Privacy Notice

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 on 19 October 2026.

1. Controller

The controller of your personal data is:

Tampere University Foundation sr. (Tampere University)
Business ID: 2844561-8
Kalevantie 4 FI-33100 Tampere, Finland

The contact person for registry matters is Sari Nieminen, sari.nieminen@tuni.fi, tel. +358 50 462 7382. To call Tampere University’s switchboard, dial +358 (0) 294 52 11.

The Data Protection Officer is Sanna Vartia, sanna.vartia@tuni.fi, tel. +358 50 431 8075. For general data protection questions, you can also contact dpo@tuni.fi.

2. Scope and purpose of data processing

Tampere University Foundation’s Centralised IT Resource User Registry. Personal data are processed as part of the centralised IT services of Tampere Universities.

Personal data are processed for the management, monitoring and statistical analysis of identities and access rights, troubleshooting, maintaining the hardware registry for support services, resolving user issues and providing customer service. Processing enables centralised electronic authentication and login to Microsoft 365 services. IT system logs are also collected and statistically analysed.

Personal data are also processed to ensure the security, availability and continuity of IT services and to detect and investigate misuse and security incidents. This includes protecting web services against malicious traffic and processing logs for security monitoring.

3. Lawful basis for processing personal data

The lawful bases for processing depend on the purpose:

Performance of a contract (Article 6(1)(b) of the General Data Protection Regulation): managing identities and access rights for centralised IT services and providing the related services.

Compliance with a legal obligation (Article 6(1)(c)): ensuring information security insofar as necessary to fulfil the obligations under Article 32 of the General Data Protection Regulation and section 13 of the Act on Information Management in Public Administration (906/2019).

Performance of a task carried out in the public interest (Article 6(1)(e)): ensuring the security and availability of web services used to perform the tasks referred to in section 2 of the Universities Act (558/2009).

4. Sources and types of personal data

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

You as the data subject.

Regular data sources include the personnel information system, educational information systems and the teacher training school's pupil register. Data are also generated through the use and security monitoring of IT and web services.

We will process the following types of personal data:

Basic information: name, personal identity code, personnel number, student number, national learner identifier, username, email address, date of birth, nationality, gender and contact details.

Employment contract information: contract number, validity period, priority, faculty or unit, job title, validity of work release, supervisor, and cost centre or equivalent financial allocation.

Study right information: contract number, validity period, attendance information, priority, faculty or unit and degree programme. For the teacher training school, grade level and validity period of the study right.

Resource agreement information: contract number, validity period, faculty or unit, responsible person, agreement type and description.

Access authorisation information: responsible unit and validity period.

Microsoft 365 messaging services process name, username, email address, responsible unit, supervisor information, and the individual's background and contact information.

Technical data: logs from access authorisation management, authentication services, Active Directory (AD) and Microsoft 365.

Security monitoring also involves processing IP addresses and other network identifiers, timestamps, web request URLs, parameters and headers, and threat and event information.

Web requests and logs may contain usernames, authentication information and personal data in request content. Processing is limited to data necessary for security purposes.

We will process data on the following categories of data subjects:

Staff, students, teacher training school pupils, applicants, visitors, partners and other users of IT or web services. Security logs may also contain information relating to sources of external traffic.

The identification and access authorisation data needed to use services requiring personal access rights must be provided. Without these data, the services concerned cannot be used. The use of web services also generates technical logs.

5. Transfer and disclosure of personal data

Data are used in the University's internal services, such as student and personnel registers. Data are disclosed to Haka federation services with the individual's consent. Microsoft 365 services, printing services and other service providers receive the personal data necessary to provide their services.

Logs are not disclosed to external parties for independent use. Data may be disclosed to the police or other authorities when investigating a security incident or criminal offence where there is a statutory basis for disclosure. Service providers may process logs on behalf of the University.

Data processors process personal data on behalf of the University under contracts and in compliance with statutory obligations. These processors include:

Microsoft: cloud services.

Ricoh: printing services. Ricoh receives information on role-based printing rights and allocated printing balances.

Fortinet, Inc.: protecting web services and related processing of personal data.

Juniper Networks, Inc.: network and network access management and related processing of personal data.

When Fortinet provides web service protection, personal data may be transferred to Fortinet, Inc. in the United States. Transfers are based on the European Commission's adequacy decision for the EU–US Data Privacy Framework (DPF). Fortinet, Inc. participates in this framework.

When Juniper provides network management, personal data may be transferred outside the European Economic Area, including to the United States. Transfers are based on the European Commission's standard contractual clauses.

6. Protecting personal data

Your personal data will be protected using appropriate technical and organisational measures. We will protect your data through technical measures, including antivirus software, firewalls and regular software updates. When logging in, users are required to provide a username and password and, in certain cases, use two-factor authentication.

Registry data are not public. Those handling data are bound by confidentiality and non-disclosure obligations. University staff are granted access only where their duties require processing the data. Logs are collected in a separate system with access restricted to designated individuals. The University’s premises have access control.

Processing is limited to data necessary for the purpose. In security monitoring, identifiers are masked or pseudonymised where possible when full identifying information is not needed.

Any physical documents will be safeguarded by storing them in locked facilities.

7. Retention period for personal data

We will retain your personal data for only as long as necessary, as determined on a case-by-case basis. The retention period also depends on statutory requirements. We will adhere to our Data Management Plan and all applicable legislation when determining the retention period of personal data.

In access authorisation management, personal data are retained for two years after the last access authorisation expires. The AD access authorisation, including Microsoft 365, is disabled for 92 days and then deleted. Personal data are removed from authentication services as soon as the individual’s access authorisations end.

Attack logs are retained in Fortinet’s protection service for a maximum of four months. Attack logs exported from the service to the University’s centralised security monitoring are normally retained for no more than two years from the logged event.

Data needed to investigate a security incident or suspected offence, or for legal claims, may be separated from these logs. They are retained only for as long as necessary, up to a maximum of five years from the event.

In Juniper’s network management service, network and device data are normally retained for a maximum of 60 days and audit logs for a maximum of six months. Data used for analytics may be retained for a maximum of one year.

8. Profiling and automated decision-making

Registry data are used for automated individual decisions, including profiling, to establish personal electronic identities, individual roles, role-based basic access authorisations and

automatic groups. Roles include staff, staff-equivalent users, students, visitors and teacher training school students.

Automatically blocking malicious traffic to protect web services is a technical safeguard, not an automated individual decision with significant effects on a person within the meaning of Article 22 of the General Data Protection Regulation.

9. Data subjects' rights and how to exercise them

Data protection legislation affords certain rights to data subjects, depending on the lawful basis for processing their personal data. Under certain circumstances, your rights may be restricted, for example, due to our legal obligations or if personal data are processed for scientific research, statistical or archiving purposes. If your rights have been restricted, we will implement appropriate and necessary technical and organisational measures to protect your privacy. As a data subject, you have the following rights which you can exercise by sending us a request.

Right of access

You have the right to request confirmation of whether we hold your personal data and to receive a copy of the data we hold.

Right to rectification

You have the right to request that any incorrect or incomplete personal data we hold about you be revised or supplemented. You can also request to have any unnecessary personal data erased from our records.

Right to erasure

Under certain circumstances, you have the right to request the erasure of your personal data (“right to be forgotten”). This right does not apply insofar as processing is necessary to comply with a legal obligation or to perform a task carried out in the public interest.

Right to restrict processing

You may have the right to restrict the processing of your personal data in certain cases defined by law. For example, this right may apply if you believe the personal data we hold about you is incorrect or that your data are being processed in violation of data protection legislation, or if you have opposed the processing of your data.

Right to object

You have the right to object, on grounds relating to your particular situation, to processing based on a task carried out in the public interest. We will then assess whether there are grounds under the law to continue processing.

Right to data portability

Under certain circumstances, you have the right to receive personal data you have provided to us in a structured, commonly used and machine-readable format and to transmit the data to another controller. This right applies to automated processing based on consent or a contract, not to security-related processing based on a legal obligation or a task carried out in the public interest.

Right not to be subject to automated decision-making

You have the right not to be subject to decisions based solely on automated processing (such as profiling) that produce legal effects concerning you or otherwise similarly and significantly affect you. However, there are exceptions to this prohibition.

Withdrawing consent

If your personal data is being processed based on your consent, you have the right to withdraw your consent at any time.

Right to lodge a complaint with a supervisory authority

You have the right to lodge a complaint with a supervisory authority (Data Protection Ombudsman), if you believe that the processing of your personal data violates data protection legislation.

Office of the Data Protection Ombudsman
Street address: Lintulahdenkuja 4, FI-00530 Helsinki, Finland
Postal address: PO Box 800, FI-00531 Helsinki, Finland
Switchboard: +358 29 56 66700
Fax: +358 29 56 66735
Email address: tietosuoja@om.fi
Requests to exercise your rights follow the University’s information request process. You can submit a request to the registry contact person or the Data Protection Officer using the contact details above.