Consent and the General Data Protection Regulation (GDPR)

The introduction of the General Data Protection Regulation (GDPR), which came into force on 25 May 2018, imposes higher requirements for the processing of personal data. One of the requirements is that all processing must have a lawful basis. Before the organisation can process personal data, a lawful basis must be established for the processing. This requirement is widely misunderstood, as many people believe consent will be required for all processing of personal data. This is not correct, as there are many other bases to justify personal data processing.

As a rule, consent should always be considered last of all lawful bases, since it will require a positive action on the part of the individual, it can be withdrawn at any time and there must not be a significant power imbalance between the parties (as, for example, between an employer and an employee). It is important to only use consent as the lawful basis in situations where this is really necessary. Using the wrong lawful basis, such as consent, may mean that the processing becomes unlawful.

Here you can read about what you need to think about when you intend to process personal data using consent as the legal basis. However, merely having the consent of the data subject for the processing is not enough. You also need to consider how you obtain consent and how to formulate your request for consent.

Consent as a lawful basis

Personal data may be processed if there is a lawful/legal basis for doing so. Consent is one of the six lawful bases listed in the GDPR. The applicable legislation imposes special requirements for consent. Among other things, it must be freely given, it must be given by a statement or a clear affirmative action (which demands ticking a box, choosing technical settings or some other conduct that clearly indicates consent), and it must be given after the data subject has received information about the personal data processing. The lawful basis must be determined before the processing of personal data begins.

In addition, particularly strict requirements apply when consent refers to the processing of sensitive personal data, such as health data. Anyone processing personal data on the basis of consent must be able to show that the data subject has given valid consent.

Conditions for consent

When processing is based on consent, the controller must be able to show that the data subject has consented to the processing of their personal data. If the data subject is to give their consent in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of the GDPR is not binding.

Data subjects have the right to withdraw their consent at any time. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal. Before giving consent, the data subject must be informed of this. It must be as easy to withdraw as to give consent.

Processing of sensitive (special categories of) personal data

Some personal data are, by their nature, more sensitive than others. The GDPR treats the following special categories of personal data as requiring special legal protection. These categories are:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- membership of a trade union
- health
- a person's sex life or sexual orientation
- genetic data and biometric data that uniquely identify a person.

Uppsala University must only process sensitive personal data when there is special support for doing so in legislation, or if the data subject has specifically consented to the specific processing operation.

Informed, freely given, specific and unambiguous indication of the data subject's wishes (positive action)

Consent must be given by a positive action establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to them, such as by a written statement, including by electronic means, or an oral statement.

This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence, pre-ticked boxes or inactivity can therefore not constitute consent.

Consent covers all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Informed

For consent to be 'informed', a person must have received access to sufficient information about what they are consenting to before giving their consent.

'Sufficient information' means that you must provide information about what types of data you are processing, what the purpose of your processing is, how long the consent will remain valid, who will receive the personal data, whether the personal data will be transferred to a third country[1], the identity of the controller[2] and how the person can contact the University's data protection officer, the fact that the person has the right to withdraw their consent at any

[1] A country outside the EU/EEA.

[2] The controller for processing activities at Uppsala University is the University in its capacity as legal person, unless another legal person is controller and Uppsala University is processor. Read more about how this is determined on the GDPR page. The controller is in any case *not* the individual researcher/doctoral student/student etc.

time and the right to request rectification, data portability, erasure or restriction of the personal data you process.

Freely given

For consent to be 'freely given', the person giving their consent must have a real opportunity to say no without being adversely affected. A person must be able to choose not to consent and to withdraw their consent once given without problematic consequences. If the requirement of freely given consent is not met, you should consider whether another legal basis is applicable.

If there is an imbalance in the power relations between the person who is to give their consent and the controller, this may mean that consent is not freely given. Such imbalances can occur, for example, in employment relationships or in relations between an individual and a public authority. In some cases, services or agreements that depend on consent cannot be considered to meet the requirement of freely given consent. In that case, there are other lawful bases on which you can base your processing. To read more about this, see the document on lawful bases on the GDPR page.

To give another example, 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.[3] This is also the reason why Uppsala University as a public authority will so rarely use consent as the lawful basis for personal data processing. It is difficult for a public authority not to have individuals in a dependent position, which means that it is difficult to obtain freely given consent. Furthermore, non-negotiable conditions and requirements cannot be attached to consent if it is to be regarded as freely given, and data subjects must not be affected by adverse consequences, such as extra charges, if they do not consent.[4]

Specific

For consent to be 'specific', you have to clearly explain what you seek to achieve by processing personal data. The simplest way to explain this is to state the purpose of the personal data processing. If the processing has many different purposes, it is important to ensure that the data subject is able to distinguish between the different purposes and to consent (or choose not to consent) to the different parts separately.[5] This does not mean that it is impossible for a person to consent to different processing operations at the same time.

For example, the data subject can consent to collection, storage and adaptation of their personal data at the same time, as long as the purpose of all the processing operations is the same (e.g. to compile a contact list). In contrast, if you are asked to consent to a contact list

---

[3] 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.

[4] Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679, p 6.

[5] Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679, p 11.

and also to consent to the use of your personal data for marketing purposes, this is a matter of different purposes and the data subject then needs to consent to them separately.

A further requirement is that the information relating to consent is separate from other information that the controller wishes to present to the data subject. Even if you have a great deal of information to give the data subject, you should avoid texts and bodies of information that by their excessive length and bulk may make it difficult for the data subject to take in the most important information.

It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

Positive action (unambiguous indication of wishes)

Consent must be given by a positive action. This means that the person whose consent is needed for processing must actively consent to processing. Providing a pre-ticked box with the text “I consent”, or a box for “yes” that is already filled in, can *not* be regarded as obtaining unambiguous consent. For the consent to be lawful, the person concerned must personally actively click the box. This means that an ‘opt-out’ clause is not permitted. One way to perform a clear affirmative action is to make an active choice of technical settings.

Consent to processing from a minor

A person giving their consent must be able to understand the meaning of consent. When it comes to information society services provided to children, such as search engines, online activities and other internet services, the child must be 13 years old in order to consent to the processing of their own personal data. If the child is under the age of 13, the consent of the holder of parental responsibility over the child is required. For personal data processing in other cases, i.e. in cases other than information society services provided to children, an assessment must be made of the child’s ability to understand what is being done. Such an assessment must be made in each individual case. It is important to remember that it is the person processing data on the basis of consent who bears the burden of proving that the consent meets the GDPR requirements.

Withdrawal and burden of proof

If you consider that consent is the relevant legal basis, you must bear in mind that data subjects have the right to withdraw their consent. Note that if you take the view that a data subject cannot withdraw their consent, you should consider whether the requirement of freely given consent is really satisfied. However, a withdrawal of consent does not mean that the processing you have performed up until the withdrawal is unlawful. It is only future processing that would be unlawful. You bear the burden of proving whether or not valid consent exists. It is therefore important that internal procedures/systems are in place that make it possible to document that such consent exists. One way to demonstrate that consent exists is to use Uppsala University’s internal systems that enable you to store the text and the positive action of the person who has given their consent.

An example in the area of research:

If a person who has given a sample completely withdraws their consent, that person's samples and data can no longer be used in new research. The researcher marks the records to ensure that samples and data can no longer be used. However, research results obtained using the samples and data before the communication withdrawing consent was received may be used to a limited extent, together with associated data and material created on the basis of these data. Other legislation may require the material to be saved so as to be able later to demonstrate the accuracy of the scientific research results or to monitor the quality of any products deriving from the processing activities.