Who may access personal data?

What sort of data are staff members at AAU allowed to disclose to colleagues and external parties under the General Data Protection Regulation (GDPR)?

Introduction

Many of our tasks and work routines entail a need to involve other parties, who thereby gain access to personal data. Such parties may include our colleagues in the same department or from other parts of the organisation as well as external parties such as IT suppliers, consultants, public authorities or collaboration partners from research projects.

What?

Before defining '*what*' may be disclosed, it must be considered '*for what*' (the purpose of disclosing data).

Purpose

Our use of personal data is inextricably linked to the purpose for which such data are needed. This means that any use of personal data must be for a purpose, and this purpose must be both explicit and legitimate. This means that it must be clear to other people, and in particular the individuals whom the personal data concern, what the specific data will be used for. The requirement for legitimacy means that the purpose for which the personal data will be used must be lawful (not to be confused with the legal basis for processing described below). This means that we must not disclose personal data for purposes such as tax evasion, money laundering or other criminal purposes.

Legal basis

In addition to a specific purpose, a legal basis for the processing of personal data must exist, which means that we must comply with the requirements concerning the basis for processing, as described in the data protection regulations. In order to process personal data for a particular purpose, we must have a *legal basis for processing* (not to be confused with the lawfulness of the purpose described above). For example, a legal basis for the processing of personal data exists if the processing is carried out as part of a contract made between AAU and an individual. This also applies to actions performed prior to the conclusion of the contract. Furthermore, AAU is entitled to process personal data for the purpose of complying with a legal obligation, or if we have obtained the consent of the individuals whose data we process.

Which data may be disclosed?

The requirements regarding purpose and legal basis also apply in connection with the disclosure of personal data to others. Any recipients of personal data must have a purpose for receiving such data, and are subject to the same requirements: the purpose must be explicit and legitimate.

The amount or categories of personal data we may disclose are determined by the purpose. According to the GDPR, personal data for processing must be *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.* This means that we must collect adequate personal data, but no more data than necessary in order for us to perform the task constituting the purpose of the processing of such personal data. This also applies in connection with the disclosure of personal data: the personal data must be necessary for the recipient to be able to perform a task.

The purpose and legal basis thus determine the personal data that we are allowed to disclose. This means that in some situations, we can disclose everything, in other situations no data can be disclosed, and sometimes we can disclose parts of data sets containing personal data.

Examples:

1: Danish Agency for Institutions and Educational Grants

Disclosure is permitted of some relevant personal data to the Danish Agency for Institutions and Educational Grants about the admission of a student to a study programme. This is relevant in connection with the admission of a student on a study programme who needs to apply for a student grant. AAU discloses information to the Danish Agency for Institutions and Educational Grants confirming that the student has been admitted to a study programme and is therefore entitled to a student grant. For this purpose, the Danish Agency for Institutions and Educational Grants must be given the data that are relevant for this purpose, including the student's identity and confirmation of admission, but the agency does not need to know that the student is a lay member of the National Committee on Health Research Ethics, or that the student has asked for access to a prayer room at the university due to his or her religious beliefs.

2: External examiners

Some relevant personal data about students may be disclosed to external examiners in connection with exams. The purpose of the processing of personal data by external examiners relates to the specific exam that they are involved in assessing. This means that they should only be given personal data relating to the individual student taking the exam in question; they do not need to know anything about the class as a whole, about other exams or other personal data about the student that are not relevant to the exam in question, for instance, that a close relative has died of cancer shortly before the exam.

3: Students

Some data may be disclosed to students about other students in connection with class lists and study groups. The purpose of the students having access to such data is for them to be able to contact their fellow students with a view to coordinating group assignments and the like. This means that data that are relevant in order to coordinate such assignments can be disclosed, whereas data including civil registration (CPR) numbers, periods of illness or exemptions etc. may not be disclosed.

Who?

When deciding to '*whom*' personal data may be disclosed, it is necessary to look at who is *authorised* to perform the task (purpose) for which the personal data are to be used.

Authorised individuals can be colleagues, external individuals or companies/organisations involved in a task which they are to perform for or in cooperation with AAU or a task which they are to perform independently and for themselves.

In companies and organisations, in particular companies and organisations of a certain size, a number of staff members are usually authorised to perform a number of tasks for a particular purpose, and consequently all staff members are allowed access to the personal data.

Internal recipients (staff members at AAU)

It must be ensured that only the staff members who are engaged in the tasks constituting the purpose of the processing of personal data actually receive the data. Under the data protection regulations, a staff member must be *authorised* to access the personal data. It also means that other staff members for whom

the data are irrelevant may not access the data. For the same reason, personal data must not be stored uncritically in various systems, such as on shared drives, where the data are shared with colleagues who do not have a purpose for accessing the data.

The authorisation of individual staff members to accessing or working with sets of personal data depends on the tasks entailed by their job title. So in order for you to be allowed to give a colleague access to a data set containing personal data, this colleague must be authorised to process this particular data set containing personal data, which means that the colleague's tasks must necessitate access to certain personal data about a specific individual or group of individuals. The processing of the personal data is of no concern to any other staff members, who must not be given access to the information.

External recipients

The disclosure of information to external parties who need access to personal data is termed a *transfer* of personal data.

A transfer of personal data is when external parties are given access to personal data held by AAU. A *transfer* covers both the disclosure by AAU of personal data to another data controller[1], and situations in which AAU arranges for the processing of personal data to be undertaken by a data processor[2].

Disclosure

AAU discloses, for example, personal data to the Danish Agency for Institutions and Educational Grants, which processes personal data for its own purposes: the agency needs personal data about students at AAU in order to be able to disburse student grants, for example.

Prior to disclosure, AAU must ensure that the disclosure of data is for a legitimate purpose.

Making data available to data processors

AAU *entrusts* the processing of personal data to, for example, KMD, which processes personal data for AAU's purposes: KMD is the supplier of WorkZone and is, among other things, responsible for storing the personal data stored by AAU in WorkZone.

When leaving the processing of personal data to a data processor, the relationship between the parties must be regulated by a data processing agreement.

When?

Prior to making personal data available to a data processor, a data processing agreement must be made. You can find more information here.

In order for you to be allowed to disclose personal data to a colleague, it must be ensured that your colleague has a valid reason for needing to access the personal data.

[1]Article 4(1), item 7 of the GDPR: 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
[2]Article 4(1), item 8 of the GDPR: 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

In order for data to be disclosed to another data controller, it must be ensured that the disclosure of personal data is for a lawful purpose, and AAU must be able to document this.

If you are in any doubt as to whether you are allowed to disclose personal data to a colleague or external party, you must contact your immediate superior or send an email to AAU's DPO at dpo@aau.dk.