15/05/2018

Instructions for HR and supervisors on processing employee personal data for employment relationship purposes

Introduction

As an employer, Aalto requires employee personal data to enable its activities and to meet its statutory obligations. We only process information necessary for the employment relationship which is 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.

As an employer and a data controller, Aalto is liable for processing employee personal data throughout its life cycle according to the data protection regulation in a manner which respects the rights and liberties of data subjects. In the general data protection notice for employment relationship affairs, we inform the employees – including you – on the university data protection practices which concern the personal information collected and processed in connection with employment relationship affairs and other similar processes. The data protection notice shall determine how personal information is systematically processed in connection with the management of employment relationship affairs, and data may not be processed in a way incompatible with purposes indicated in the notice.

It is particularly important that all supervisors and HR employees are able to take into account both issues related to the protection of employees' privacy and data security in practical measures and that they are also aware of their obligation of secrecy.

Data protection policy

The university has an established data protection policy. Please familiarise yourself with it and ensure that data protection policy and other issues related to data protection are discussed in connection with the orientation of new employees.

Online training:

The Aalto University basic data protection online course is available to all employees in the MyCourses learning environment. All supervisors and HR employees are required to complete this online course.

Roles and responsibilities for data controllers

The registers for employment relationship affairs, payrolls and recruitment maintained on the university level consist of both data stored in systems and so-called manual materials (such as employment contracts and transfer of rights agreements). **As an employer, Aalto is the proprietor of the data processed in these registers and shall be liable for the various obligations of the data controller**. All of these registers have a designated contact person (practical administration of the register), a system administrator in charge of the administration of data system user names and user rights, and a designated university-level person in charge of the

registers. Data processed in the registers may only be processed by individuals in charge of such work tasks (= personal data users designated by the employer).

The 'Approval authorisation for employment relationship affairs' document confirmed by the President and the HR director determines the approval authorisation for key employment relationship affairs. These approval authorisations will determine the competencies on the level of schools and departments when employee personal data is processed for processes related to employment relationship affairs. Further information is available from your school HR director.

Data storage:

The storage periods and the criteria for determining the storage periods for personal information stored in the system and for documents created in employment relationship processes have been confirmed in the Aalto University Information management plan. According to the data protection principles, we cannot store expired or unnecessary information on current or former employees. As for registers maintained on the university level, persons in charge of registers / system administrators shall be in charge of destroying information in the archive and in the systems. The University payroll team shall be in charge of storing information in the employment affairs and payroll basic register (information storage in the systems, employment contracts and other centrally stored forms) and of deleting this information. Individual personal data users will always be liable for not storing information / documents whose storage period under the Information management plan has ended.

- Further information on the Information management plan (TOS) is available at the document administration and, in terms of issues related to employment relationship affairs, from the Legal Adviser for Employment Relationships.

Use of personal information by supervisors and HR

The processing of personal information may involve anything beginning with the collection, the recording, the organisation, the use, the transfer, the disclosure, the storage, the modification, the combination protection of data and ending with the deletion and destruction of the data.

- This means that the processing of personal information includes features such as the preparation of employment contracts, the approval of annual leave in the EES system, the documentation of objective discussions, the issuing of a certificate of employment, and the electronic or manual storage of various documents containing personal information.

The processing of employee personal information is an essential part of the work tasks of supervisors and HR, and the data protection regulation will not change this fact. As a user of personal data designated by the employer and depending on your role, you may process the personal data of the entire school, individual or several departments or the employees in your team. You will process personal information in various ways, orally in discussions, in writing, in electronic workflows, in data systems and by e-mail. Access rights to HR data systems will always be determined according to your work tasks.

The data you process may be related to recruitment, the creation of employment contracts, payrolls, budgeting, travel, performance, work ability, interests, absences etc. Under the Act on the Openness of Government Activities, some of the information processed must be kept confidential or is sensitive (health information), which places particular demands on data processing.

Personal identity number

Employees' personal identity numbers are processed on the grounds that there is a need to identify employees non-ambiguously in order to meet various employer obligations. The processing of personal identity numbers must be as restricted as possible, and it must not be indicated in documents such as leave lists circulated at the University. Personal identity numbers must not be included in documents, reports or other similar materials where the non-ambiguous identification of employees is not necessary (such as budgeting).

Personal identity numbers must always be hidden in documents (such as employment contracts) disclosed to third parties (such as auditors).

The obligation of secrecy is emphasised when the information processed must be kept secret

The management of employment relationship affairs and supervisory tasks also involves the processing of information related to the characteristics, personal situations, health conditions or financial position of employees. This information must be kept secret, and it must not be disclosed to third parties.
In addition to parties external to Aalto, third parties include all Aalto employees not in charge of processing the personal information of the employees concerned.

- Particular attention should be paid to the processing of the following information: Bank account number, tax card information, various information on personal situations (lifestyle, hobbies, family life, political convictions, information on financial position), assessments made for the grounds for remuneration, objective discussions, personal pay component, disciplinary measures.

Health information

Information on individuals' health is sensitive and is therefore included in the key areas of privacy protection. In terms of sensitive health information, individuals' right to self-determination and privacy are particularly emphasised.

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.

- Thus, health information includes all information on individuals' physical or mental health, not only medical findings or diagnoses. Thus, health information also includes

information on rehabilitation, referral agreements, the discussions in work ability negotiations and corresponding memoranda, the statement of the occupational health service on the employee's work ability, decisions on partial disability pension, and the information provided in occupational accident reports.

In which cases may the employer process health information?

The employer may only process information on the employee's health information if it is collected directly from the employee or from other sources with the employee's written consent.

In addition, it is required that one of the following grounds for processing be met:

- The information is required for processing the employee's pay during illness or comparable benefits related to the employee's health condition, or
- for establishing whether there is a justified reason for absence; or
- the employee specifically wishes that their work ability is determined based on information on their health condition; or
- the information is processed based on another legal act (such as the Occupational Safety and Health Act Section 8)

Processing of sick leave certificates at Aalto:

The employee may submit a sick leave certificate / copy of an electronic sick leave certificate directly to the payroll team of their unit which will establish whether the employee is entitled to pay during illness and which will ensure the central storage of sick leave certificates. In this case, the content of the sick leave certificate may be revealed to the supervisor or the school HR only to the extent of revealing whether the sick leave certificate has been issued by the occupational health service or not. However, the employee may reveal the diagnosis to the supervisor at their own initiative. The supervisor and HR will also be informed of whether the employee will be entitled to pay during illness.

If the employee had submitted a sick leave certificate (scanned or in printed form), do not store any certificate information on your computer or copy the sick leave certificate for your own archive. Let the employee know that you will submit it to the payroll contact person in your unit.

Obligation of secrecy for processing health information

Individuals processing employee health information have a particular statutory obligation of secrecy. According to this obligation, employee health information may not be disclosed to third parties during or after the employment relationship.

Please keep in mind that the supervisor or HR are not in charge of assessing the employee's health condition or providing diagnoses! This should only be done by healthcare professionals.

Information on sick leave:

Information on an employee's sick leave should not be announced in public at the workplace. The simple information that an employee is ill is not considered sensitive personal information, but it is still personal information. However, the cause of the illness is sensitive personal information. The information on the employee's sick leave may in individual cases be revealed to their closest colleagues, but it is sufficient to inform others of the fact that the employee is 'absent', unless it has been agreed with the employee, for instance during a discussion, that the reason for the absence may be revealed. This also applies to situations where the absence is due to the illness of the employee's child.

Further information:

Further information on the subject is available from your school HR director, work community service experts and the Legal Adviser for Employment Relationships.

Organisation of the Information Management life cycle

Examine your own archives (electronic archives and potential paper archives) critically to find out which employee-related information they contain and how old it is. It is important to leaf through these archives regularly in the future – **at least every six months** – and to delete unnecessary information, paying particular attention to the following:

School or department-specific archives or personal archives

It is difficult for Aalto to meet the data controller's obligations if information and documents related to the management of the life cycle of employment relationships are stored not only in the central archives of HR data systems but also in school or department specific or personal media such as network drives.

The objective is that documents (such as various HR forms and their annexes) containing personal information whose content is stored in the University HR data system or the documents which themselves are centrally stored in the payroll unit archive or, for instance, an electronic case management system (such as visitor agreement) are not filed on network drives or other electronic platforms for personal information users acting on behalf of schools, departments or individually.

HR network drive archives:

- These archives must be discontinued and their data must be deleted in a controlled manner by the time the new HR data system has been implemented. The measures for the transition periods have been discussed with school HR managers.

Reports containing personal information, made for individual purposes:

The tasks of supervisors and HR involve the processing of various reports containing personal information, such as time tracking, sick leave, annual leave, information on interests, HR planning reports etc. The information within these reports is mainly derived from information stored in data systems.

When the objective of the report has been achieved, the report must be destroyed no later than six months later according to the instructions for destroying information materials.

Requests related to individual employees - requests related to the pay system, requests for decorations etc.)

Once a request for an individual purpose has been submitted to the party dealing with the matter and once it has been processed, there is no need to store the request.

Certificates of employment:
Five years after the end of the employment relationship, the employee shall be entitled to receive a so-called extensive certificate of employment, and ten years after the end of the employment relationship, a limited certificate of employment. If an extensive certificate of employment has been issued, please submit the certificate of employment to the HR contact person in your unit for centralised archiving.

Printed documents:
Should you print documents containing any personal information for another individual (e-mails, job applications and their annexes, objective discussions, completed forms etc.), you should store such documents in a locked cabinet and ensure their destruction once they have served their purpose (recruitment or objective discussion is over).

E-mail as a tool for employment relationship affairs
E-mail may still be used to deal with many issues related to employment relationship affairs.

However, always be sure to pay attention to the types of issues you deal with by e-mail and to whom / to how large a group of people you send information on another individual. Please note that many issues may be dealt with without the name of the employee. Avoid processing health information concerning employees by e-mail.

Should you send confidential personal information or information which must be kept secret by e-mail, encrypt the personal information by using features such as the Encrypt button in the Aalto University Outlook.

Protected e-mail should always be used when confidential personal information (such as bank account numbers or personal identity numbers) are sent outside of Aalto.

What is encrypted or protected e-mail? More detailed instructions on the data security for processing personal information is available in the ITS guidelines.

Recruitment instructions

Aalto processes job applicants' information in a manner which respects their rights and liberties. If there are external experts involved in recruitment, an agreement will be made with them on the processing of personal information.

By participating in the recruitment you may receive limited fixed-term access rights to the electronic recruitment system (SAIMA). Access rights to the electronic recruitment system are for personal use only and may not be given to others. You will be personally responsible for all aspects of the use of the username and the information you processes and save using it.

Materials related to recruitment will only be processed by those involved in the recruitment concerned. Please ensure that you do not distribute, on your own initiative or at any request, job applications to your colleagues or share views on individual applicants formed based on interviews. Please ensure that you always transfer potential information requests related to recruitments to the HR contact person for the recruitment concerned.

Materials related to recruitment are stored centrally according to the University Information management plan. The storage of the materials shall be ensured by the HR contact person for the recruitment concerned. Thus, when the recruitment process is completed, there is no need to store materials related to the recruitment personally (on your computer or in printed form). Instead, you should ensure that you delete the materials (application materials, expert statements, protocols etc.) from your computer and that you destroy any printouts (Setec, shredder). Please make sure that you browse through your archives every six months and that you delete the materials for completed recruitment processes.

Please note that potential notes made in connection with interviews are also part of recruitment materials and they must also be submitted to the HR contact person.

--

DATA PROTECTION CHECKLIST

1. Remember that the right to privacy protection is a basic right for all, also in connection with job applications and in the workplace.
2. Identify your role and your work tasks which involve the processing of employees' personal information
3. Familiarise yourself with the Aalto data protection policy, other instructions on the processing and data security of personal information and complete the online training on basic data protection.
4. Make sure you are always careful when processing the personal information of job applicants and employees, regardless of whether the data processed is in electronic, oral or printed form.
5. Take particular care when processing sensitive (health information) personal data, or personal data which must be kept secret (such as personal identity numbers, objective discussions, performance management), and do not forget to protect the information from third parties!
6. Do not store in your own archive any documents which are stored centrally and whose information content is saved in the HR data system.
7. Browse through your archives at least every six months and learn to delete information!
8. Report on suspicions at the following address: security(at)aalto.fi, tietosuoja-vastaava(at)aalto.fi

9. Remember your obligation of secrecy and always adapt your discussions and your working methods to your environment: Do not discuss the affairs of other people, and protect your computer screen from third parties.
10. If you do not know something, please ask! (Data Protection Officer, Legal Advisor for Employment Relationships, HR manager. Data security: ITS services)