

General privacy notice of the Tampere higher education community

This privacy notice describes how we process your personal data in compliance with data protection legislation. In data protection legislation, the term “data subject” refers to the person whose personal data are processed. In this privacy notice, we refer to the data subject as “you” and to the controller as “we”.

This privacy notice may be updated or edited if necessary. You will be notified of any significant changes as mandated by data protection legislation.

Updated: 18 September 2026.

1. Controller

Depending on the activity, the controller of your personal data is:

Tampere University Foundation sr (Tampere University)

Business ID: 2844561-8

Visiting address: Kalevantie 4, 33014 Tampere University, Finland

Tampere University of Applied Sciences Ltd (TAMK)

Business ID: 1015428-1

Visiting address: Kuntokatu 3, 33520 Tampere, Finland

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

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

2. Scope and purpose of data processing

This privacy notice describes the common personal data processing practices of Tampere University and Tampere University of Applied Sciences, which together form the Tampere higher education community (the “Community”). More detailed information on personal data processing is provided in activity-, service- or research-specific privacy notices. This general notice applies together with those notices.

The Community processes the personal data of, for example, its students, employees, those with a resource agreement, short-term guests, customers and other stakeholders in the context of its operations. The Community is committed to protecting the rights and privacy of individuals and to complying with applicable data protection legislation.

3. Lawful basis for processing personal data

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

- **Legal obligation:** The Community 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 is 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.

4. Sources and types of personal data

Depending on the circumstances, we may collect personal data either directly from you or from other sources.

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).

Whether providing personal data is mandatory and the consequences of not providing it depend on the activity or service concerned. Further information is provided when the data are collected or in the activity-specific privacy notice.

Cookies on our website

The Community's website uses cookies. The use of cookies is described in more detail [elsewhere](#).

5. Data processors, disclosures and international transfers

Personal data processors

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 external service provider processes personal data in accordance with the Community's instructions and the data processing agreement. Your personal data may only be disclosed to the extent necessary for the 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.

We also use AI-assisted services to support work tasks and document processing.

The Community uses the following personal data processors, among others, in its work and support services. The services used depend on the activity concerned.

Name of processor	Location of processor	Service provided	Geographical location of processing
Efecte Finland Oy	Finland	Service request management	EU/EEA
Microsoft	EU/EEA	Microsoft 365 communication and office services, including Copilot	EU/EEA
Legora AB	Sweden	AI-assisted document work	EU/EEA

Other personal data processors are described in activity-specific privacy notices.

Disclosures of 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.
- **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 is 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.

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 Regulation (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. Protecting personal data

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. Retention period for personal data

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.

8. Profiling and automated decision-making

Further information about any profiling or automated decision-making is provided in the activity-specific privacy notice.

9. Data subjects' rights and how to exercise them

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.
- **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 address: Lintulahdenkuja 4, 00530 Helsinki, Finland

Postal address: PO Box 800, 00531 Helsinki, Finland

Email: 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.

Exercising 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 1). 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 one month. 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 one month. However, we always respond to requests no later than three months after the date of receipt.