24 May 2018

The General Data Protection Regulation – basic principles

On 25 May 2018, the Swedish Personal Data Act will be replaced by the European Union's **General Data Protection Regulation (GDPR)**.[1] The GDPR imposes higher requirements for the processing of personal data and the penalties for infringements are considerably tougher than in the current regulations. This means that if Uppsala University fails to comply with the basic principles of the GDPR when processing personal data, such infringements, in certain circumstances, could result in higher administrative fines being imposed.

In the sections below, you will find information about the principles that apply and that must be respected in all personal data processing activities. Always keep them in mind when handling personal data, for your guidance.

Principles

In addition to having at least one lawful basis, all processing of personal data must comply with the fundamental principles specified in the GDPR. These principles entail, among other things, that personal data may only be collected for legitimate purposes that are not described in too general a way and that 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. Any actor processing personal data must be able to show that they are complying with the principles. The principles must be observed in all processing. Any actor processing personal data must therefore have procedures for ensuring compliance with the principles.

The six basic principles are:

- the principle of lawfulness, fairness and transparency
- the principle of purpose limitation
- the principle of data minimisation
- the principle of accuracy
- the principle of storage limitation, and
- the principle of integrity and confidentiality.

Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

The requirement that the personal data processing be **lawful** means, among other things, that the processing must have a legal basis.

The requirement of **fairness** assumes that the data subjects know about the processing, i.e. that they are informed in accordance with the GDPR rules. Fairness could also mean that you are not allowed to use covert arrangements to collect data without the data subject being aware of it, e.g. wire tapping or developing and using secret processing methods.

The requirement of **transparency** means, among other things, that it must be clear and transparent to data subjects how their personal data are collected and processed. Data subjects must therefore receive information about the processing, for example, after requesting an extract from records they must receive the information in an easily accessible form and formulated in clear and plain language.

Purpose limitation

The GDPR prescribes that all personal data collected must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. It is the purposes determined in advance that set the limits for the processing. They must be explicit and legitimate and determined at the time of the collection of the personal data. It is not possible to postpone the determination of the purpose until a later time, nor can a purpose be added afterwards.

The purposes must be documented in writing and the data subject must receive information about the purposes when the data are collected and whenever the data subject otherwise asks for it. If, at a later point, the intention arises to process the personal data collected for other purposes that are compatible with the original purposes, the data subjects must also be informed of this. The personal data collected may be processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes without it being considered incompatible with the original purposes, provided that the rights of data subjects are protected by appropriate safeguards.

In some cases, the purposes may be given in legislation, and if so, the controller has to comply with those regulations. Whether the purposes have been determined by statute or not, however, it is always the controller that is responsible for ensuring, and being able to demonstrate, compliance with the basic principles. It is the controller that is responsible for ensuring that the processing is only done for the specified purposes. In the event of a dispute, the controller bears the burden of proof, since it is the controller that principally determines the purposes.

Data minimisation

The principle of data minimisation means that the personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In other words, you are not allowed to collect personal data for indeterminate future needs. Further, personal data collected may not be processed if, for instance, they are so old that they are no longer relevant to the original purposes.

The principle that the personal data must be limited to what is necessary in relation to the purposes for which they are processed means that you must not hold excessive amounts of personal data. This requires, in particular, ensuring that the period for which the personal data

are stored is limited to a strict minimum. Do not collect more or less personal data than you really need in relation to the purposes of the processing, and do not collect irrelevant data. A useful guideline could be that you must be able to explain why the various pieces of data are needed to achieve the purposes of the processing.

One practical implication of this is that a controller using free text fields online for some particular purpose should give written instructions on the type of information that is relevant to provide in the field. In order to ensure that the personal data are not kept longer than necessary, Uppsala University has time limits for erasure and for periodic review.

Accuracy

Personal data must be accurate and up to date. Any actor processing personal data must take every reasonable step to ensure that inaccurate personal data are erased or rectified without delay. If necessary for the purposes, the personal data must also be kept up to date. This means that the controller needs to actively ensure the quality of the personal data and must not wait to act until the data subject uses their right to rectification of inaccurate personal data. The circumstances in the individual case must be considered. The relevant factors could include the purposes of the processing, the amounts of personal data processed and the potential consequences of inaccurate data for the data subject. Whether it is necessary to keep the data up to date should be decided with reference to the purposes of the processing.

Storage limitation

Personal data may not be stored, i.e. kept in a form which permits identification of data subjects, any longer than is necessary for the purposes for which the personal data are processed. When the personal data are no longer needed for these purposes, they must be erased or anonymised. In order to ensure that the personal data are not kept longer than necessary, any actor processing personal data should establish time limits and procedures for erasure or anonymisation.

The personal data collected may be stored for a longer period for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, provided that the rights of data subjects are protected by appropriate safeguards.

The GDPR also requires the controller to provide information to data subjects about the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. This applies regardless of whether the personal data come from the data subjects themselves or not, i.e. whether they have been obtained from some other party. The same information must also be provided if the data subject requests an extract from records.

Integrity and confidentiality

Personal data must be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Actors processing personal data must therefore take appropriate technical and organisational measures to protect the personal data. Personal data must therefore be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

In this context, integrity is a security principle meaning that personal data are not changed or destroyed by mistake, either by an unauthorised person or by the process. Confidentiality is also a security principle meaning that information is not made available or disclosed to an unauthorised person or process. Both concepts are part of general information security.

Accountability

Actors processing personal data are responsible for compliance with the principles of personal data processing and must be able to demonstrate how they are being complied with. There are several ways of demonstrating this, for example, by providing clear information to data subjects, documenting the processing operations performed at the organisation and the considerations taken, and having documented internal guidelines for data protection (a data protection policy). The data protection officer verifies the organisation’s compliance with the GDPR and the internal guidelines, and this is also a way of satisfying the requirement of accountability.