Privacy Notice

dated 05.01.2024

Tampere University Foundation's Centralised IT Resource User Registry

1. **Data Controller**

   Tampere University Foundation

   Address: Kalevantie 4, 33100 Tampere, Finland

   Phone: +358 3 355 111

   Business ID: 2844561-8

2. **Contact Person for Registry Matters**

   Jussi-Pekka Pispa

   Email: jussi-pekka.pispa@tuni.fi

   Phone: 040 75 444 66

3. **Data Protection Officer**

   Sanna Vartia

   Email: sanna.vartia@tuni.fi

   Phone: 050 431 8075

4. **Registry Name**

   Tampere University Foundation's Centralized IT Resource User Registry

5. **Purpose of Processing Personal Data and Legal Basis**

   Purpose:

   - Management, monitoring, and statistics of centralized IT services' identities and access rights for Tampere universities, troubleshooting, hardware registry for support services, resolving user issues, customer service, enabling centralized electronic authentication, and facilitating login to Office365 services (identities and access rights). Additionally, collecting and statistically analyzing IT system log data.

   Legal basis:

   - Contract

6. **Contents of the Registry**

   Basic information:

   - Identifying details (name, personal identification number, personnel number, student number, national learner identifier, username, email address), as

well as the individual's birthdate, nationality, gender, and contact information.

Contract information:

- Employment contract: contract number, validity period, priority, faculty (unit), job title, validity of work release, supervisor, cost center or equivalent financial allocation.
- Study right: contract number, validity period, attendance information, priority, faculty (unit), degree program.
- Resource agreement: contract number, validity period, faculty (unit), responsible person, contract type, description.
- Normaalikoulu (teacher training school) study right: grade level, validity period.

Access authorization information: responsible unit, validity period.

Office365 messaging service details: name, username, email address, responsible unit, supervisor information, and relevant background and contact information.

Log data from access authorization management, authentication services, Active Directory (AD), and Office365.

7. **Regular Sources of Information**

- Personal data system
- Educational information systems
- Normaalikoulu student register
- Information provided by the data subject.

8. **Regular Disclosures of Data and Recipient Groups**

Regular disclosures to third parties:

- Internal services, e.g., student and personnel registers.
- Haka federation services with the individual's consent.
- Office365 services.
- Printing services.
- Necessary personal data may be disclosed to external service providers for service implementation.

Log data is not disclosed externally. However, in the event of a security incident investigation or criminal investigation, the university may have the right to disclose information to the police or other authorities.

The processing of personal data in the registry has been outsourced through a service agreement:

- Yes, additional information about outsourced processing:

        - Office 365 messaging services are cloud-based.
        - Printing services are provided by Ricoh. Ricoh receives information related to role-based printing rights and granted printing balances.
    - External partners process personal data based on contracts and comply with legal obligations related to personal data processing.

9. **Transfer of Data Outside the EU or EEA**

    Are registry data transferred to a third country or international organization outside the EU or EEA?

    - No

10. **Principles of Data Protection**

    Registry data is not public. Those handling the data are bound by confidentiality and non-disclosure obligations.

    Access to the registry requires a personal username and password, granted only to university staff members whose roles and responsibilities are associated with the mentioned access rights. Access control is in place for the controller's premises.

    The log registry data is collected in a separate system, and access rights are restricted only to designated individuals.

11. **Retention Period for Personal Data or Criteria for Determining Retention Time**

    In access authorization management, an individual's data is retained for 2 years after the expiration of their last access authorization to protect their privacy.

    The access authorization for Active Directory (including Office365) is disabled for 92 days, after which it is removed.

    Personal data from authentication services is immediately deleted once an individual's access authorizations have ended.

12. **Information on the Existence of Automated Decision-Making or Profiling, and Information on the Logic and Significance of Processing for the Data Subject**

    The registry data is used for automated individual decisions, including profiling for the following purposes:

    - Tampere universities' personal electronic identity.
    - Individual roles (staff, staff equivalent, student, visitor, TNK student).
    - Basic access authorizations based on roles.
    - Automatic groups.

13. **Rights of the Data Subject**

    When the data controller processes personal data, it must take appropriate measures to ensure the exercise of data subjects' privacy rights. It must also facilitate the use of these rights by the data subjects.

- Right to Access Data:

  The data subject has the right to know whether their personal data is being processed and what personal data about them is stored.

- Right to Rectification:

  The data subject has the right to request that incorrect, inaccurate, or incomplete personal data concerning them be corrected or supplemented without undue delay. Additionally, the individual has the right to request unnecessary personal data to be deleted.

- Right to Erasure:

  In exceptional cases, the data subject has the right to have their personal data completely erased from the data controller's registers (right to be forgotten).

- Right to Restriction of Processing:

  In certain situations, the data subject has the right to request the restriction of processing of their personal data until their information has been properly verified, corrected, or supplemented.

- Right to Object:

  In specific circumstances, the data subject has the right to object to the processing of their personal data based on their personal, specific situation.

- Right to Data Portability:

  In certain situations, the data subject has the right to receive their personal data, which they have provided to the data controller, in a structured, commonly used, and machine-readable format, and the right to transfer this data to another data controller.

- Right to Lodge a Complaint with a Supervisory Authority:

  The data subject has the right to lodge a complaint with the supervisory authority responsible for their habitual residence or place of work if they believe that the processing of their personal data violates the EU General Data Protection Regulation (EU) 2016/679. Additionally, the individual has the right to use administrative remedies and other legal protections.

  Requests related to the exercise of data subject rights should follow the data controller's information request process.