

Privacy Notice – Secure Operating Environment VISU

This privacy notice describes how the University of Oulu collects and processes your personal data when you act as a user of the VISU secure operating environment. Users of the VISU secure operating environment include individuals processing data under the Act on the Secondary Use of Social and Health Data (the “Secondary Use Act”) as well as those handling other types of data in the VISU environment. Additionally, University of Oulu personnel who maintain the system are considered users.

Data controller

University of Oulu
Pentti Kaiteeran katu 1
P.O. Box 8000
90014 OULUN YLIOPISTO

Responsible person for matters related to the VISU secure operating environment:
Chief Information Officer Kari Keinänen

Contact point for matters related to the VISU secure operating environment:
VISU-support@oulu.fi

Contact details of the University of Oulu Data Protection Officer: dpo@oulu.fi

Kommentoinut [JO1]: visu-support@oulu.fi

Purpose of processing personal data and legal basis for processing personal data

Those who have received a data permit under the Secondary Use Act may process datasets specified in the permit within the VISU secure operating environment provided by the University of Oulu. VISU may also be used for processing datasets for purposes other than those defined in the Secondary Use Act. The personal data of individuals identified in the data permit, those processing non-Secondary Use Act data, and University of Oulu personnel acting as system users are processed for the purposes of managing user credentials, enabling data processing and monitoring data processing activities.

The environment complies with the regulation set by the Finnish Social and Health Data Permit Authority (Findata) in accordance with Section 24(2) of the Secondary Use Act “Requirements for other service providers' secure operating environments” (1/2022 Diary number THL/214/14.00.07/2022). Compliance with these requirements necessitates the processing of personal data of both users and administrators.

Legal Basis for Processing:

Article 6(1)(c) of the GDPR: Processing is necessary for compliance with a legal obligation to which the controller is subject.

Article 6(1)(b) of the GDPR: Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Categories of Personal Data Processed

The following categories of personal data are processed within the secure operating environment:

1. Users authorized under a data permit or other basis:
 - First and last name
 - Personal identity code
 - Contact details
 - Username
 - Login data and timestamps
 - Network identifiers (e.g., log data such as date, time, IP address, browser type)
2. University of Oulu personnel acting as system administrators
 - First and last name
 - Username
 - Login data and timestamps
 - Network identifiers (e.g., log data such as date, time, IP address, browser type)

Origin of personal data

Personal data of the users is collected from the user when the secure environment order form is completed (name, personal identity code, and contact details). Other personal data is recorded when the environment is deployed and during its use.

Recipients or categories of recipients of personal data

In addition to the University of Oulu, the service provider of the service management system processes the names and contact details of users included in the order form which is delivered via the service management system. Personal data is not regularly disclosed to other data controllers.

Data transfers

Data is processed in Finland for the purpose of maintaining the environment and providing the service. Information stored in the service management system (usernames, personal identity codes, and contact details from the order form) is stored in a cloud-based database within the EU/EEA. No data is transferred outside the EU/EEA or to international organizations.

Data storage time

Personal data of users and administrators is retained for 12 years after the end of access rights. Usage log data is retained for 12 years after the expiration of the data permit authorizing the use. Storage times are defined in the Secondary Use Act.

Automated Decision-Making and Profiling

Your personal data is not used for automated decision-making or for any other purpose than those described in this privacy notice.

General description of the technical and organisational protection measures

The VISU secure environment complies with Findata's requirements for other service providers' secure operating environments.

Only individuals whose job duties require it may process your personal data. The University as the Data Controller uses appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against damage or loss.

Data Subject Rights

You have the following rights as a data subject:

- Right to access your data
- Right to have inaccurate data corrected (make sure to keep your contact information up to date)
- In certain situations, the right to have data erased ("right to be forgotten")
- In certain situations, the right to restriction of processing
- In certain situations, the right to object to processing
- In certain situations, the right to have data transferred from one system to another if the processing is based on consent or agreement and is performed automatically.

Please note that the applicability and scope of your above-mentioned rights will be specified on a case-by-case basis in accordance with the EU General Data Protection Regulation, depending on e.g. the grounds for processing the data, and that you do not have the above-mentioned rights in all cases.

If you have any questions about your rights, you can communicate with the University's Data Privacy Officer or the contact person of the responsible unit.

If you want to use the above-mentioned rights, please send a request to the University's registry office: kirjaamo@oulu.fi, where you will get the necessary additional instructions.

Right of appeal to the supervisory authority

In addition to the rights mentioned above, you have the right to file a complaint about the processing of your personal data with the Office of the Data Protection Ombudsman as the supervisory authority. The contact details and opening hours can be found on [the website of the Data Protection Ombudsman](#).