Aalto University
IT Services

Privacy notice for Aalto University IT services

Effective as of 25 May 2018
Updated 20 December 2019

1. **Introduction**
2. **Why and on what basis does Aalto University process your personal data?**
3. **What personal data does Aalto University collect and process?**
4. **How do we collect personal data?**
5. **To whom do we disclose personal data?**
6. **Transfer of personal data to third countries**
7. **Period for which personal data is stored**
8. **Rights of the data subject concerning personal data**
9. **Exercise of rights**
10. **Right to receive notice of a security breach of your personal data**
11. **Controller, person in charge and contact details**
12. **Your responsibility**
13. **Personal data and principles of privacy protection**
14. **Amendments to the privacy notice**

1. Introduction

Protecting your privacy and processing your personal data responsibly is a high priority for us at Aalto University.

This privacy notice describes the Aalto University policy on the personal data collected and processed by the Aalto University IT Services (ITS) in connection with the services it produces and the processes it executes.

2. Why and on what basis does Aalto University process your personal data?

Aalto ITS processes personal data on the basis of its role as a provider of information technology services in all systems produced and administered by Aalto ITS. Some of the services are produced by contracted partners and subcontractors. Aalto ITS holds responsibility for any such services in the same way as it does for the services it produces itself.

In order to provide services, we process personal data in customer relationship management, customer and user identification, order processing and service delivery, service and product quality control, customer service, repairing malfunctions and disruptions, and processing complaints. We process personal data also when communicating with customers, such as when sending notifications on our services and contacting our clients in matters related to our services.

We process personal data:

- when managing centralised identity information, such as usernames and access rights and in the management of information system resources such as networks, applications, services and network drives.
- to monitor the use of systems and prepare statistics on the use, as well as to perform various tasks related to electronic approvals or workflows.
- in connection with the management system of workstations, which is used to keep the workstations usable and their information secure. Usually, a workstation means a personal computer, which may be a desktop or laptop computer or other IT device (e.g. smartphone).
- in the electronic working environment (O365), which is designed to provide electronic communication services to the Aalto University staff and students, as well as to any subcontractors and performers of commissioned work who have been created an Aalto University IT account.
- in connection with printing, printing management and user-based invoicing on the basis of the cost-pool code of the user.
- in order to develop and manage our services and the related processes and associated quality control, for instance: analysing the supply processes and related complaints in order to streamline the processes and to find a better and faster way of serving our customers.
- to understand the needs and wishes of our customers regarding the features or contents of our services.
- for information security purposes related to the use of services, e.g. when looking at successful or failed login to services that require registration.
- when taking care of service requests and investigating problems with IT services and information security incidents
- to identify and prevent fraud and misuse of services.

Personal data and transactional data are processed to detect technical errors and faults and in order to ensure the information security of all our services, information systems and communication networks and to test them. We process transactional data to technically develop our communication service, such as to optimise the operations of our communication networks. In addition, we can prepare statistics for the purposes of service development or other analysis.

The Aalto data warehouse, which is a reporting and integration service offered by Aalto to its units, also processes personal data. The data warehouse is also used for reporting to the authorities.

Aalto ITS uses advanced analysing, machine learning and artificial intelligence tools which process personal data, for instance, to improve cyber security and ensure the integrity of data.

The Aalto information system portfolio is very broad-based, and Aalto has a information system map, which is regularly updated. It describes the key features of the information systems in the portfolio, such as purpose, owner, administrator and possible contractor.

To make the Aalto information system portfolio more intelligible, Aalto ITS has divided it into logical entities. The logical entities are made up as follows:

- context in which the information is used
- service provided to the user
- the technical functions/components that are performed in order to provide the service.

Contexts related to operations that are jointly used by Aalto but are the responsibility of Aalto ITS:

- Aalto joint services
- Electronic communication and cooperation

- Electronic communication and cooperation / background systems
- Infrastructure
- Infrastructure / background systems

Other contexts at the Aalto level are:
- human resources
- financial services
- teaching and learning
- campus services
- research and innovation

The services are logical entities offered to the users.

From an information system viewpoint, providing a user with a service involves technical processing of data at three levels:
- in business components that execute the logic needed by the service
- in platform components, where information is processed and stored temporarily
- in network components, which are responsible for data transfer

The following example clarifies the structure:
- the service provided to the user is an email service (agreement on email service)
- the email component is the technical execution of the functions or set of functions required by the email service.
- the email component is run on platform components (servers and database servers)
- Network components take care of the transmission of data between the platform components and terminal devices

As regards Aalto employees, personal data is processed primarily on the basis of the university's legitimate interest, which itself is based on the employment relationship between Aalto and the employee or other operational affiliation with the university (e.g. fee-recipients, academic visitors or other visitors, grant recipients).

As regards Aalto students, the university's right to process personal data as the controller is based on the necessity to perform a task carried out in the public interest or in the exercise of official authority.

As regards users external to Aalto, the right to process personal data is based on either agreement or consent. If a person external to Aalto is granted an Aalto IT account with the help of an HR form, this constitutes an agreement, as is the case when persons activate additional services using the HAKA federation identification.

When persons external to Aalto begin using a mobile application offered by Aalto, the basis of Aalto's right to process their personal data is their consent.

In the electronic working environment the user has a chance to allow the information content he or she produces to be used by others and get information about his or her networks and friends.

3. What personal data does Aalto University collect and process

The personal data processed by the university may be divided into the following categories:

- identification data:
    - name
    - personal identification number
    - date of birth
    - contact details
    - employee number (staff)
    - student number (student)
    - national learner ID (student)
- username and password
- access rights
- device information
- information collected by customer services:
    - name
    - contact details
    - username
    - location on campus
    - information related to the service request
    - employee number (staff)
    - unit (staff)
    - supervisor (staff)
    - student number (student)
    - school (student)
- In the electronic working environment, when there are two or more parties to the communication and/or users of the electronic team working environment, the following personal data are processed:
    - name
    - job title
    - organisational unit
    - username
    - email address
    - telephone number
    - in addition, the user has a chance to give optional information in the service, e.g. photo
- Data collected in connection with the printing service:
    - name
    - email
    - username
    - printer ID
    - time stamp
    - card ID when using secure print
- data collected in connection with the use of IT systems:
    - time stamp
    - username
    - communication

In the electronic working environment, the contents of the message and any attached files (whether they be text, images, sound, video or other electronic communication) are primarily considered confidential data and are thus only processed in exceptional circumstances specified by law.

In accordance with the Aalto University log management policy, all systems record data of at least the following activities and their timestamps (to be considered also in the other log types specified below, as appropriate):

- successful and failed logins at the level of users, groups and applications;
- logouts
- successful and failed changes of passwords
- successful and failed changes of access rights and use of access rights
- changes (creation, modification or deletion) to usernames and user groups and related roles and permissions.
- If single sign-on is used to log in, the logged information must include an identification of the terminal device with which the login, change of password, or other successful or failed activity was performed.
- Usage and error data specific to services and systems
- Scheduled tasks and their access rights

The IP log files store at a minimum the following data:

- Timestamps
- IP and physical addresses
- Internal and public address
- Log-in data (as above) for workstations in common use
- Node

The file logs for the email system stores the following data at a minimum:

- The system from which email arrived
- Sender and recipient data
- The size of the email with attachments
- A unique identifier for each email message
- The timestamps of every processing stage
- The processing state

The following data, at a minimum, are stored in transaction (database) log files:

- Timestamp
- IP address
- Username / system that made changes
- Event type: read with search criteria, write, modify, delete
- File
- System-level database processing
- The extent of the data stored in transaction log systems – apart from systems containing personal, study attainment or financial data – is decided by the data owner, taking into account the data content and the data protection requirements

Data transmission logs store, as applicable, the following data at a minimum:

- Timestamps
- Source and destination addresses and ports
- The protocols used
- The scale of the traffic
- The passive DNS log stores timestamps, domain names and the IP addresses of name servers.

Security logs store, as applicable, the following data at a minimum:

- Timestamp
- Source and destination addresses and ports
- Username
- Event type and event target
- Malware infections and their handling status
- In the logs of firewalls and other systems that filter traffic; traffic processing; and network interfaces with processing involving the status IDs of TCP handshakes

Web server logs store the following data at a minimum:

- Timestamp
- IP address
- Content requests and content transmitted
- Error messages relating to requests
- Error, warning and notifications relating to system operations

Maintenance and change logs store the following data at a minimum:

- Timestamp
- The agent of a change
- The type of change (add, edit, delete) and target (especially when relating to access rights)
- In cases of critical maintenance, the entire audit trail is stored

4. How we collect personal data

Identity management and user identification data are obtained from the basic registers for Aalto University students and staff.

Data on staff are collected also from e-service requests and from use of Aalto's network printer service.

Data on staff is also obtained from the detected or inferred use of services and systems owned or administered by Aalto, when staff use Aalto office, computer or telephone devices and programs, including electronic communications, email and internet applications.

5. To whom do we disclose personal data?

Personal data is processed only by those Aalto employees or those contracted individuals working on behalf of Aalto who have a right to process the data.

Personal data is disclosed to Haka identity federation services with consent for disclosure given by the user on his or her first use of the services.

We may disclose your personal data to third parties where access to or processing personal data is necessary:

- to comply with applicable legislation and/or court order
- to detect, prevent or otherwise address technical or security issues or malpractice.

Personal data is not disclosed on a regular basis.

Users who download Microsoft Office 365 under the agreement between Aalto University and the service provider agree to the Office 365 terms of use regarding data disclosure.

6. Transfer of personal data to third countries

The data protection policy of the university is to exercise particular care if transferring personal data outside the EU and European Economic Area (EEA) to countries that do not offer the level of data protection required by the European General Data Protection Regulation (GDPR). Transfers of personal data outside the EU and EEA are also done in accordance with the requirements of the GDPR.

As general rule, however, our processing of the personal data of employees occurs only within the EU or EEA. In exceptional cases of, for instance, international assignments or the use of certain services, your personal data may need to be transferred outside the EU or EEA. In such cases, we see to ensuring a level of personal data protection adequate to conform with the level required by legislation, such as in the standard agreement clauses approved by the European Commission.

7. How long is personal data is stored?

The periods for which personal data may be retained in systems is based on law and on the records management plan (TOS) of Aalto University.

8. Rights of the data subject concerning personal data

Right to access and rectify data

According to the GDPR, you have a right to know what information on yourself is stored in the personal data file.

You have the right to request that any inaccurate or erroneous data on yourself be rectified without undue delay. If data you wish have rectified or erased is maintained by an Aalto partner, we will request that the partner take the appropriate measures.

Right to be forgotten, withdrawal of consent:

Barring certain exceptions, the GDPR guarantees your right to have your erased, or as it is termed, your right to be forgotten. However, this right does not obtain in cases where the university's right as the controller to process personal data is based on the university's obligation to perform tasks carried out in the public interest or in the exercise of official authority.

If the processing of personal data is based on your consent, you may also withdraw your consent. In that case you may submit a request to us to erase data concerning yourself from our system. If there is not other legal grounds for processing your data, we will delete it.

Right to restriction of processing

If you contest the accuracy of the personal data or the lawfulness of the processing, or or if you have exercised your right to object to the processing, you may request that the processing of the personal data be restricted to storage only. The processing of the data is then confined to its storage only until, for example, the accuracy of the data is verified.

If you do not have the right to request erasure of the data, you may request instead that Aalto University limit its processing to only that needed in order to store the data.

Right to object to processing where Aalto University has a legitimate interest

You always have the right to object to the processing of your personal data when the processing is for marketing purposes.

9. Exercise of rights

You may exercise your rights by submitting a GDPR-compatible request via Aalto's personal data portal: Aalto University personal data portal

Note, however, that if the matter concerns a change of contact information or other routine changes, you should contact: servicedesk(at)aalto.fi.

If you have questions regarding this privacy notice, you may contact the Aalto University data protection officer:

Data protection officer: Anni Tuomela
Tel.: (exchange) 09 47 001
Email: dpo@aalto.fi

If you, the data subject, consider the processing of your personal data to be an infringement of privacy protection legislation, you have the right to lodge a complaint with the data protection ombudsman (www.tietosuoja.fi), which is the supervisory authority.

10. Right to receive notice of a personal data breach

We have an obligation to communicate personally any security breach of personal data to those data subjects whom the breach concerns. The right enters into force if the breach may likely result in a high risk to the rights and freedoms of the individual, e.g. in the form of identity theft, payment fraud or other criminal activity.

An information security team operates at Aalto (email security(at)aalto.fi) to process reported data protection and information security incidents concerning the university and to help resolve them, investigating whether data breaches have occurred.

11. Controller, person responsible and contact details

The controller is Aalto University.

The register person-in-charge is Christa Winqvist.
Tel. (exchange): 09 47 001
Email: servicedesk(at)aalto.fi

The Aalto University communications director is responsible for university-level communications and marketing.

12. Your responsibility

You are responsible for the information you supply or make available to Aalto University recipients, and you must ensure the accuracy of the information.

13. Personal data and principles of privacy protection

Due diligence is observed in the processing of personal data and data security measures are followed as appropriate. Technical solutions such as firewalls and encryption are employed and they comply with current standards. The controller ensures that stored information, user permissions and other

data critical for the security of personal data are processed according to instructions, confidentially and only by individuals whose job descriptions authorise the processing.

14. Amendments to the privacy notice

Updated versions of this notice will show the date of the new version at the beginning of the document. If we make changes to content of this notice, we will take appropriate measures to keep you informed in a manner consistent with the significance of the change.