

**DATA PROTECTION POLICY**

Based on the EU General Data Protection Regulation

Created/amended: 19.12.2025/

Controller of the register

University of Lapland
Yliopistonkatu 8
96300 Rovaniemi

1. Representative of the controller

Director Merija Timonen
Teaching and Learning Services
firstname.lastname@ulapland.fi

2. Contact persons in matters related to the register

Maija Törmänen, University Counsellor (administrator)
firstname.lastname@ulapland.fi

The system users engaged in client work (university counsellor and study psychologist) are in charge of processing the data of their own clients. Within the framework of substitute arrangements, university counselors are granted access to client information of other counselors. University counselors do not have access to the student psychologist's client information, nor do the student psychologist have access to the client information held by the counselors.

3. Contact information of the data protection officer

Jari Rantala, Data Protection Officer
Legal Services
+358 40 547 2583
firstname.lastname@ulapland.fi

4. Purpose of personal data processing

The personal client data stored in AJAS – University Counsellors' and study psychologist's Client Information System of the University of Lapland are processed to maintain the university counsellors' and study psychologist's client relationships.

As social welfare specialists, the counsellors are obligated to abide by the following Acts in their work:



DATA PROTECTION POLICY

Based on the EU General Data Protection Regulation

Created/amended: 19.12.2025/

- Act on the Status and Rights of Social Welfare Clients (812/2000)
- Act on social welfare client documentation (254/2015, no existing English translation)

According to these Acts, it is in the interest of the client to maintain a client register and to record client encounters. In addition, the contact request data and anonymous statistics stored in the register are utilised to develop and to control the quality of university counselling work.

In accordance with legislation regulating the operation of the controller, the university does not function as a social welfare service unit. The activities of the university are governed by the obligations arising from the Universities Act (558/2009) and other applicable legislation.

As health care specialists, psychologists are obligated to abide by the following Acts in their work focusing on the individual:

- Act on Health Care Professionals (559/1994)
- Act on the Status and Rights of Patients (785/1992)
- Decree on patient documents (24/2022)

In accordance with legislation regulating the operation of the controller, the university does not function as a health care service unit and does not consider study psychologist's work to be health care work. Therefore, documents created in individual counselling are not regarded as patient documentation. The operation of the university is guided by obligations provided in the Universities Act (558/2009) and other related legislation. The study psychologist's job description requires the processing of sensitive information. The basis for processing information produced in study psychologist's counselling is the performance of a task carried out in the public interest (GDPR Art. 6, 1e and section 45b of the Universities Act).

The basis for processing personal data is prescribed by law. In addition, the contact request data and anonymous statistics stored in the register are utilised to develop and to control the quality of study psychologists' work.

5. Legal basis for processing personal data

The processing is based on the EU General Data Protection Regulation, Article 6, 1 a-f. At least one item must apply.

The specific grounds for processing are as follows:

- the data subject's consent
- performance of a contract (to which the data subject is party)
contract:
- fulfilling a legal obligation to which the controller is subject



DATA PROTECTION POLICY

Based on the EU General Data Protection Regulation

Created/amended: 19.12.2025/

enactments:

- interests of the data subject or of another natural person
- a task carried out in the public interest or the exercise of official authority vested in the controller
 - official duty in the public interest
 - scientific or historical research or compilation of statistics
 - archiving of research materials and cultural heritage materials
- realising the legitimate interests of the controller or of a third party
 - the legitimate interest in question:

The EU General Data Protection Regulation, Article 9 (special categories of personal data)

- the data subject's consent
- carrying out the obligations of the controller or of the data subject in the field of labour law, social security, or social protection
- protecting the vital interests of the data subject or of another natural person
- legitimate activities by a foundation or association with a political, philosophical, religious or trade union aim
- the personal data have been made public by the data subject
- establishment, exercise, or defence of a legal claim
- substantial public interest
- occupational health care purposes
- public interest in the area of public health
- archiving purposes in the public interest, scientific or historical research or collection of statistics

6. Processed personal data groups and the data storage period

The register contains the following information:

- the employee's name
- the client's personal data
 - names, social security number
 - contact information
- study right information
 - name of the educational institution and degree programme/major subject
 - information on special study arrangements that potentially apply
- parties of collaboration (according to the student's report, the following: mental health services, student health care, third-sector actors, etc.)



DATA PROTECTION POLICY

Based on the EU General Data Protection Regulation
Created/amended: 19.12.2025/

- previous
- current
- client report
 - party that made contact
 - reason for becoming a client
 - meetings, discussions, consultations, and persons present
 - plans and recommended measures
 - summaries, statements, referrals, and examination results
 - assessment
- document exchange
 - document forwarding: the employee who made the entry, date, the client's consent, document name, target, grounds for the forwarding (context, the client's request, statutory)
 - received documents: date of arrival and source

In the storage and erasure of the data, the data management plan of the University of Lapland and the regulations and directions of the National Archives of Finland applicable at each time shall be observed.

Information generated in the individual guidance sessions provided by the university counsellor and the study psychologist are stored for four years, after which they are erased from the register.

7. Data systems used in processing

AJAS – University Counsellors' and Study Psychologist's Client Information System

8. What is the source of the personal data needed in processing? Is the data subject obligated to deliver the needed personal data? Consequences if the data subject does not deliver the needed personal data.

Data entered into the register are received from

- The data subjects themselves (students)
- A partner/another operating unit such as the FSHS with the client's consent.

If the data subject submits their personal data for processing, the grounds for submitting the data are as follows:



DATA PROTECTION POLICY

Based on the EU General Data Protection Regulation
Created/amended: 19.12.2025/

- the controller's statutory duty
- an agreement between the controller and the data subject (services cannot be used without an entry agreement)

9. Regular data transfers and forwarding

The personal data in the register are secret.

Personal data in the register are not forwarded on a regular basis. The right to forward secret data is primarily based on the client's consent. Secret data can only be forwarded with the data subject's express consent or if there is a specific provision on forwarding or on the right of access to the data in an Act (chapter 7 of the Act on the Openness of Government Activities, section 18 of the Act on the Status and Rights of Social Welfare Clients).

Statistical data without personal identifiers can be produced from the register for the use of the University of Lapland. No personal data are forwarded to direct marketing.

The right to deviate from secrecy obligations

University counsellor services:

It is possible to deviate from the secrecy obligations concerning social welfare as provided in Chapter 7 of the Act on the Openness of Government Activities, unless otherwise provided in this or another Act (Act on the Status and Rights of Social Welfare Clients, section 18). A person performing tasks referred to in this Act has the right, notwithstanding the secrecy obligation, to provide the police with information necessary for assessing a threat to life or health and for preventing a threatening act if the person, when performing the tasks, has received information on circumstances based on which he/she has reason to suspect that someone is in danger of becoming victim to violence. (Unofficial translation.)

Study psychologist services:

Secret data created in using study psychologist services may be forwarded with the client's consent to an authority with a statutory right of access to the data at the authority's written request which states the Act on which the right of access is based. Access to data may be granted without the client's consent if data forwarding or the right of access to data is specifically provided in an Act.

10. Transferring or forwarding data outside the EU or EEA and grounds for it

No student information is transferred outside the EU or the European Economic Area.

11. Personal data protection principles

The server administrator used by the Data Controller and the Data Processor in accordance with the GDPR is Ajas Oy.



DATA PROTECTION POLICY

Based on the EU General Data Protection Regulation

Created/amended: 19.12.2025

Ajas is certified as a Class A1 patient information system. During the certification process, its information security practices were verified by an external auditing company.

The online service used for processing registry data is protected with passwords, and the server as well as other servers are secured with firewalls, passwords, and other technical safeguards. Passwords are not stored on the server in plain text; instead, they are kept salted and encrypted using a method that is considered secure at any given time. The server is located in a locked and monitored facility in Upcloud Oy's data center in Helsinki. Data retention is ensured through automatic backups.

The personnel of Ajas Oy are bound by confidentiality, and each employee has signed a non-disclosure agreement committing them not to disclose any information related to client data.

The storage, archiving, erasure and other processing of the information possessed by the University of Lapland are guided by a data management plan and data secrecy and data protection instructions. The register has been protected from external parties with firewalls and other technological solutions. The connections between the register and user workstations have been protected. Using the system requires a personal username and password.

Employees can only process the personal data that they need in performing their tasks. The right of access to the system expires when a person's employment relationship ends or the person leaves the tasks for which the right of access has been granted. Employees processing the data are bound by a non-disclosure obligation that continues after the end of the employment relationship.

The system registers faulty logins and all data processing and accessing performed in the system. Data protection and the confidentiality, integrity and usability of personal data in the client register are ensured through appropriate technical and administrative measures.

12. Automated decision making

No automated decisions are made in the processing.

13. IP Data

In the Ajas appointment booking system used by the Data Controller, the IP addresses of visiting users are stored in a designated log. The log is used for potential error investigations and for maintaining information security. Access to the log is restricted to specific, pre-authorized personnel within the Ajas system used for registry management.

14. Rights of the data subjects

According to the EU General Data Protection Regulation, Articles 15–22, the data subjects have the following rights:

- obtaining access to their own data and examining them
- rectifying the data
- erasing the data



DATA PROTECTION POLICY

Based on the EU General Data Protection Regulation

Created/amended: 19.12.2025/

- restricting the processing of the data
- transmitting the data forward
- objecting to the processing of the data

The contact person in issues related to the rights of the data subjects is the data protection officer, whose contact information is at the beginning of this document.

Attending students:

Data subjects have the right to access and examine their own data. They are entitled to request their counsellor or study psychologist to inform them of the entries stored in the system during counselling. The data can also be delivered as a client printout of the register entries.

When the study right has expired:

Clients may order in writing and through physical mail the records, summaries, statements, certificates and recommendations that are stored on them in the register. This is done by emailing an examination request to the Registry of the University of Lapland at kirjaamo@ulapland.fi, from where the request is forwarded to the counsellor or psychologist.

Clients are entitled to claim rectification of erroneous data in the register. Data rectification requests are submitted in a similar manner as examination requests.

Clients are entitled to file a complaint with the Office of the Data Protection Ombudsman if the effective data protection legislation has been violated in the processing of their personal data.

Advice and instructions on the rights of the data subject are given by the data protection officer, whose contact information is in section 3. The web page [Data protection](#) also contains relevant instructions and the forms to be sent to the Data Protection Ombudsman.