What is most important to remember?
• always ensure the processing of personal data is lawful
• do not process personal data other than strictly when necessary
• collect personal data only for specified and explicit purposes
• keep personal data no longer than is necessary
• in the event of a request from a data subject, access to personal data related to the data subject shall be provided

What is personal data?
Personal data is any information relating to an identifiable natural person. Typical examples are name, address and personal identity number. Even photographs are personal data in cases where a person in the photograph is identifiable. A car’s registration number may be personal data if the information about the car links to a specific person.

Special categories of personal data
The General Data Protection Regulation (GDPR) differentiates between personal data and special categories of personal data, which includes:
• racial or ethnic origin,
• political opinions,
• religious or philosophical beliefs,
• trade union membership,
• information concerning health, sex life or sexual orientation, and
• genetic or biometric data used to uniquely identify a natural person.

The main principle of the regulation prohibits the processing of special categories of personal data. There are, however, some exceptions to this principle such as if the data subject has given his or her explicit consent to the processing of data. Special categories of personal data are considered to be at greater risk than other personal data and thus require greater protection.
What is processing of personal data?

Processing is more or less any operation performed on personal data, such as collection, recording, storage, alteration, correcting, erasure or transmission of data. GDPR governs all processing of personal data regardless of whether the processing of data is by automated means or not.

To process personal data you must have a lawful reason…

To be able to process personal data you must have a lawful reason for doing so. For the university to fulfil its function, at least one of the following should apply:

- **Public interest or exercise of official authority** – the university has to follow a number of different laws, such as the Higher Education Act and the Higher Education Ordinance. Based on these laws, we have the right to process personal data concerning our students and our employees.

- **Legal obligation** – the university also has other legal obligations, such as providing employees’ salary details to the Tax Agency, and thus have the right to process personal data for this purpose.

- **Contracts** – the university has the right to process information about a data subject in order to fulfil a contractual obligation to the data subject.

- **Consent** – explicit consent given by a data subject allows the university to process personal data.

…and you must follow the basic principles

GDPR lists a number of basic principles always to be adhered:

- Processing of personal data shall be lawful, fair and in a transparent manner in relation to data subject.
- Collection of personal data shall only be for specified, explicit and legitimate purposes.
- Personal data shall be relevant and limited to what is necessary in relation to the purpose.
- Personal data shall be accurate and kept up to date.
- Storage of personal data shall not be for longer than is necessary.
- Apply appropriate protection when processing personal data.
- The controller (i.e. the university) is responsible for ensuring, and being able to demonstrate, compliance with the above principles.

Note that certain information is subject to the principle of public access to official records and therefore must be preserved in accordance with the Archive Act.
Security and register requirements

Process personal data with sufficient security measures to avoid theft or unintended erasure or alteration. For this reason, it is imperative only to use tools and storage locations approved by the university. As controller, the university is obliged to be able to demonstrate compliance to the regulation. In order to control processing of personal data, the university must maintain a record of processing activities. Among other things, this record shall contain a description of the categories of personal data that is processed, purpose of the processing, and contact details to the employee responsible. This may be a head of department or director of research, for example.

Inform the data subject

One key purpose of GDPR is to afford individuals greater control of their personal data. In the case of personal data being processed, the data subject has the right to be informed of the processing, what data is being processed and for what purpose. The information shall be concise, using clear and plain language and be easily accessible.

Data subjects has the right to request access to their personal data and can, under certain circumstances, request erasure of personal data. This must, however, be considered in the light of other applicable legislation that may require personal data to be preserved. A student, for example, cannot request erasure of personal data from Ladok.
What is new in the General Data Protection Regulation?

The main differences between the GDPR and previous legislation are:

• the university must have a Data Protection Officer
• data subject rights are strengthened by additional privileges such as being informed and allowed correction, erasure and transfer of personal data
• data processors, i.e. third parties who process personal data on behalf of the university, have defined responsibility and accountability
• fines may be levied organisations that do not comply with the GDPR

Learn more about how the university process personal data at gu.se/personuppgifter