PRIVACY POLICY OF Aalto-yliopiston kauppatieteiden ylioppilaat ry
Updated 5.11.2026
Approved at the KY Board meeting 28/2026

Aalto-yliopiston kauppatieteiden ylioppilaat ry is committed to complying with and processing personal data in accordance with applicable data protection legislation.

Data protection legislation refers to the applicable data protection laws, such as the General Data Protection Regulation of the European Union (2016/679) and the Data Protection Act (5.12.2018/1050). Terms related to data protection not defined in this privacy policy are interpreted in accordance with data protection legislation.

Data Controller
Aalto-yliopiston kauppatieteiden ylioppilaat ry (2214976-2)
Konemiehentie 4, 02150 Espoo
040 353 8283

(Hereinafter "**Data Controller**")

Contact Person
Aada Hakakoski, Executive Director
aada.hakakoski@ky.fi
050 043 0546

Personal Data Registers Maintained by the Data Controller

- Membership Register
- Activity Points and Granted Acknowledgements Register
- Access Control Register
- Supporting Members Register
- Association Register
- Office Personnel Registers
- Volunteer Registers, including Committees, Tutors and Representative Council Members
- Facility Booking Registers
- Event Participants Registers
- Event Photo Registers
- Surveillance Camera Register for the Association's Event Spaces and Office

- Code of Conduct Violations Register
- Payment Information Registers
- Related Parties Register

Purpose and Legal Basis for Processing Personal Data

The Data Controller processes personal data on several legal grounds. The primary purpose of processing personal data is the maintenance of membership registers, event organization, management of recruitment and employment-related information, protection of the Data Controller's legitimate interests, upholding of the Code of Conduct in order to protect the Data Controller and its members, and fulfillment of contractual and statutory obligations.

The primary legal bases for processing personal data are the consent of the data subject, a contractual relationship, or the legitimate interest of the Data Controller.

Processed Personal Data

Information stored in the registers may include, for example:

- Name
- Address
- Personal identity number
- Student number
- University enrollment and right to study
- Membership number of Suomen Ekonomit
- Nationality
- Phone number
- Email address
- Company name
- Association name and operational information
- Photos
- Videos
- Social media identifiers
- Special dietary and accessibility requirements for event organization
- Competence and qualification data collected for recruitment purposes
- Taxation and payment information

- Information of related parties of the association, including the persons and legal entities close to the association
- A concise description of the misconducts, measures taken, sanctions and their durations related to Code of Conduct enforcement
- The surveillance camera register records data on individuals present in the event spaces and the office of the Data Controller, along with the recording time. Audio is not recorded in the surveillance camera register.

The use of surveillance cameras is based on the legitimate interest of the Data Controller or a third party:

- Ensuring the safety of events, office spaces, and individuals present
- Protecting the property of the Data Controller or a third party

Personal data collected from witnesses of Code of Conduct violations and through surveillance cameras is processed for the following purposes:

- Upholding the Code of Conduct
- Ensuring event safety
- Preventing and investigating possible criminal, misuse, damage, or accident situations
- Protecting property and preventing and investigating property-related crimes and other misconduct

Some of the surveillance cameras on KY's premises are managed by the Data Controller (Aalto-yliopiston kauppatieteiden ylioppilaat ry), and some are managed by Aalto-yliopiston kauppatieteiden ylioppilaiden säätiö sr. The footage collected by each camera is processed separately by its respective controller in accordance with their own privacy policy. The privacy policy of Aalto-yliopiston kauppatieteiden ylioppilaiden säätiö sr is available here.

We use Void Analytics to collect anonymous statistical data about the usage of our websites. Void Analytics does not use cookies and does not store personally identifiable information such as IP addresses. No user profiles are created, and individual visitors cannot be identified. The data collected through Void Analytics includes, for example:

- The pages visited
- The browser and device type
- Referring websites
- Approximate location based on timezone and browser language settings

- Time of visit and duration

This data is used solely for the purpose of improving the website's performance, content, and user experience. The data is processed within the European Economic Area (EEA) and is not shared with third parties. However, we may share aggregated and anonymous page view statistics with selected partner organizations regarding their own pages hosted on our website. For example, if a partner organization has a dedicated promotional page on our site, we may inform them of how many visits that specific page has received in a given month.

Regular Data Sources

Personal data is primarily collected directly from the data subjects, for example, during membership registration and event sign-ups. Data is also collected during recruitment processes for volunteer and employee positions. Members of the Data Controller may submit nominations and justifications for the Badge of Dedication.

Personal data regarding Code of Conduct violations can be collected from people who have witnessed misconduct.

The Data Controller collects personal data for the Activity Points from the associations' board chairperson and other contact persons.

The Data Controller uses surveillance cameras in its office and event spaces. The Data Controller may photograph events it organizes.

Contact information of representatives of companies and other organizations can also be collected from public sources such as websites, directory services, and other organizations.

Data Processors and Disclosure of Personal Data to Third Parties

Personal data is primarily processed by the Data Controller's board and employees. Additionally, personal data may be processed by committee members and other responsible persons directly connected to the Data Controller in the contexts of event organization and coordination of tutoring activities.

The Data Controller processes surveillance camera data itself, and only a designated responsible person handles such data. Personal data may be disclosed to competent authorities as required by their requests or for investigating criminal, misuse, damage, or

accident situations in accordance with current legislation. Data may also be disclosed to insurance companies for damage claim processing.

External data systems may also be used for processing personal data. In such cases, the Data Controller ensures that the data is handled confidentially and in compliance with applicable data protection legislation.

- KY's membership register is provided by Vitec Avoine (1935337-5). Vitec Avoine processes the personal data provided during registration in accordance with its own privacy policy, which can be found here.
- The association's members are entitled to member services provided by Suomen Ekonomit (0202108-3). Data relevant to providing and verifying rights to said services is provided to Suomen Ekonomit from KY's membership register. Suomen Ekonomit processes the personal data provided during registration in accordance with its own privacy policy, which can be found here.
- Images from the Data Controller's events may be published on the gallery platform kuvat.fi provided by Mediadrive Oy (0638594-1) and the images are processed in accordance with its own privacy policy, available here.
- Information of the association's Related Parties is disclosed annually to the auditor of the association.
- Event registrations are primarily handled through the Kide.app service. Kide.app processes the personal data provided during registration in accordance with Treanglo Oy's (2623329-1) privacy policy, available here. Some events use Google Forms for registration.
- Google Workspace services are used to process and store certain personal data. This can, for example, include event registrations or internal communication involving identifiable individuals. Google's privacy policy is available here.
- Facility bookings are primarily handled through the Skedda service. Skedda processes the personal data provided during registration in accordance with their own privacy policy, available here.
- Cloudflare is used to process booking calendar data on behalf of the Data Controller to remove names, contact details and free-text booking information before transferring

the resulting calendar data to Aalto University Student Union (AYY). AYY uses this data to display the availability of KY's facilities in its booking calendar. The transferred data includes facility names, booking times, status and technical calendar information, with booking identifiers replaced by pseudonymous identifiers. Cloudflare also retains technical request logs for operational and security purposes. Processing may take place outside the EEA subject to the safeguards described in this policy. Cloudflare's Data Processing Addendum is available here.

- Mailchimp (Intuit Inc.) is used to manage and send weekly Monday Mail newsletter. Mailchimp processes the data in accordance with its own privacy policy, available here.

- Payment processors
  The Data Controller offers MobilePay (Vipps MobilePay AS) and card payments via Zettle by PayPal (PayPal (Europe) S.à.r.l. et Cie, S.C.A.) as payment methods for merchandise sales. Personal data such as the customers' name, phone number, last digits of the card number and transaction details can be collected during the payment transaction. The service providers process the personal data in accordance with their own privacy policy, which can be found for MobilePay here and for Zettle here.

- Tutoring for new students is organized in cooperation with Aalto University (2228357-4). The Data Controller selects the tutors and maintains the Volunteer Register. For the practical coordination of tutoring and for assigning new students into tutoring groups, the Data Controller discloses to Aalto University the necessary personal data of tutors (e.g., name, email address and phone number). Aalto University uses the data only for coordinating tutoring activities and group assignments. The legal basis for the disclosure is the legitimate interest of the Data Controller and Aalto University in organizing and implementing tutoring activities.

Data is not regularly disclosed to other parties than mentioned above. Data may be published to the extent agreed with the data subject.

The Data Controller may also disclose personal data to competent authorities when required by law or when involved in legal proceedings or similar processes. In the event of an association merger or similar arrangement, personal data may also be disclosed.

The Data Controller complies with applicable data protection legislation when disclosing personal data.

Transfer of Personal Data Outside the EEA

Personal data is primarily processed within the European Economic Area ("EEA"). If personal data is processed outside the EEA and the European Commission has not issued an adequacy decision on the level of data protection, the transfer is carried out in accordance with the European Commission's standard contractual clauses (2021/3974/EU, as amended).

Subcontractors or servers used by the Data Controller may be located outside the EEA. In such cases, the Data Controller ensures the lawfulness of data transfers and adequate safeguards, for example, by using the European Commission's standard contractual clauses.

For example, services such as Cloudflare, Google Workspace, Mailchimp and Zettle by PayPal may involve the transfer of personal data outside the EEA. These transfers are subject to the European Commission's standard contractual clauses.

Data Protection and Retention

Care is taken when processing the register, and data processed through information systems is appropriately protected. Register data is stored on internet servers, and the physical and digital security of their hardware is appropriately maintained. The Data Controller ensures that stored data, server access rights, and other critical personal data security information are handled confidentially and only by those whose job descriptions include it.

The Data Controller retains personal data only for as long and to the extent necessary for the purposes defined in this privacy policy or as required by contracts or legislation. Retention periods vary depending on the purpose of use and situation; additional information on retention periods is available upon request. The Data Controller also strives to update registered data proactively from time to time.

General Rights of the Data Subject

The Data Controller adheres to the rights guaranteed to the data subject by data protection legislation. The applicability of these rights depends on the specific circumstances and purpose of personal data processing.

The data subject has:

- **The right to access data**
  The data subject has the right to obtain confirmation as to whether personal data are processed by the controller and to have access to the data. The data subject has the right to obtain a copy of the personal data and to receive information on the processing of personal data as defined in the data protection legislation.

- **The right to withdraw consent**
  Where the processing of personal data is based on the data subject's consent, the data subject has the right to withdraw consent.

- **The right to rectify data**
  The data subject has the right to obtain the rectification of inaccurate or incorrect personal data and the completion of incomplete personal data.

- **The right to erasure of data and to be forgotten**
  The data subject has the right to have personal data erased in accordance with data protection legislation. The Data Controller may refuse this request if it has a legitimate reason to retain the data.

- **The right to restrict data processing**
  The data subject has the right to request restriction of the processing of personal data under the conditions laid down in data protection legislation.

- **The right to data portability**
  The data subject has the right to have personal data transferred to another controller, where technically feasible, in accordance with the conditions laid down in data protection legislation. This right applies where personal data are processed automatically, where personal data are processed on the basis of consent or contract, where the data concern the data subject and are provided by the data subject, and where the transfer does not adversely affect the rights of third parties.

- **The right to object to data processing and avoid automated decision-making**
  The data subject has the right to object to the processing of personal data on the basis of legitimate interests, subject to the conditions laid down in data protection legislation. However, the controller has the right to refuse a request where the processing is necessary for the purposes of the legitimate interests pursued by the

controller or by third parties. The data subject has the right not to be subject to a decision based solely on automated processing, such as profiling. However, the controller has the right to refuse the request in accordance with the applicable exceptions in data protection legislation. The data subject always has the right to object to the processing of personal data for direct marketing purposes.

Exercising Rights

The data subject can make requests regarding their rights via email to the data protection officer's email address listed above. Requests must include the data subject's name, address, and phone number. The Data Controller verifies the data subject's identity with a copy of an identity document (such as a passport or driver's license). The Data Controller responds within a reasonable time.

Any viewing of the camera recording takes place on the premises of the Data Controller. A data subject recorded on camera has the right to request deletion of the footage concerning them. The Data Controller may refuse this request if it has a legitimate reason to retain the footage (e.g., pending investigation or legal obligation).

The data subject can always contact the competent data protection authority if they believe their data is being processed in violation of data protection legislation.

Updating the Privacy Policy

The Data Controller updates this privacy policy as needed, for example, when legislation changes. Data subjects are informed directly of changes affecting the Data Controller's privacy practices, and it is advisable to review this privacy policy periodically.