Privacy Notice

Approved by the Board of the National Union of Students in Finnish Universities of Applied Sciences SAMOK in August 2024.

This is the privacy notice of the National Union of Students in Finnish Universities of Applied Sciences SAMOK (later referred to as 'union') in accordance with the EU General Data Protection Regulation (2016/679). The notice was created on 15 February 2023.

Data controller

National Union of Students in Finnish Universities of Applied Sciences SAMOK
1056678-8
Lapinrinne 2, FI-00180 Helsinki, FINLAND

Representative(s) of the controller

Veeti Mieskonen, Administration and Events Coordinator
veeti.mieskonen@samok.fi
Lapinrinne 2, FI-00180 Helsinki, FINLAND

Vellu Taskila, Executive Director
vellu.taskila@samok.fi
Lapinrinne 2, FI-00180 Helsinki, FINLAND

Name of personal data register

- Stakeholder register
- Alumni register
- Event attendee register(s)
- Supporting member register
- Member register

Data sources, purposes and legal basis of processing the personal data of data subjects

The main purpose of processing is to carry out the union's activities, monitor the interests of the union's members, maintain stakeholder relations and promote events organised by the union. The

union meets the obligation specified in section 11 of the Finnish Associations Act (1989/503) to maintain a register of its members and their personal data.

Under section 11 of the Associations Act, the board of trustees of a registered association is responsible performing the duties of the data controller. The Board of the union has appointed the union's Administration and Event Coordinator and Executive Director to act as representatives of the controller and exercise the rights of data subjects in cases where the data subject is a natural person. The controller's representatives do not have any specified responsibilities related to the management of the personal data register.

The primary sources of personal data are forms provided by the union, including event registration forms and the form for becoming a supporting member. To ensure that data is up-to-date, data in the registers can also be updated from other publicly available registers, including telephone number services operating in Finland or publicly available contact information on the websites of associations or businesses, for example.

The primary legal basis for the processing of personal data is the data subject's consent in accordance with Articles 6.1(a) and 9.2(a) of the GDPR, the connection formed with the union under Article 9.2(d) by the data subject becoming a member of the union and, in the case of data that falls under a special category of personal data, on the basis of Article 9.2(e) when the data is manifestly made public by the data subject. The processing of personal data by the union in the appropriate registers is based on the legal obligation of the data controller to maintain a member register in accordance with section 11 of the Associations Act (1989/503) and Article 6.1(c) of the GDPR.

Content of the registers

The following categories of personal data can be stored in registers maintained by the union.

- First and last name
- Date of birth or age
- Contact information such as email, phone number or home address

For the purposes of developing event and member services, executing event payments or for statistical purposes, the following personal data may also be processed:

- Banking information, such as e-invoice address
- Self-identified gender
- Membership of the union's member association
- Languages spoken
- Dietary information
- Position in the organisation

Data automation and data subject profiling

Position-based profiling is used in event marketing to ensure that event invitations are sent out to the appropriate recipients (for example, the invitation to the Staff Days event is sent out only to members of staff of student unions).

Other processors of personal data

Personal data may be processed in the following systems:

- Google Drive
- Slack
- Monday.com
- Trello
- Mailchimp

The primary processors of personal data in the registers are those members and elected officials of the union whose duties require access to the data. Processors are bound by a non-disclosure obligation.

Personal data is regularly disclosed to service providers used by the union in connection with events, such as catering and accommodation service providers. Personal data is anonymised to the extent possible.

Personal data is also disclosed to Oy OSS-Järjestöpalvelut Ab, which provides invoicing services for the union's events. Disclosure is based on the consent of the data subject.

Retention period of personal data

In the event that the data subject does not require the erasure of their personal data from the register in the manner described below, the controller will erase the data subject's personal data when its processing is no longer necessary, taking into account the purpose of the processing, but no later than two full calendar years after all of the data subject's memberships have been ended or terminated.

Transfers of data outside the EU or EEA

Personal data is stored in a cloud service whose server may be physically located outside the EU and/or EEA. Personal data will not be transferred outside the European Economic Area for processing if the data

protection level of the destination country has not been considered adequate by the European Commission.

Rights of data subjects

In accordance with Articles 13.2(b), 13.2(c), 13.2(d) and 13.2(e) of the GDPR, data subjects have the following rights:

- Right of access to your personal data
- Right to rectification
- Right to erasure of data
- Right to restriction of processing
- Right to object
- Right to data portability
- Right to lodge a complaint with the supervisory authority

If you wish to exercise your right of access, rectification, erasure, restriction of processing or transfer of your data from one controller to another, you may contact the controller by email or visit the controller's office in person. If you wish to withdraw your consent to the processing of your data in accordance with Articles 13.2(d) and 14.2(e) of the GDPR, you can do so by contacting the controller by email or mail.

If you wish to make changes to your personal data processed by the controller, you must make the request using the electronic form that includes proof of identify of the person making the request. You can verify your identity with your electronic signature, for example. If you make the request in person at the controller's office, please be prepared to verify your identify with a photo ID.

Upon request, the data subject must specify the time period for which the data is accessed, erased or rectified, and the format in which the data should be provided.

The controller is obligated under Article 12.3 of the GDPR to provide data subjects with information on the measures taken on a request made pursuant to Articles 15 to 22 without undue delay and within one month of receiving the request at the latest. This period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

If the data subject considers that the processing of personal data relating to him or her infringes the GDPR, the data subject shall have the right to lodge a complaint with a supervisory authority in the

member state of his or her habitual residence, place of work or place of the alleged infringement. The supervisory authority in Finland is the Office of the Data Protection Ombudsman.

Security of personal data processing

The security of the processing of personal data is ensured in the following ways:

- The data is located on a device in the controller's possession, the contents of which are encrypted, or on a virtual server on a computer with adequate physical safeguards.
- The confidentiality of data is safeguarded by encrypted communications.
- The processors of data are bound by a non-disclosure obligation.
- The ability to recover data quickly in the event of a failure is ensured with regular backups. The availability of the services is otherwise ensured with regular software updates.
- The union strives to assess the effectiveness of technical and organisational safeguards of personal data processing on a regular basis.
- When procuring systems, applications and services used in processing activities, data security is taken into consideration already during the procurement process.
- Modifications to the registers and access to data in the registers is prevented by technical means from persons other than those specified above as having the right to access the data. Persons with the right to access and process data are identified by appropriate access control measures.