



VISU7-002 Terms of Service

Document ID: VISU7-002

Document Version: 1.0

effective Date: 17.6.2026

Document title: Terms of service

Author: Sauli Holappa

Revision history

Version	Effective Date	Reviewers	Significant Changes
1.0	17.6.2026	Samuli Malinen Janne Suokas	First version
2.0	3.9.2026	Janne Suokas	Updating 8. Exporting results Derived from Data Outside the User Environment

Table of Contents

Revision history	1
1. Introduction	2
2. Ordering and Formation of the Agreement.....	3
3. Responsibilities	5
4. Data transfer into the Service	5
5. Access Rights and User Authentication	6
6. Use of the Service	6
7. User Account Suspension	7
8. Exporting results Derived from Data Outside the User Environment	7
9. Closure of the User Environment and Termination of the Agreement.....	8
10. Data protection	8
11. System Integrity and Security	9
12. General Obligations	9
13. Procedure in Cases of Detected Misuse	9
14. Subcontracting of Service provision	10
15. Scheduled maintenance Windows and other Service Interruptions.....	10
16. Amendments to the Terms	10
17. Force Majeure	10
18. Governing Law and Dispute resolution	11

1. Introduction

By using VISU (the "Service"), a secure computing environment provided by the ICT Services of the University of Oulu (UO), you agree to these Terms of Use and the information security practices described in the Privacy Notice.

The Service is provided and maintained by the University of Oulu.

Visiting address:

Pentti Kaiteran katu 1, Linnanmaa

Postal address:

P.O. Box 8000

FI-90014 University of Oulu

Telephone: +358 294 480 000

Email: ict@oulu.fi

The current service instructions, pricing information, Privacy Notice, and these Terms of Use are available on the University of Oulu ICT Services websites at ict.oulu.fi or patio.oulu.fi (login required).

The Service is a secure processing environment as defined in Section 20 of the Finnish Act on the Secondary Use of Health and Social Data (552/2019, the "Secondary Use Act") and complies with the requirements for secure processing environments issued by the Finnish Social and Health Data Permit Authority Findata ("Findata") (Regulation 1/2022).

2. Ordering and Formation of the Agreement

Orders for the Service (the "User Environment") and any changes thereto shall be submitted using the order and change request forms designated by the University of Oulu ICT Services and completed in accordance with the applicable instructions. The forms are completed electronically and submitted to the service management system for processing by the administrators.

The persons who require access to the User Environment must be listed on the order form. Ordering the Service and obtaining access rights require University of Oulu user credentials and an affiliation with the University of Oulu.

The ordering party ("Customer") is identified on the order form and may be either an organization or a natural person. The individuals listed on the order form become customers of ICT Services. An agreement ("Agreement") between the Customer and ICT Services (the "Parties") for the provision of the Service is formed once ICT Services (VISU Administration) has approved and confirmed the order.

Customers are not provided with a separate order confirmation. However, the administration may acknowledge receipt of the order and inform the Customer when the deployment of the environment has begun.

VISU Administration shall approve an order provided that the approval criteria are met and all information requested on the order or change request form has been correctly completed in accordance with the instructions, including any required attachments. ICT Services reserves the right to reject an order if the form is incomplete or if there is no legal basis for the order. In such cases, the form will be returned to the applicant for completion.

Where the User Environment is associated with a data permit, only the contact person designated in the permit, or another comparable natural person acting as the permit holder, may order the Service. If the original contact person is no longer available to ICT Services during the validity period of the permit, the permit and Service authorization must be renewed, even if the replacement contact person is listed in the permit as another authorized data processor.

For modifications to the Service, the new contact person must provide ICT Services with an amendment decision to the data permit indicating the new contact person. If such documentation is unavailable, ICT Services may request written confirmation from the organization of the original contact person.

The Customer must promptly notify ICT Services of any changes to a data permit affecting datasets, users, or access rights.

The Customer shall provide ICT Services with sufficient and accurate information necessary for service delivery and shall otherwise reasonably cooperate with ICT Services. The Customer is responsible for the accuracy and maintenance of all information and instructions provided.

If the software available within VISU is insufficient for the Customer's needs, customizations may be implemented. All customizations are performed by a system administrator. If required software is not included in the service portfolio, the Customer shall provide the installation media, and the administrator shall perform the installation. The Customer is solely responsible for ensuring software licensing compliance and for all licensing-related costs.

The Service is subject to a fee.

Charges and the designated payer shall be agreed upon when acquiring the Service. Costs will be allocated either to a cost center or project number.

The Customer may choose to pay for the User Environment either as a one-time payment or through monthly invoicing.

Monthly charges commence, or the one-time fee is invoiced, when:

- a) the ordered User Environment has been established;
- b) users have received access instructions by email; and
- c) the dataset has been transferred to the ordered User Environment.

Current pricing information is available on the ICT Services website. Prices are stated in euros and invoices are issued in euros.

The Customer may terminate the order before the agreed end date specified in the order confirmation. Any fees already charged for the minimum billing period (the current month, where monthly billing applies) or the remaining portion of a one-time payment are non-refundable.

ICT Services reviews pricing periodically and reserves the right to change prices. Price changes automatically take effect for existing subscriptions at the start of the next billing period following the current billing period.

ICT Services may suspend user access rights if the Customer fails to pay invoices related to the Service.

3. Responsibilities

Tilausten tekijät ovat vastuussa VISUn lomakkeille syötettyjen tietojen oikeellisuudesta. Lomakkeiden lähettämisen ja tilauksen hyväksymisen jälkeen Oulun yliopiston ja asiakkaan välille syntyy asiakkuussuhde. Asiakkaan pyytäessä sovellusta, joka tarvitsee erillisen lisenssin, asiakas vastaa sovelluksen lisensointiin liittyvien ehtojen selvittämisestä ja noudattamisesta yhteistyössä VISU -ylläpitäjien kanssa. Asiakas vastaa myös kaikista sovelluksen lisensseistä ja lisensoinnista aiheutuvista kustannuksista.

Asiakas on vastuussa olemaan tietoinen VISUn hinnoittelusta ja kuinka hinnoittelu suoritetaan ennen tilauksen tekemistä.

Asiakkaan vastuulla on varmistaa käyttäjäympäristössä käsiteltävän aineiston oikeellisuus sekä tilattavan käyttäjäympäristön soveltuvuus käsiteltävään aineistoon ja mahdolliseen tietolupaan nähden. Asiakkaan on ilmoitettava tilauksessa, käsitelläänkö ympäristössä toisilain alaista aineistoa sekä toimittamaan mahdollinen tietolupa tilauksen yhteydessä.

Toisilain alaisen käyttäjäympäristön tilauksessa on huomioitavaa, että vain tietoluvassa mainitulla luvansaajan yhteyshenkilöllä tai tähän rinnastettavissa olevalla luonnollisella henkilöllä, joka on luvansaaja, on oikeus tilata hankekohtainen käyttäjäympäristö, koska kyseinen yhteyshenkilö on ainoa taho, jonka sidonnaisuussuhde luvansaajaan on tietoluvassa määritelty. Tilauslomakkeelle lisätään käyttäjiksi vain henkilöt, jotka ilmenevät myös tietoluvassa.

Kun käyttäjäympäristö on pystytetty ja mahdollinen lähdeaineisto siirretty ylläpidon toimesta, tilaajalle myönnetään pääsy ympäristöön ja hän käy tarkistamassa, että siirretty aineisto vastaa tietolupaa sekä asennetut ohjelmat ovat tilauksen mukaiset ja toimivat.

VISUn ylläpidolla on velvollisuus tarkistaa lomakkeilla annetut tiedot mahdollisuuksien mukaan mm. tietolupa ja sen tietojen vertailu tilauksessa annettuihin tietoihin.

4. Data transfer into the Service

Users may not independently transfer datasets governed by the Secondary Use Act into or out of the User Environment. Instead, the Customer must submit a service request to the administrators through the service management system.

An authorized external party delivers datasets requested by the Customer to the administrators, who transfer them through a quarantine environment to the User Environment specified in the data permit. This procedure ensures compliance with security requirements and permit conditions.

Within the quarantine environment, an administrator initiates automatic extraction of data packages, malware scanning, and integrity verification. If a dataset is found to be corrupted, the administrator shall inform the Customer and destroy the defective dataset. Verified data is transferred to the User Environment.

The Customer must verify without delay that transferred data is correct. Any suspected discrepancies or errors must be reported immediately to the administrators.

The administration reserves the right to refuse a data transfer if it determines that there is no lawful basis for transferring the data into the User Environment.

5. Access Rights and User Authentication

The Customer is responsible for ensuring that the users named in the order form are authorized to access and process the project data.

Users are granted standard user-level access rights to the Service. Users are identified and authenticated using strong multi-factor authentication (MFA). Users access their User Environments in accordance with the procedures described in the service instructions. No separate usernames or passwords are issued specifically for logging into the Service.

Access rights within the Service follow the principle of least privilege. Administrative rights to systems included in the Service, confidential information processed by ICT Services personnel or users, and all other information requiring restricted visibility or access are protected through access control definitions and system processing policies based on the principle of least privilege.

VISU system administrators are responsible for maintaining the secure processing environment and are the only individuals with access to administrative and maintenance functions. System administrators are not permitted access to data stored within User Environments. Access to the User Environments themselves is permitted only through privileged accounts and solely when there is an exceptionally compelling and justified operational need.

6. Use of the Service

Users shall use the Service in accordance with these Terms of Use and the applicable service instructions.

The User Environment may be used beginning from the start of the first billing period associated with the relevant order.

Access to the Service is provided through a remote connection in which only display output, keyboard input, and mouse input are transmitted between the user's device and the Service.

Users have access to service instructions provided by ICT Services.

Neither the Customer nor the users may resell, redistribute, or otherwise provide the Service to any third party.

7. User Account Suspension

A user's access rights and access to the User Environment shall be locked when the User Environment subscription period ends or, at the latest, when the associated data permit expires.

User access may be temporarily locked if multiple consecutive login attempts fail. Users first authenticate through MFA on the initial login screen and must subsequently log in separately to their User Environment.

ICT Services may suspend a user's access to the User Environment if the user violates these Terms of Use, causes service disruptions, or is deemed to present a threat to the Service. In such cases, the removal of the user's accounts may also be considered. The user and the Customer will be informed of such actions.

8. Exporting results Derived from Data Outside the User Environment

Environment Subject to the Secondary Use Act

The Customer is responsible for anonymising result datasets exported from the User Environment and for carrying out a risk assessment in accordance with Findata's prevailing guidelines. The export of result datasets is performed by VISU system administrators. If Findata's guidance or the outcome of the risk assessment requires verification of anonymity, the result dataset shall be submitted to Findata for review prior to its export. In other cases, the result dataset may be exported from the User Environment after the risk assessment has been completed and the required notification has been submitted to Findata.

Sensitive Data Environment

Within the Sensitive Data Environment, users may independently transfer data both into and out of the User Environment using the SFTPGO service over a secure SFTP connection.

9. Closure of the User Environment and Termination of the Agreement

When a User Environment is closed, the service agreement between the University of Oulu and the Customer also terminates.

The User Environment shall be closed upon reaching the end date specified in the order confirmation. Where a data permit is associated with the User Environment, the environment shall be closed no later than the expiration date of the data permit.

Closure of the User Environment and termination of the service subscription may be requested before the end of the agreed usage period by the Customer's designated contact person. Such requests must be submitted through the service management system using the change request form.

ICT Services shall retain a closed User Environment, including its data, for a maximum of six (6) months following the expiration of the applicable data permit. After that period, the environment and its contents shall be permanently deleted in accordance with Findata regulations unless otherwise required by law or the data permit.

If a user requests access to data during the six-month retention period, a new environment order must be submitted. ICT Services will verify that the user holds a valid authorization or data permit for processing the data.

ICT Services reserves the right to close a User Environment in cases of violations of these Terms of Use or other forms of misuse.

10. Data protection

ICT Services collects and stores personal data as well as statutory technical and usage log information as described in the Privacy Notice.

Access to the Service is strictly personal. Users must not intentionally or unintentionally disclose authentication credentials to another person, nor leave an endpoint device unlocked while logged into the Service. Users are responsible for securely using and safeguarding all authentication methods required for access.

When processing data, users must ensure that confidential information is not disclosed to unauthorized parties. Even where data has been pseudonymized, it remains confidential both during and after use of the User Environment.

In particular, users are prohibited from attempting to circumvent the security controls of the Service in order to obtain non-aggregated data on their own devices or on any storage medium located outside the User Environment.

11. System Integrity and Security

ICT Services shall not be liable for damages resulting from technical failures, software defects, or improper use of resources.

ICT Services reserves the right to modify the content, functionality, and availability of the Service as necessary for development purposes or for other justified reasons, at its discretion and without restriction.

If a user identifies a security vulnerability, the user must immediately report it to ICT Services or the administrators. Information concerning security vulnerabilities must not be disclosed to third parties. Any security weaknesses discovered during use of the Service must be reported to ICT Services.

At all times, users shall comply with good scientific practice, the rules and guidelines of the University of Oulu, and applicable Finnish law.

12. General Obligations

ICT Services is responsible for ensuring that the Service conforms to the Agreement and that all responsibilities assigned to ICT Services are performed diligently and with the professional competence required for the tasks involved.

ICT Services shall promptly inform the Customer of any circumstance that may prevent the Service from being used in accordance with the Agreement.

The Customer ordering the User Environment is responsible for ensuring that all tasks under its responsibility are carried out diligently and in accordance with the Agreement.

The Customer is responsible for acquiring, maintaining, licensing, financing, and ensuring compliance of all required devices, network connections, and software other than the standard software provided with the Service.

Administration reserves the right to reject software requested by the Customer if it is considered harmful to information security or otherwise unsuitable for the environment.

13. Procedure in Cases of Detected Misuse

Upon detecting misuse or having strong grounds to suspect misuse, ICT Services or the administrators shall take immediate action to prevent damage or further damage.

Actions to minimize damage may include:

- a) restricting or revoking access rights;
- b) temporarily closing User Environments; or
- c) initiating an appropriate investigation process involving ICT Services and, where necessary, relevant authorities.

14. Subcontracting of Service provision

To provide the Service, ICT Services procures data center services from Oulun DataCenter Oy as a subcontracted service provider.

15. Scheduled maintenance Windows and other Service Interruptions

Software related to data center technologies and information security is updated as required during scheduled maintenance operations.

If a maintenance outage is necessary, ICT Services or the administrators shall notify customers in advance through public service announcements issued by ICT Services.

ICT Services does not guarantee uninterrupted or error-free operation of the Service. The Service is regularly monitored and maintained to prevent disruptions.

The service provider reserves the right to suspend the Service due to modifications, upgrades, maintenance activities, installation work, similar operational requirements, or where required by legislation or regulatory authority.

Users will be informed of service interruptions as early as reasonably possible.

16. Amendments to the Terms

ICT Services reserves the right to amend these Terms for justified reasons.

Changes shall be announced on the ICT Services website and separately communicated to Service users where appropriate.

Notifications may be omitted where the changes are minor or purely technical in nature.

17. Force Majeure

ICT Services shall not be liable for delays or damages caused by circumstances beyond its reasonable control that could not reasonably have been foreseen or whose consequences could not reasonably have been avoided or overcome.

Unless otherwise demonstrated, force majeure events include, for example:

- war or civil unrest;
- earthquakes, floods, or similar natural disasters;
- interruptions of public transportation;
- interruptions of public telecommunications services;
- interruptions of public electricity supply;
- import or export restrictions;
- strikes, lockouts, boycotts, and comparable industrial actions.

A strike, lockout, boycott, or similar labor dispute affecting ICT Services itself shall also constitute force majeure unless proven otherwise.

Force majeure further includes governmental decisions, orders, or legislative changes that prevent ICT Services from fulfilling its contractual obligations, as well as large-scale internet infrastructure disruptions, global cybersecurity incidents, or other comparable events beyond the control of ICT Services.

A force majeure event affecting a subcontractor of ICT Services shall likewise be considered a force majeure event for ICT Services. However, a mere lack of subcontractor resources or financial difficulties shall not constitute force majeure unless caused by one of the events described above.

A Party shall notify the other Party without undue delay upon becoming aware of a force majeure event and its effects. Once the force majeure event ceases, contractual obligations shall resume without unnecessary delay, and each Party shall make reasonable efforts to mitigate the effects of the event.

18. Governing Law and Dispute resolution

This Agreement shall be governed by and construed in accordance with the laws of Finland, excluding its conflict-of-law provisions.

Any disputes arising from this Agreement shall primarily be resolved through negotiations between the Parties.

Disputes that cannot be resolved through negotiation shall be settled by the District Court of Oulu.

If separately agreed by the Parties, a dispute may instead be referred to arbitration. Arbitration shall be conducted in accordance with the Arbitration Rules of the Finland Chamber of Commerce. The seat of arbitration shall be Oulu, Finland, and the proceedings shall be conducted in Finnish unless otherwise agreed by the Parties.

