24 May 2018

Lawful/legal basis for processing of personal data

For the processing of personal data to be lawful, the processing must have a clear and well-defined **purpose**, it must be **necessary** to achieve that purpose and it must have a lawful (legal) basis. In practice, for the processing to be necessary it must be impossible to achieve the intended purpose in any other way. For example, if you can achieve the purpose by using anonymised data or without automating the data (i.e. processing the data via a technical means such as a computer), the processing is not considered necessary.

The General Data Protection Regulation (GDPR) gives a number of different lawful bases for personal data processing. These are specified in Article 6 of the GDPR. It is very important to be clear about the lawful basis for your processing before the processing begins. Anyone who intends to perform personal data processing at Uppsala University must state the lawful basis for the processing. The lawful basis must be stated on the eForm used for notification of personal data processing.

The sections below describe the lawful bases you will find in Article 6. Read through them all thoroughly. It is important that you consider carefully which basis is appropriate for your particular processing operation. It can be easy to stop at the first basis, i.e. consent from the person whose personal data you intend to process, but there are other bases and often one of these is more appropriate than consent. If you use consent even though another lawful basis would be more appropriate, you have based your processing on the wrong lawful basis.

In the following sections, the person whose data are to be processed is referred to as ‘the data subject’.

- **Article 6(1)(a): consent from the data subject**

Personal data may be processed if the consent of the person whose personal data are concerned has been obtained. The GDPR requires special conditions for consent, for example, it must be **freely given**. This means that a person cannot consent to a situation where they are in a position of dependence.

One example of this is that consent cannot be freely given if a doctor offers a sick person medical care in exchange for their consenting to take part in the doctor’s study. In this situation, if the sick person cannot receive medical care without consenting, the consent is not freely given.

(Naturally it is possible to offer medical care in connection with studies, the above example is only intended to illustrate that one cannot do this on *the basis of consent* unless a person can also obtain medical care without consenting to participate in the study.)

Further, consent must be given **by a statement or a clear affirmative action (a positive action)**. This means ticking a box, choosing technical settings or some other conduct that clearly indicates consent. It may be a good idea to provide a form that the person whose consent is sought can fill in. You must be able to prove later that the person whose personal data you are processing has given their consent.

The consent must be given after the data subject has received **information about the personal data processing**. Among other things, you must inform data subjects that they have the right to withdraw their consent at any time and tell them the purpose of the processing and how long it is expected to continue.

In addition, particularly strict requirements apply when consent refers to the processing of **sensitive personal data**, such as health data.

Any actor processing personal data on the basis of consent must be able to **show** that the data subject has given valid consent.

If you are already conducting processing activities based on consent and are going to provide notification of this to the register of records (in which **all** processing activities must be recorded), you must verify that the consent meets the requirements of the GDPR. If it does, you can continue the processing on this basis. If the consents do not live up to the GDPR requirements, you must obtain new consents for the processing to be lawful.

- **Article 6(1)(b): performance of a contract**

Another possible lawful basis for personal data processing is that the **processing is necessary for the performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. Examples of this are the processing of personal data in connection with recruitment, and client and staff administration systems for purposes such as invoicing and calculating salaries.

- **Article 6(1)(c): compliance with a legal obligation**

Personal data may also be processed if it is **necessary for compliance with a legal obligation to which the controller is subject**. In this case, the basis for processing must follow from either EU or Swedish law. One example of a legal obligation is the obligation to keep accounts laid down in the Bookkeeping Act.[1]

- **Article 6(1)(d): protection of the vital interests of the data subject**

Processing of personal data is permitted if it is **necessary in order to protect the vital interests** of the data subject or of another natural person. This means interests that are a matter of life and death for the data subject or another natural person. One example is personal data processing that is necessary for vital medical care in emergency situations when the data subject is incapable of giving their consent. This could involve personal data such as blood group, medical history, notification of next of kin, etc., when someone has lost consciousness.

Processing of personal data based on the vital interests of another natural person **should in principle take place only where the processing cannot be manifestly based on another legal basis**. One example is when processing is necessary for humanitarian purposes, for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

- **Article 6(1)(e): performance of a task carried out in the public interest**

[1] The Bookkeeping Act (1999:1078).

Processing of personal data is permitted if it is **necessary for the performance of a task carried out in the public interest**.[2] The task must be prescribed in **EU law or Swedish law**. This means that the task must follow from an act or other statute or from a decision issued pursuant to an act or other statute. Archiving, research and statistics are examples of tasks that can be in the public interest. Other examples are tasks carried out by public authorities in response to explicit instructions from the Riksdag or the government.

- **Article 6(1)(e): performance of a task carried out in the exercise of official authority**

Processing of personal data is also permitted if it is **necessary in the exercise of official authority vested in the controller**. The exercise of official authority must be based on EU law or Swedish law. It is primarily central and local government authorities that may process personal data in the exercise of official authority.

- **Article 6(1)(f): balance of interests**

Processing of personal data may be permitted after a **balancing of interests**. In this case, the processing must be **necessary for legitimate interests that are not outweighed by the interest of the data subject in the protection of their personal data**. Children are considered to warrant special protection. Public authorities can *not* base their processing on a balance of interests when processing personal data in the exercise of their official duties. Such processing has to be based on an act or other statute instead.

The list of lawful bases given above is **exhaustive**. It is possible for more than one lawful basis to be applicable to the same processing operation. If none of these lawful bases is applicable to the processing, the processing is not lawful and may therefore not be carried out.

All processing of personal data **must also comply with the fundamental principles** specified in Article 5 of the GDPR. These principles entail, among other things, that personal data may only be collected for legitimate specified purposes that are not described in too general a way. The amount of data must be limited to what is necessary for these purposes. The data must not later be processed in a way that is incompatible with these purposes, nor may they be retained longer than necessary. One important innovation in the GDPR is that it states explicitly that any actor processing personal data is responsible for complying with the provisions of the GDPR and must be able to demonstrate that they have done so (accountability). Any actor processing personal data must therefore have procedures for ensuring compliance with the provisions. This means that the procedures established for Uppsala University must be followed in every case of personal data processing.

In summary

The lawful (legal) bases on which you can base your processing are:

- consent
- performance of a contract
- performance of a legal obligation
- protection of the vital interests of the data subject

[2] Cf. Judgment of the Court of Justice in Case C-524/06 Huber v. Germany (C:2008:724), on the requirement of necessity.

- performance of a task carried out in the public interest
- exercise of official authority
- balance of interests (note that this basis cannot be used in the authority’s principal area of activity).

The lawful grounds used for personal data processing carried out at Uppsala University will primarily be consent, task of public interest and exercise of official authority.