

7.7 The main user of the personal data information system shall make sure that the personal data information system can be used by telecommuting if compliance with the requirements for data security arising from the Act, this Procedure and other legislation has been ensured and the head of the structural unit has granted permission for that with the approval of the coordinator for protection of personal data.

7.8 The main user of the personal data information system is required to contact the coordinator for protection of personal data in matters concerning the requirements for processing and protection of personal data.

7.9 In case the main user of the personal data information system becomes aware of violation of the requirements for processing and protection of personal data, he or she is required to notify immediately the coordinator for protection of personal data.

8. Requirements for processing of personal data

8.1 A structural unit is required to process personal data:
8.1.1 in a legal manner, i.e. personal data shall be collected only in an honest and legal manner;
8.1.2 with high quality, i.e. the personal data processed shall be up-to-date and complete;
8.1.3 in a secure manner, i.e. security measures shall be applied in order to protect personal data;
8.1.4 in a purposeful manner, i.e. personal data shall be collected only for the achievement of determined and lawful objectives;
8.1.5 minimally, i.e. personal data shall be collected only to the extent necessary for the achievement of determined objectives;
8.1.6 by taking into account participation of the data subject, i.e. the data subject shall be notified of data collected concerning him or her, the data subject shall be granted access to the data concerning him or her and the data subject has the right to correct the data, if necessary.

8.2 A structural unit may process personal data without the consent of the data subject:
8.2.1 on the basis of law;
8.2.2 for performance of a contract entered into with the data subject or for ensuring the performance of such contract (unless the data to be processed are sensitive personal data);
8.2.3 in individual case for the protection of the life, health or freedom of the data subject or other person if obtaining the consent of the data subject is impossible.

8.3 A structural unit may transfer personal data to a person with need for access or grant such person access to personal data without the consent of the data subject if the person with need for access:
8.3.1 processes personal data for the performance of a task prescribed by legislation;
8.3.2 requests information obtained or created in the process of performance of public duties provided by an Act or legislation issued on the basis thereof and the data requested do not contain any sensitive personal data and access to it has not been restricted for any other reasons;
8.3.3 processes personal data in individual cases for the protection of the life, health or freedom of the data subject or other person if obtaining the consent of the data subject is impossible;
8.3.4 processes personal data for the needs of scientific research or official statistics in a coded form by applying the required information security measures.

8.4 A structural unit shall keep records on paper or electronically concerning which personal data, for what purpose, to whom and when are released.

8.5 A structural unit shall determine the objectives of processing of personal data pursuant to the Act and other legislation.

8.6 A structural unit shall process the collected personal data only for purposes conforming to the objectives of data processing.

8.7 A structural unit may communicate the collected personal data to another structural unit if the objectives of processing of personal data of the relevant structural units are overlapping or in concord.

8.8 For processing the collected personal data for purposes different from the initial purpose, a structural unit shall obtain a written consent of the data subject in a format which can be reproduced in writing.

8.9 A written consent of a data subject shall clearly define the following information:
8.9.1 the data for the processing of which permission is given;
8.9.2 the purpose of the processing of the data ;
8.9.3 the persons to whom communication of the data is permitted;
8.9.4 the conditions for communicating the data to persons with need for access;
8.9.5 the rights of the data subject concerning further processing of his or her personal data.

8.10 The burden of proof of the consent of a data subject lies on the structural unit.

8.11 A structural unit is required to erase or close personal data which are not necessary for achieving the purposes.

8.12 A structural unit shall determine the categories of personal data to be processed in compliance with the Act and other legislation.

8.13 At the request of a data subject, the structural unit shall communicate the following to the data subject:
8.13.1 the personal data collected in the structural unit concerning the data subject;
8.13.2 the purposes of processing of his or her personal data;
8.13.3 the categories and sources of his or her personal data;

8.13.4 the persons with need for access to whom transfer of the personal data is permitted;
8.13.5 the persons with need for access to whom the personal data of the data subject have been transferred.

8.14 If a person requests information which contains restricted personal data concerning him or her or third persons, the structural unit shall identify the person making the request for information. If a person requests restricted personal data concerning a third person, the structural unit shall ascertain the basis and purpose of accessing the information.

8.15 A structural unit may restrict the rights of a data subject to receive information and personal data concerning him or her if this may:
8.15.1 damage rights and freedoms of other persons;
8.15.2 endanger the protection of the confidentiality of filiation of a child;
8.15.3 hinder the prevention of a criminal offence or apprehension of a criminal offender;
8.15.4 complicate the ascertainment of the truth in a criminal proceeding.

8.16 A structural unit is required to provide a data subject with information and the requested personal data or state the reasons for refusal to provide data or information within five working days after the date of receipt of the corresponding request. TTÜ may demand a fee of up to 0.19 euros per page for release of personal data on paper starting from the twenty-first page.

8.17 A structural unit shall make sure that the personal data processed are up-to-date and accurate.

8.18 In case of incomplete or inaccurate personal data, the structural unit shall:
8.18.1 immediately take measures for amendment or rectification of the personal data;
8.18.2 close the personal data which are contested on the basis of accuracy until the accuracy of the data is verified or the accurate data are determined;
8.18.3 store inaccurate data with a notation concerning their period of use together with supplemented and amended data;
8.18.4 upon rectification of personal data, inform the persons who provided the personal data or to whom the personal data were forwarded if this is technically possible and does not result in in disproportionately high costs.

8.19 In precontractual negotiations or upon preparation of an employment contract, the structural unit may ask the person applying for employment only for data with regard to which TTÜ has legitimate interest. A structural unit shall not request personal data which disproportionately concern the private life of a person or which are not related to his or her suitability for a job.

8.20 A structural unit shall ask the employee’s consent for publishing data concerning his or her birthday on TTÜ Intranet.

8.21 A structural unit shall not grant access through the document register to electronic documents containing private or sensitive personal data registered in the document register and administered in the document management system.

8.22 A structural unit shall consider, before allowing processing of personal data for journalistic purposes and disclosure in the media, if there is predominant public interest for it and disclosure of data does not cause excessive damage to the rights of the data subject. A structural unit shall contact the data subject, if necessary, for deciding the relevant issue.

8.23 Audio, photographic or video recordings related to natural persons may be published on TTÜ website only if the natural person agrees to the recording or it is a public event. If a natural person does not agree to disclosure of his or her personal data on TTÜ webpage, the structural unit who published the data shall remove the relevant personal data from the TTÜ website.

8.24 In the access control system and surveillance equipment used in TTÜ premises, personal data are processed for the purposes of ensuring access of persons and security of property. The personal data in the access control system and surveillance equipment can be processed for other purposes only with the approval of the head of the Real Estate Office and the coordinator for protection of personal data. [entry into force 25.05.2016]

8.25 Information on the surveillance equipment in the premises and on the territory of TTÜ, which transfers and records personal data for the protection of property, shall be provided on the relevant notification signs, which include TTÜ’s contact details.

9. Requirements for protection of personal data

9.1 A structural unit shall apply information security measures for the protection of personal data upon processing of the personal data.

9.2 A structural unit shall store the data carriers containing personal data in the room for processing of personal data of the structural unit.

9.3 It must be ensured that personal data cannot be accessed by unauthorised persons in the room for processing of personal data of the structural unit.

9.4 The room for processing of personal data of a structural unit has:
9.4.1 a security and fire alarm system;
9.4.2 a lockable door and an access control system.

9.5 In case the measures for information security in the room for processing of personal data of the structural unit prove to be insufficient, the structural unit is required to apply additional security measures (lockers, lockable shelves, drawers, etc.) for storage of data carriers containing personal data.

9.6 The room for processing of personal data of the structural unit shall be locked and the security alarm must be turned on by the last employee of the structural unit leaving the room.

9.7 An unauthorised person my stay in the room for processing of the personal data of the structural unit only at the presence of an employee of the relevant structural unit.

9.8 If an unauthorised person staying in the room for processing of the personal data of the structural unit can gain access to personal data, the structural unit is required to apply additional security measures (lockers, lockable shelves, drawers, etc.) for storage of data carriers containing personal data.

9.9 Data carriers containing sensitive personal data shall be stored in a locker, on a lockable shelve, in a lockable drawer or in the archival repository.

9.10 In exceptional cases, data carriers containing sensitive personal data may be processed outside TTÜ premises with the permission of the coordinator for protection of personal data.

9.11 The following shall be guaranteed in the personal data information system:
9.11.1 confidentiality of personal data, i.e. unauthorised persons cannot access personal data;
9.11.2 availability of personal data, i.e. a user of the information system can access only to permitted personal data and for permitted data processing;
9.11.3 integrity of personal data, i.e. personal data have not been altered accidentally or intentionally.

9.12 The structural unit who grants the rights of access to the rooms for personal data processing or information systems shall make sure that the obligation to guarantee confidentiality is established in a contract for the provision of support services (maintenance, repairs, ancillary works, cleaning, support and technical work, surveillance tasks, etc.) entered into with natural or legal person needing access.

9.13 Upon disposal of electronic data carriers, personal data shall be securely erased from the electronic data carrier and overwritten, if possible. For the purposes of secure erasure of personal data a special secure erasure software or a magnetic erasing device that complies with the standard DIN 33858, level A3 or B3, shall be used.

9.14 The electronic data carriers, from which data cannot be erased electronically, must be destroyed physically.

9.15 In a structural unit data carriers containing personal data, the need for use of which has ended and the storage period of which has expired, shall be destroyed by secure shredding.

9.16 For shredding data carriers containing personal data the following shredders shall be used:
9.16.1 for destruction of ordinary personal data on paper, a shredder complying with the standard DIN 32757 No. 2 or DIN 663997 level P2 (maximum strip width 6 mm);
9.16.2 for destruction of private and sensitive personal data, a shredder complying with the standard DIN 32757 No 3 or DIN 663997 level P3 (maximum strip width 2 mm maximum or material particle size 4x60 mm);
9.16.3 for destruction of ordinary personal data on an electronic data carrier, a shredder complying with the standard DIN 66399, classes O, T, E, F, H, level 2;
9.16.4 for destruction of private and sensitive personal data on an electronic data carrier, a shredder complying with the standard DIN 66399 classes O, T, E, F, H, level 3.

9.17 In case of a larger amount of data carriers containing personal data, the structural unit may, by agreement with the Internal Audit Office, collect the data carriers for secure destruction. [entry into force 01.02.2022]

10. Violation of requirements for processing and protection of personal data and elimination of such violation

10.1 If violation of the requirements for processing and protection of personal data is detected, the coordinator for protection of personal data shall immediately take necessary measures for reducing the damage caused by the violation.

10.2 If violation of the requirements for processing and protection of personal data is detected, the coordinator for protection of personal data is entitled to issue an order to the head of the structural unit for temporary suspension of processing of personal data in the structural unit.

10.3 The coordinator for protection of personal data shall take an explanation from the person who has violated the requirements for processing and protection of personal data.

10.4 The coordinator for protection of personal data shall make proposals to the employee who violated the requirements for processing and protection of personal data and the head of the structural unit for elimination of the violation.

10.5 The coordinator for protection of personal data shall notify the Rector of the violation of the requirements for processing and protection of personal data and the proposals made for the elimination thereof.

10.6 The Rector shall issue orders to the head of the structural unit who violated the requirements for processing and protection of personal data for elimination of the violation.

10.7 In order to improve processing and protection of personal data, the coordinator for protection of personal data shall make proposals to the head of the structural unit for application of appropriate measures for processing and protection of personal data.

10.8 The coordinator for protection of personal data shall conduct follow-up inspection of elimination of the violation of the requirements for processing and protection of personal data in the structural unit.

10.9 In case of failure to take the required measures for elimination of violation of the requirements for processing and protection of personal data, the coordinator for protection of personal data shall notify the Rector and the Data Protection Inspectorate of the violation.

10.10 In case a person fails to comply with the requirements for processing and protection of personal data, the person may be prosecuted under the law.