

Unofficial translation

**Aalto University
HR Services**

General privacy notice for employment relationship matters

Valid from 25 May 2018 onwards

Updated 29.8.2018

- 1. Introduction**
- 2. Lawful basis for processing**
- 3. How we collect information**
- 4. How we process information**
- 5. For what purposes we collect and process personal data**
- 6. What information we collect and process**
- 7. To whom we disclose information (*updated 29.8.2018*)**
- 8. Transfer of personal data outside the EU or EEA**
- 9. How long do we retain information**
- 10. Your rights**
- 11. Other rights**
- 12. Who you can contact**
- 13. Your responsibility**
- 14. Amendments to the notice**

1. Introduction

Protecting your privacy and your personal data is of the utmost importance. We at Aalto are committed to complying with the requirements that data protection regulation places upon us in the processing of your personal data.

This general privacy notice for employment relationship matters, aimed at employees, describes the university data protection policies concerning the personal information collected and processed in connection with employment relationship affairs and other similar processes.

FURTHER INFORMATION:

Personal information refers to all identifiable information related to a natural person. As for the processing of personal information, it refers to operations targeting personal information.

At Aalto, also a **Personal Data Policy** for the protection of personal data has been confirmed as a code binding the members of the university community.

In addition to legislation regarding the protection of personal data, the university is bound by the Act on the Openness of Government Activities (621/1999). According to the prin-

principle of public access, all information held by the university is public unless otherwise decreed. Thus, the publicity of personal data is determined by this legislation. The legislation also applies to the divulgence of personal data from the university's personal data registers. In accordance with the Act on the Openness of Government Activities, the university may be required to divulge information that includes personal data to third parties.

In addition to the above, the processing of personal data at Aalto is guided and complemented by the **University Data Control Plan**.

Aalto has designated a **Data Protection Officer** (tietosuoja@aalto.fi, dpo@aalto.fi).

2. Lawful basis for processing personal data

As an employer, Aalto requires personal information from employees in order to meet the various employers' obligations as well as perform statutory and voluntary tasks. In addition to the management of employment relationships, we process personal information for various other reasons, for instance for the authorities when managing taxation and social security payments, and for the management of personnel administration and supervisory work. The information is also needed for the management of processes related to the operation of the university and for collecting information, for statistics and for reporting.

The lawful basis for processing of personal employee information is based on either **the legal obligation** to which the controller (Aalto as employer) is subject **or legitimate interest** consisting of an employment relationship between Aalto and the employee or another functional connection with the university (e.g. Academic and other visitors, and grant recipients).

In our operations, we take the employees' privacy protection into account. It includes the possibility of having an effect on the processing of their own personal data and the right to be assessed based on correct information. We only process information which is immediately necessary for the employment relationship and related to the management of the rights and obligations of the parties to the employment relationship or to the benefits provided by Aalto to its employees or which is due to the special nature of the work tasks. We make sure we do not collect unnecessary information even with the consent of the employee.

FURTHER INFORMATION:

The Act on the Protection of Privacy in Working Life:

The processing of personal employee information is governed by the Act on the Protection of Privacy in Working Life (759/2004), which determines what types of personal employee information the employer may process and how the information is collected. The Act also includes specific provisions on merit rating and aptitude tests, health tests, drug tests as well as camera surveillance and e-mail protection.

The general principles and practices related to the protection of employee privacy shall be discussed in the co-operation procedure: At Aalto, this occurs either in the University

co-operation committee or between the employer's representatives and the chief trade union representatives. The personal information of individuals is not processed in the co-operation procedure described above.

E.g. the following principles and practises has been discussed in the co-operation process: The university data protection policy, this General Privacy Notice for employment matters, principles for merit rating and aptitude tests as well as credit data verification in connection with recruitment, health tests for employees, camera surveillance, other technical surveillance and e-mail protection.

Health-related information:

Information on health condition or so-called health information is specific (sensitive) data. According to the definition of the data protection regulation, health information includes all information concerning the data subjects' health condition or disclosing information on the former, current or future physical or mental health condition of the data subject. According to the basic principle, health information may only be processed based on registered consent.

The employee shall be entitled to process information on the employee's health condition if:

1. it is required for processing the employee's pay during illness or comparable benefits related to the employee's health condition;
2. it is required on justifiable grounds to establish whether there is a right to be absent;
3. the employee specifically wishes that their work ability be determined based on information on their health condition.
4. In addition, the employer shall be entitled to process information on the employee's health condition in situations and to the extent provided for elsewhere in legislation. (such as the Occupational Safety and Health Act Section 8).

3. How we collect information

We collect information primarily from individuals themselves, mainly in written form through the current HR form or electronic system used at Aalto University.

Information on employees is also collected through electronic service requests, cost management and time tracking as well as camera surveillance. The information collected on employees may also be observed and derived from the use of services and systems owned or administered by the University as the employee uses the office, computer and telephone devices as well as software, including electronic communication, e-mail and Internet applications provided by the University.

We also collect information from sources other than the employee, such as supervisors, insurance companies, occupational healthcare and the authorities (such as the tax authorities or the Social Insurance Institution of Finland). If information on the employee have been collected from sources other than the employee, we will notify the employee of the information we have received before it is used for decision-making concerning the employee.

When required, we will ensure that we request the written consent of the employee for collecting information from other sources. For instance, we always request the written consent of the employee for collecting information on the employee's health condition from third parties.

FURTHER INFORMATION: Information collected from other parties:

(1st line) managers: Various information on employment relationship administration, such as: The approval of work plans, processing absences, objective discussions, the performance support process, referrals to work ability negotiations, information on processes under the salary system (requirement level of the task and the assessment of the personal performance)

Employer's representative: Information under the salary system process, service personnel career information

Occupational health care:

Statement on the final conclusion of a health check (work ability assessment / compulsory health check to be performed on the initiative of the employer's representative / supervisor, the Occupational Health Care Act Section 13)

Necessary information on the use of occupational health services (name data, dates of visit, information on whether the visit was a Kela 1 visit (preventive), a Kela 2 (treatment of illness) or Kela 0 visit (non-refundable by the Social Insurance Institution of Finland). The information does not include the reason for the visit / diagnosis, and the information received will not be stored in the HR data system.

Enforcement authorities: The payment prohibition addressed to the employer for garnishment of salaries.

Tax authorities: Tax card information is received directly from the Tax administration for all employees with a valid employment relationship (regular monthly salary, hourly-paid teacher, hourly-paid employee) on 31 December and whose employment relationship will also continue after 1 February.

The Social Insurance Institution of Finland KELA: Decisions on daily sickness benefits

Insurance company: Decisions related to accidents, decisions on rehabilitation support

4. How we process information

We will process the data subject's personal data according to the Data Protection Regulation in ways that respect their rights and liberties. We will ensure that the principles of data protection are followed in all stages of personal data processing.

Personal information will be processed both manually (on paper), and electronically and in various different data systems which are administered either by Aalto University or its partners. Key registers related to employer activities and employment relationship matters are maintained in the university personnel service data systems. In terms of salary accounting, personal information is also processed in the university accounting system.

In various processes related to employment relationship affairs, personal employee data is processed exclusively by the university employees or partner employees who are entitled to process personal information. Access and reading rights on the data systems are determined and granted, to the extent required by the task, only to individuals who need the personal data file information within the data system concerned in order to perform the task assigned to them.

Employees processing personal data have a statutory obligation of secrecy. This means they may not disclose information in the personnel register to third parties.

Information is processed as required in the Act on the Openness of Government Activities and the Universities Act (621/1999) and in data protection legislation. When information is disclosed from the university personnel register, the university must ensure that the recipient has the right to store and use such personal information under the provisions on personal data protection.

Registers related to employment relationship affairs contain confidential information under various paragraphs of the Act on the Openness of Government Activities and the Universities Act Section 24 (such as bank account numbers, information on health conditions, assessments made for the grounds for remuneration, personal pay component, information on the direct recovery of membership fees, decoration proposals).

FURTHER INFORMATION:

The processing of information on health conditions:

The processing of information on health conditions has been limited to the minimum number of people. At Aalto, information may only be processed by employees who, based on this information, are preparing or making decisions on employment relationships or implementing such decisions. Employees processing information on health conditions may not disclose this information to third parties, and the obligation of secrecy continues even after the end of the employment relationship.

The information received from occupational healthcare (statements on work ability, memoranda on work ability negotiations, visits to occupational healthcare services) is not stored in the HR data system, and it is kept separate from other information in a locked facility.

Processing of sick leave certificates: The employee may submit a sick leave certificate directly to the payroll team of their unit, which will ensure grounds for salary payments. In this case, information on the diagnosis may not be revealed to parties such as supervisors without the employee's consent. In this case, it may only be revealed whether the sick leave certificate is issued by occupational health services or not. Sick leave certificates are stored in the payroll team facilities in a locked archive separately from other stored materials.

5. For what purposes we collect and process personal data

We collect personal data for various purposes related to employers' obligations, salary payments and the management of employment relationship affairs.

Employee personal data processing purposes include:

Statutory employer tasks:

- Management of employment pensions and insurance for occupational accidents and occupational diseases
- Occupational safety management
- Organisation of occupational health care
- Statutory notices and payments to the authorities and to pension and insurance companies

Management of tasks due to employment relationships (or other relationships)

- Implementation of provisions in the collective agreement applicable to universities and the management of related processes
- Implementation of provisions related to local Aalto agreements and the management of related processes
- Tasks related to the processing and payment of salaries, fees and grants and related statistics
- Tasks related to the processing and payment of various expenses and reimbursements and related statistics
- Management of IT permits and access rights
- Management of benefits provided by the university
- Management of information related to competence and their development
- Management of processes related to work ability
- Management of performance support process
- Management of personnel working abroad
- Targeting working hours (for sharing salary costs for projects)
- Management of the process of employment relationship termination
- Selection of residents for company residences

Other tasks related to university activities:

- Collection of feedback
- Organisation of personnel events
- Management of decorations
- Production of visibility services (academic personnel)
- Review of the impact of university activities
- Reporting on employment relationship affairs and management of such reports
- Organisation of elections for various university bodies
- Management of co-determination procedures
- Personnel reporting and planning of personnel affairs
- Management of university and personnel communications
- Management of facilities

- Management of information technology and data communications such as e-mail systems
- Ensuring the physical and IT-related safety of personnel
- Logging, scans, camera surveillance and access monitoring
- Management of judicial processes
- Management of audits and other similar affairs and processes
- Production of information for stakeholders (auditors, the Ministry of Education and Culture, the Academy of Finland)

6. What information we collect and process

Registers related to employment relationship matters contain the personal data of current and previous employees, wage-earners, beneficiaries of fees, academic and other visitors and beneficiaries of grants.

The personal data groups under the data protection regulation processed in the register include

- basic information
- personal information with specific requirements (such as bank account numbers and personal identity numbers)
- particular personal information (health information, such as sick leave certificates)

The information contained in the registers are completed as the employment relationship progresses and throughout out its validity.

We collect e.g. the following personal data required for maintaining an employment relationship or other status:

Various identification data, such as:

- Name, contact details
- Personal identity number
- Citizenship
- Gender
- Information on degrees

Information due to the employment relationship and created during the employment relationship, such as:

- Employment contract information
- Information related to pay and payment
- Information on residence or work permits, and the validity of passports
- Information on the assessment process under the university salary system
- Information on objective discussions
- Information on work ability
- Information on work plans (total working hours system)

- Career information (service personnel)
- Information on secondary occupations and interests
- Information on participation in personnel training / trade union training
- Information on absences and on the grounds for absences
- Recorded information related to access rights / information recorded on access events
- Time tracking information and information recorded on working time stamps
- Trade union membership / unemployment funds when the employee has given a proxy for direct recovery (particular personal information)
- Tasks representing employees
- Information on State awarded decorations and Aalto Awards

FURTHER INFORMATION:

Other collected information which is collected based on meeting statutory obligations:

Exposure to substances: The employer has a statutory obligation to systematically collect information on chemicals and other substances causing exposure, in accordance with the provision in Government Decree 603/2015, to inform employees of dangers to foetal development or to pregnancy if factors potentially causing such risks are used or present at work. The occupational safety expert of Aalto University will be in charge of the register.

Management of personal safety:

Ensuring the occupational safety of employees in separately determined working facilities serves as the grounds for keeping a register. The register only includes employees in whose working space the employer has considered it appropriate to install an alarm service. The Head of Security and Risk Management at Aalto University will be in charge of the register

Camera surveillance:

The purpose of camera surveillance is the prevention of crime and vandalism targeting university property located in public spaces, teaching and hardware facilities, and examining the questions on liability for damages caused. The purpose of surveillance is also to monitor the safety of the facilities and to uphold order, thus ensuring and improving the safety of personnel and students as well as the other individuals visiting or working in university facilities.

At the university, surveillance cameras have been installed in:

- IT class and hardware facilities
- lobby facilities
- entries to buildings
- the immediate vicinity of buildings.

The Head of Security and Risk Management at Aalto University will be in charge of the register

Reports on exceptional events

Aalto collects information on events related to workplace safety and occupational safety. Reports on events may be made by Aalto employees and students. Based on the information received, workplace safety and occupational safety will be improved. The Head of Security and Risk Management at Aalto University will be in charge of the register.

Administration of occupational accident reports:

As an employer, Aalto University has the statutory obligation to examine the accident and causes leading to the accident and to report the accident to insurance companies and, where necessary, to the authorities (serious occupational accidents). As an employer, Aalto University also has the obligation to maintain a list of accidents.

The university has a designated accident officer acting as a contact person for the register and providing additional information in questions related to occupational accidents.

Occupational safety orientation:

Aalto University maintains a register on occupational safety orientation. As an employer and an educational institution, Aalto has a statutory obligation to ensure sufficient occupational safety orientation.

Reserve location register:

Management of temporary working premises due to indoor air quality.

Aalto's designated occupational safety expert serves as a contact person for the register.

7. To whom we disclose information

As an employer, Aalto has statutory obligations to disclose the personal data of its employees to parties such as various national authorities (such as the tax authorities), employment authorities in the EU and to banks, insurance companies and occupational health services. According to the provisions in the collective agreement applicable to universities, we also disclose personal employee information to personnel representatives (chief trade union representative) and actors such as auditors in connection with internal audits.

Aalto University also purchases certain personal data processing services from its partners. A service provider is a processor to the extent that it processes personal data for purposes defined by Aalto University. In situations where the service provider defines the purposes for processing personal data, the service provider is considered the controller of the data. This processing is subject to the service provider's own privacy notice. For example, when an employee orders a cloud service platform as a representative of the organization, the service provider is the processor of the personal data that is included in the data files uploaded to Aalto University's instance of that cloud service platform. However, for information related to the company's contact person at Aalto, such as their name and email address, the service provider will define the purposes of processing. The service provider may process personal data it is the controller of in accordance with its own privacy notice.

We have only selected personal data processors who comply with good personal data processing practices by means of appropriate technological and organisational measures, that meet the requirements of data protection regulation, and who are able to ensure that your rights are adhered to to act as our partners.

In addition, Aalto University transfers personal data in accordance with the privacy notice for Aalto communications, for example when photographing events and publishing these images on social media platforms such as Instagram.

FURTHER INFORMATION:

Information disclosed to occupational health services:

Aalto has a contractual obligation to submit to the occupational health care service provider the names, personal identity numbers and the information on the validity of the employment relationship for individuals entitled to occupational health care. To perform its statutory task, Aalto regularly submits to occupational health care services the information on employees' sick leave period and its duration and on the substances to which employees may be exposed due to their work.

The sick leave periods and diagnoses external to occupational health care services may be disclosed to occupational health care service providers, unless the employee exercises their right of prohibition. The prohibition may apply to individual disclosures or certain periods. The employee may communicate the decision to exercise their right of prohibition through the e-support service. Despite the fact that the employee exercises their right of prohibition, we may disclose the information on the period and duration of the employee's sick leave to occupational healthcare services.

Carrying out work ability negotiations: Referral of an employee to work ability negotiations on the initiative of the employer. Based on this, occupational healthcare services will arrange work ability negotiations between the employee, the supervisor and the HR representative.

Carrying out a work ability assessment / mandatory health check: Referral to the work ability assessment / mandatory health check. Based on this, occupational healthcare services will arrange a work ability assessment for the employee.

Information disclosed to personnel representatives (head personnel representatives) based on the collective agreement applicable to universities:

At least twice a year, information on **new fixed-term employment relationships**

- Information on name, task, unit within the organisation, start date of the employment relationship, the duration of the employment relationship known to the employer and grounds for the fixed-term employment relationship.

8. Transfer of personal data outside the EU or EEA

The university's data protection policy involves particular care when personal data is transferred outside the EU and the European Economic Area (EEA) to countries which do not offer outside data protection in accordance with the EU Data Protection Regulation. Transferring personal data outside the EU and the EEA shall be carried out in accordance with the requirements of the Data Protection Regulation.

As a rule, we process employees' personal information only within the EU or the EEA. In some exceptional cases, for instance in connection with employees posted abroad or with the use of certain services, it may be necessary to transfer your personal information outside the EU or the EEA. In that case, we will ensure a sufficient level of protection for personal information as required in legislation, for instance by using contractual clause templates approved by the European Commission.

9. How long do we retain information

Registers for employment relationship matters consist both of so-called manual materials (such as employment contracts, transfer of rights agreements and various forms) and of information stored in systems. This retention times for personal data stored in the system and the retention times for documents created in employment relationship processes are based on legislation and on Aalto University's information management plan.

According to the data protection principles, we do not store expired or unnecessary information on current or former employees.

After the end of the employment relationship, it is usually only necessary to store employee data as long as employees are entitled to file a claim against the employer. The time limit for filing a claim may be based on the Employment Contracts Act, the Working Hours Act, the Act on Equality between Women and Men or on the Penal code, which all contain various time limits for filing claims. As for the storage of pay data, the provisions of the Accounting Act must also be taken into account.

Permanent storage

- Storage of work history information
- Information on awarded decorations

Fifty-year storage:

- Most information related to payroll accounting and information which may have an effect on pensions
- Employment contracts and transfer of rights agreements

10. Rights of the data subject

Right of access and the right to the correction of data

Based on your rights under the data protection regulation, you are generally entitled to know which personal information on you is stored in the personnel register.

You have the right to request that we correct your inaccurate and erroneous personal information without unnecessary delay. Should our partners be in possession of your information which requires correction or deletion, we will request that our partners carry out appropriate procedures.

Rights to be forgotten, withdrawal of consent

With such exceptions, the data protection regulation also guarantees your right to delete your data, or the so-called right to be forgotten. If there are no other legal grounds for processing personal data, we will delete the data.

If the processing of personal information was based on consent, you will also have the right to withdraw your consent. In this case, you may request that we delete your information from our systems. If there are no other legal grounds for processing personal data, we will delete the data.

11. Other rights

Right to lodge a complaint with a supervisory authority

If the processing of your personal data is in breach of applicable legislation, you have the right to lodge a complaint with the national supervisory authority. You can lodge the complaint with a competent supervisory authority. In Finland, this is the Data Protection Ombudsman, and the complaint must be lodged in accordance with instructions provided by the Office of the Data Protection Ombudsman. Please see <http://www.tieto-suoja.fi> for more information.

Right to be notified of a personal data breach

We have an obligation to notify directly the data subjects whose data are affected by a personal data breach. The right will take effect, if a violation is likely to result in a great risk to the rights and freedoms of the individual, for instance in the form of identity theft, fraud related to means of payment or other criminal activities

Aalto has the data security unit (e-mail security@aalto.fi), which processes reports on data security and data protection anomalies affecting Aalto University, and provides assistance for solving anomalies, for instance by investigating potential hacking.

12. Who you can contact

Should you like to exercise any of your rights mentioned above, you may contact us by sending an email to [dpo\(at\)aalto.fi](mailto:dpo(at)aalto.fi).

Registers maintained in HR systems: Information requests on registers maintained in HR systems may be addressed as a service request [e-support-hrssystem\(at\)aalto.fi](mailto:e-support-hrssystem(at)aalto.fi)

Data protection notice: If you have questions or concerns about this data protection notice, please contact us by sending email to [dpo\(at\)aalto.fi](mailto:dpo(at)aalto.fi) or by post to Aalto-yliopisto/kirjaamo/Tietosuojavastaava, PL 11000, 00076 Aalto. Please refer to this data protection notice addressed to applicants in your message.

The Data Protection Officer will answer questions related to data protection policy, the University's compliance with the data protection regulation and other legislation on personal information and the processing of personal information at the University.

13. Your responsibility

You are responsible for the information you submit or make available to Aalto University. You must ensure that the information is correct and accurate and not misleading in any way.

14. Amendments to the notice

This data protection notice is not part of an employment contract or other contract, and we update it where necessary. When this notice is updated, the date of the latest update will be indicated at the top of the notice. If we make substantive changes to this notice, we may take appropriate measures to inform you in a way that is consistent with respect to the significance of the changes. We encourage you to check this notice often to be aware of how Aalto University protects your data.