

Privacy Notice – TCSC AI Cluster

In this privacy notice we provide you with the information required by data protection legislation on how we process personal data. Data protection legislation uses the term “data subject” for the person to whom the personal data relate. In this privacy notice we refer to the data subject as “you” and to the controller as “we”. In this document, this system is referred to as the AI Cluster.

This system is used to develop and run various research-related programs.

- This privacy notice covers the processing of the personal data of the users and administrators of this system, regardless of the type of research use for which the user has been granted access to the system.
- This privacy notice does not cover the processing of personal data contained in the programs developed by the system’s users or any other processing of personal data within research projects. Each research project or other user party is responsible for the privacy notice required for the processing of personal data carried out in its own operations.

This privacy notice may be updated or amended where necessary. If a change is significant, we will inform you in the manner required by law.

This privacy notice entered into force on 9.6.2026.

1. Controller

The controller of the personal data of the users and administrators of this system is:

Tampere University Foundation sr (Tampere University)
2844561-8
Kalevantie 4, 33100 Tampere, Finland

The contact person for matters concerning the processing is Juha Nisso (juha.nisso@tuni.fi).
The university switchboard can be reached at +358 (0) 294 52 11.

For general questions relating to data protection, you can contact the Data Protection Officer at dpo@tuni.fi.

2. Subject and purpose of the processing

The processing forms a personal data file, “AI Cluster users”.

The purpose of processing personal data is to maintain the user and access rights data of the AI Cluster, which are processed in order to manage user accounts, enable use of the system, monitor processing and maintain information security.

3. Legal basis for the processing

The basis for processing your personal data is:

- ☐ consent (of the data subject)
- ☐ performance of a contract
- ☐ compliance with a legal obligation of the controller
- ☐ protection of vital interests
- ☒ performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- ☐ legitimate interests of the controller or a third party

If special categories of personal data (e.g. health data, data relating to criminal convictions) are processed, the basis is:

- ☐ explicit consent (of the data subject)
- ☐ protection of vital interests where consent cannot be given
- ☐ establishment, exercise or defence of legal claims
- ☐ another basis under data protection legislation, as specified in national law:

4. Sources of personal data and the data processed

Depending on the situation, personal data may be collected either directly from you or from other sources. Data are obtained:

- ☒ from you as the data subject
- ☐ from the following regular data sources:

We process the following categories of personal data:

- ☒ General personal data:
 - Name
 - User ID
 - Access rights data
 - Contact details
 - Login data and times of use, including log data on system use
- ☐ Special categories of personal data, so-called sensitive data:
 - ☐ Health data:
 - ☐ Racial or ethnic origin

- ☐ Political opinions or religious/philosophical beliefs
- ☐ Trade union membership
- ☐ Sexual behaviour or orientation
- ☐ Genetic data
- ☐ Biometric data for the purpose of uniquely identifying a person
- ☐ Data relating to criminal convictions or offences

☒ Technical data: Online identifiers (IP addresses used by the system user, browser type and other similar technical data on devices, as well as other corresponding technical data necessary for the use of the system and for information security)

☐ Other data:

We process the data of persons belonging to the following groups of data subjects:

☒ Employees ☒ Students ☐ Research participants ☒ Researchers ☐ Other

The provision of personal data is not a statutory or contractual requirement. Failure to provide personal data may, however, prevent access from being granted or the system from being used.

5. Transfers and disclosure of personal data

This privacy notice does not apply to situations in which a user processes datasets outside the EU/EEA. If the data permit for research datasets also allows the datasets to be processed from outside the EU/EEA via a remote connection, the controller of the dataset covered by the data permit is in that case responsible for the transfer bases and for the safeguards required for the transfer of personal data under data protection legislation.

☒ Your personal data are not transferred outside the EU/EEA

☐ Your personal data are transferred outside the EU/EEA as follows: . The transfer mechanism and safeguards are as follows:

☒ Your personal data are not disclosed to other controllers on a regular basis.

☐ Your personal data may be disclosed to other controllers on the basis of legislation as follows:

.

Your personal data may also, on a case-by-case basis, be processed by processors with whom we conclude appropriate data processing agreements.

6. Protection of personal data

Your personal data are protected using appropriate technical and organisational safeguards. We protect your data technically by means such as virus protection, a firewall and regular software updates. In addition, we require a password and user ID at login and, where appropriate, two-factor authentication.

We also protect your data by organisational means. Our staff are bound by confidentiality and access to data is restricted internally. Where necessary, we also implement specific additional safeguards, such as separate storage locations.

Any manual materials are protected by storing them in locked facilities.

7. Retention period of personal data

Your personal data are retained for the period assessed to be necessary on a case-by-case basis. Retention periods are also affected by the requirements of legislation. In retaining personal data we comply with our records management plan (TOS) and applicable legislation, and the retention of the system's personal data is tied to the expiry dates of data permits and access rights.

In this context, your personal data are retained as follows:

- Social welfare and health data under the Act on the Secondary Use of Health and Social Data are retained in the environment for the period of validity of the data permit and are destroyed no later than 6 months after the data permit ends.
- Access rights data are destroyed 12 years after the access right ends.
- Usage log data are destroyed 12 years after the data permit ends.

8. Profiling and automated decision-making

Your personal data are not used for profiling or automated decision-making.

9. Data protection rights and how to exercise them

Data protection legislation guarantees you certain rights as a data subject. The rights depend in part on the basis for processing personal data. In certain cases, your rights may be restricted, for example owing to a legal obligation on our part or where processing is carried out for the purposes of scientific research, statistics or archiving. If your rights are restricted, we will implement the appropriate and necessary safeguards required by law. You have the following data protection rights, which you may exercise by submitting a request to that effect.

Right of access

You have the right to obtain information on the processing of personal data and to access the personal data concerning you.

Right to rectification

You have the right to request the rectification of inaccurate and incomplete personal data. You also have the right to require that unnecessary personal data be deleted.

Right to erasure

In certain situations, you have the right to request the erasure of your data (the so-called right to be forgotten).

Right to restriction of processing

You may have the right to restrict the processing of personal data in the cases laid down by law. The right to restriction may apply, for example, if you consider the personal data concerning you to be inaccurate, if they are processed unlawfully, or if you have objected to the processing of your data.

Right to object

In certain situations you have the right, on grounds relating to your personal situation, to object to the processing of your personal data.

Right to data portability

In certain situations, you have the right to request the transfer of the personal data you have provided yourself from one system to another.

Right not to be subject to automated decision-making

You have the right not to be subject to a decision based solely on automated processing, such as profiling, which produces legal effects concerning you or similarly significantly affects you. There are, however, exceptions to this prohibition.

Withdrawal of consent

Where the processing of your personal data is based on 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 the supervisory authority (the Data Protection Ombudsman) if you consider that the processing of your personal data infringes data protection legislation.

Office of the Data Protection Ombudsman

Visiting address: Lintulahdenkuja 4, 00530 Helsinki

Postal address: P.O. Box 800, 00531 Helsinki

Switchboard: 029 56 66700

Fax: 029 56 66735

Email: tietosuoja@om.fi