General privacy notice of the Tampere higher education community

The University of Tampere and Tampere University of Technology have merged to create the new Tampere University on 1 January 2019. Together, the new Tampere University and Tampere University of Applied Sciences comprise the Tampere higher education community (hereinafter the "Community").

The Community processes the personal data of, for example, its students, employees, those with resource agreement, short-term guests, customers and other stakeholders in context of its operations. The Community is committed to protecting the rights and privacy of individuals and to complying with applicable data protection legislation. This Privacy Policy outlines the practices and principles that we follow while processing personal data.

Please note that this Privacy Policy and other privacy notices may be updated from time to time. The most recent version of the Privacy Policy is always available on this web page.

This privacy notice was updated on 26 August, 2021.

1. Purpose of processing personal data

As a data-intensive organisation, the Community processes personal data for multiple legitimate purposes, such as:

- **Legal obligation**: The University may process your personal data to meet its legal obligations. We may process your data to comply with legal requirements (such as obligations imposed on the Community as an employer or in the context of providing education and related support services), to ensure the safety and security of the Community and the continuity of our operations, to satisfy our statutory reporting requirements, and in response to lawful requests by public authorities.
- **The Community's legitimate interests:** The Community may store and process your personal data when it is necessary for the purposes of the Community's legitimate interests. We may, among other things, send you information about our activities and carry out processing activities for the purpose of analysing, maintaining and developing our operations and services.
- **Tasks carried out in the public interest or in the exercise of official authority:** We may process your personal data in the public interest, for scientific or historical research purposes, for statistical or archiving purposes, or in the exercise of official authority vested in the Data Controller.
- **Consent:** We may process your personal data with your explicit consent. Personal data is regularly processed on the basis of consent, for example, in marketing activities of the Community. You may withdraw your consent at any time. If you withdraw consent, we will immediately stop processing your data if there are no other lawful basis for the processing.
- **Contract:** We may process your personal data if the processing is necessary for the performance of a contract to which you are party or in order to take steps at your request before entering into a contract. We may, for example, process the personal data of the users of our services, our customers, and candidates for an open position at the Community. This lawful basis does not apply if there are other reasonable and less intrusive ways to meet contractual obligations or take the steps requested.

- **Vital interests:** We may process your personal data under exceptional circumstances in order to address an urgent problem or minimize damages that you might otherwise incur. This type of processing protects your vital interests.

2. What type of personal data do we collect?

The lawful basis for processing personal data determines the types of data that we collect. We may, for example, collect the following types of data:

- General personal information, such as name, personal identification number, address and contact details.
- Data related to the study rights of students, their student benefits, academic records and student support services.
- Employment data, such as the type and duration of an employment contract, an employee's unit, job title, salary, fees, and holiday entitlement.
- Data related to safety and security, such as access rights of the members of the campus community, camera surveillance and facility bookings.
- Data related to the use of our services, including this website, such as cookies and facility bookings.
- Data required for research, statistical or archiving purposes (the data is anonymised to the maximum extent possible to prevent re-identification).

3. Cookies on our website

The Community's website uses cookies. The use of cookies is described in more detail elsewhere.

4. Disclosing personal data

We process personal data only within the Community and to the extent necessary for the fulfilment of the stipulated purpose. We may disclose personal data to third parties only in the following circumstances:

Your consent: Your personal data may be disclosed with your express consent for example for uses relating to third-party services.

The Community's service providers: The Community may outsource data processing by entering into an agreement with an external service provider. Personal data is then processed on the Community's behalf by an external service provider to fulfil a purpose specified by the Community. The Community remains the Data Controller.

The Community and the external service provider are mutually responsible for the protection of your data. Your personal data may only be disclosed to the extent necessary contracted service provider to provide services for the Community for the purposes specified by the Community.

If processing activities are outsourced, the Community shall only employ service providers with the expertise and resources to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data. All external service providers must comply with data protection legislation.

Partners: Our Community maintains close ties with a broad range of partners. For example, we engage in collaborative activities with national and international research and educational institutions, pursue educational collaboration, provide services (such as sports services) to data subjects, and collaborate with the Student Union. This type of collaboration may necessitate the sharing of personal data between the partners. We shall only disclose your personal data to our partners to the extent necessary to pursue such collaboration or provide services.

For research purposes: We may disclose data for research purposes in compliance with data protection legislation.

For legal reasons: We may disclose your personal data to third parties, for example, if there is a statutory or legal obligation to disclose the data or if it necessary in order to detect, prevent or address misconduct or security or technical issues. We will always inform you of this type of processing, if possible.

Legal obligations under the Act on the Openness of Government Activities: The Finnish Act on the Openness of Government Activities (621/1999) applies to the Community's activities. The documents and data stored in the personal records held by the Community are generally considered public under the constitutional principle of publicity and the provisions of the Act on the Openness of Government Activities, unless they are defined as non-public under applicable laws. The Act on the Openness of Government Activities governs the disclosure of data.

5. International data transfers

The Community ensures that your personal data is processed within the EU and the EEA. However, the Community's services and activities may, in some cases, be implemented by using service providers, services or servers located outside the EU and the EEA. It is therefore possible that your personal data is transferred outside the EU and the EEA, for example, to the United States. The EU's General Data Protection Regulations (GDPR) imposes strict requirements for the transfer of data to countries where data protection legislation differs from the GDPR. The Community is committed to providing adequate levels of protection when transferring personal data outside the EU and the EEA and to ensuring that external service providers comply with data protection legislation.

6. Data protection principles

Data protection is an integral part of the Community's information security policy and general administration. The Community collects and processes personal data only through systems and databases that are compliant with the information security policy. Personal data is stored in locked and monitored facilities or in systems and databases that are only accessible by authorized users. Access to personal data is limited to authorized persons who process personal data in connection with their professional responsibilities or to maintain services provided by the Community. Any use of personal data that is unauthorized or contrary to the specific purpose for the processing is strictly prohibited.

7. Rights of data subjects

Unless stipulated otherwise in data protection legislation, data subjects have the following rights:

- **Right of access:** You are entitled to find out what information the Community holds about you or to receive confirmation that your personal data is not processed by the Community.
- **Right to rectification:** You have the right to have any incorrect, inaccurate or incomplete personal details held by the Community revised or supplemented. You are also entitled to

have any unnecessary personal data erased from our records. If such a request is refused, we will provide you with a written notice that specifies the reasons for the refusal. The notice will also include instructions for appealing against the decision, such as filing a complaint with the relevant supervisory authorities.

- **Right to erasure** ('right to be forgotten'): In certain circumstances, you have the right to have your personal data erased from our records. This right to erasure does not apply, if the processing is necessary in order for the Community to comply with legal obligations or perform tasks carried out in the exercise of official authority. The storage and deletion of personal data held by the Community is governed by our Archive Management Policy and the statutory retention periods for different types of data.
- **Right to restrict processing:** In certain circumstances, you have the right to request the Community to restrict processing your personal data until the accuracy of your data or the basis for processing your data has been appropriately investigated and potentially revised or supplemented.
- **Right to data portability:** You have the right to obtain a copy of the personal data that you have submitted to the Community in a commonly used, machine-readable format and transfer the data to another Data Controller. This right applies to situations where data is processed automatically on the basis of consent or contract. The right to data portability does not therefore apply to data processing that is necessary for the performance of a task carried out in the public interest or to fulfil legal obligations imposed on the Data Controller.
- **Right to object:** You may at any time object to the processing of your personal data for special personal reasons, if the basis for processing is a task carried out in the public interest, the exercise of official authority, or the Community's legitimate interests. After receiving such a request, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for processing your data.
  You have an absolute right to prevent your data from being used for direct marketing purposes.
- **Right to lodge a complaint with a supervisory authority:** You have the right to lodge a complaint with a supervisory authority, if you consider that the processing of your personal data violates the provisions of the EU's General Data Protection Regulation (EU 2016/679) or other data protection legislation.

Office of the Data Protection Ombudsman

Visiting addresss: Lintulahdenkuja 4, 00530 Helsinki
Postal address: PL 800, 00531 Helsinki, Finland
E-mail: tietosuoja@om.fi
Phone: 02956 66700

In addition, you may follow other administrative procedures to appeal against a decision made by a supervisory authority or to seek a judicial remedy. You also have the opportunity to take legal action against a Data Controller or Data Processor, if you consider that your rights have been violated through non-GDPR compliance.

8. Enforcement of the rights of data subjects

We strive to make the management of personal data as easy as possible for our data subjects. Our students, employees and guests have the opportunity to review the general data that the Community processes via the Community's self-service portals.

Other subject access requests and requests concerning the rights of data subjects are made to the Community's data protection officer (see section 9). The data subject's identity will be verified to ensure that the person requesting the information is the data subject. Data subjects may verify their identity by presenting official photo ID (European driving license, passport or an identity card issued by the police authorities). Student card provided by the Student Union of Tampere University or TAMKO with a valid annual registration sticker and an identifiable photo can also be accepted.

We will make every effort to respond to your request within 30 days. If we are, for a justifiable reason, unable to respond within this period, we will inform you of the delay and the cause thereof within 30 days. However, we always respond to requests no later than three months after the date of receipt.

9. Who do I contact with questions about data protection?

The data controller is Tampere higher education community (business ID 2844561-8), visiting address Kalevantie 4, 33014 Tampereen yliopisto (Tampere University) or Tampere University of Applied Sciences (business ID 1015428-1), visiting address Kuntokatu 3, 33520 Tampere (TAMK).

The requests concerning the rights of data subjects are made to DPO of the Tampere higher education community (by email to dpo@tuni.fi, or by post to DPO, Tampere University, 33014 Tampere University).

The data subject's identity will be verified when disclosing the data at latest to ensure that the person requesting the information is the data subject. The data subject's identity can be verified already at the time of request.

If you have other questions regarding the data processed by the Community, you can contact the DPO by email using the contact information above.