Processing personal data at the University of Gothenburg

Illustrations: Dolling Tahko
Personal data at the University of Gothenburg

The University process personal data of

- **Students** (for example in Ladok)
- **Staff** (for example in Agresso and Primula)
- **Other data subjects** (for example research subjects, alumni, business partners and conference guests)

From May 25th 2018, the processing of personal data is governed by a new legislation.
The aim of the General Data Protection Regulation is to

• create a uniform regulatory framework and facilitate the free flow of personal data within the EU/EEA

• protect the personal integrity of the individual

The General Data Protection Regulation (GDPR) is an EU regulation, which means that the rules will apply directly and in the same manner in all EU member states.

General Data Protection Regulation (GDPR) = Allmän dataskyddsförordning (DSF) in Swedish
In Sweden, GDPR will replace

• the Data Protective Directive (95/46/EG)
• the Data Protection Act (1998:204)
• the Personal Data Ordinance (1998:1191)
• regulations from the Swedish Data Protection Authority

GDPR also allows certain national departures. In Sweden, GDPR is complemented with other legislation.
What is new in the GDPR?

Basically all requirements in the Data Protection Act are still valid for the GDPR, and a lot of the information in this presentation is therefore not new.

If you are familiar with these requirements, you have a head start!

However, there are some additional rules included in the GDPR.
Changes in the GDPR include

• extended rights for data subjects (the individuals whose personal data is being processed)
• the university must have a Data Protection Officer
• data processors (third parties who process personal data on behalf of the university) have defined responsibility and accountability
• fines may be levied on the university if we do not comply with the GDPR
## Important roles defined by the GDPR

<table>
<thead>
<tr>
<th>Role</th>
<th>which means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller</td>
<td>responsible official authority, institution or body, in our case the university</td>
</tr>
<tr>
<td>Data Protection Officer</td>
<td>role at the university who verifies that we process personal data correctly according to GDPR</td>
</tr>
<tr>
<td>Processors</td>
<td>other parties who process personal data on behalf of the university, such as Statens Servicecenter</td>
</tr>
<tr>
<td>Regulator</td>
<td>The Swedish Data Protection Authority (Datainspektionen)</td>
</tr>
<tr>
<td>Data Subject</td>
<td>the individual whose data is being processed</td>
</tr>
</tbody>
</table>
What is personal data?
Personal data is any information related to a natural person that can be used, **directly** or **indirectly**, to identify that person. Examples are:

- name
- identification numbers (such as personal identity numbers)
- email address
- postal address
- photographs and video recordings
- hair colour
- online identifiers, such as location data via mobile phones

The important issue is whether or not data can be linked to a person. Hair colour do not constitute personal data unless it can be used with other data to identify someone.
Sometimes multiple data is required to be able to identify someone:

- Woman who is Vice-Chancellor of a Swedish university
- Eva Wiberg, 158 people found on Eniro
- Eva Wiberg, Vice-Chancellor of the University of Gothenburg
Special categories of personal data

This includes data concerning:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs

- trade union membership
- health, sex life or sexual orientation
- genetic or biometrical data

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.
Personal identity numbers and other identification numbers can only be processed in the following cases:

A. Consent from the data subject

B. Without consent if the processing is necessary for:
   1. the purpose of the processing
   2. the need for a secure identification, or
   3. some other considerable reason
What is processing of personal data?
Processing of personal data includes...

- collection
- organisation and storage
- reading and use
- alteration and correcting
- transmission
- erasure and destruction

…and any other operation that can be done on personal data.
For example, when a co-worker at the university...

• administers examination of students

• administers employment

• collects personal information from participants in a public event

• collect research data consisting of personal data – either directly from the data subject or from another source

…he or she is processing personal data.
Lawful processing of personal data

For processing of personal data you must:

• follow the basic principles (article 5 in GDPR)

• have a lawful basis for the processing (article 6 in GDPR)
The basic principles for processing includes

- **lawfulness, fairness and transparency** – processing of personal data shall be lawful, fair and in a transparent manner in relation to the data subject

- **purpose limitation** – collection of personal data shall only be for specified, explicit and legitimate purposes

- **data minimisation** – personal data shall be relevant, adequate and limited to what is necessary in relation to the purpose

- **accuracy** – personal data shall be accurate and kept up to date

- **storage limitation** – storage of personal data shall not be for longer than is necessary

- **integrity and confidentiality** – apply appropriate protection when processing personal data
Lawful reasons for processing

Personal data may not be processed unless at least one lawful basis apply to do so:

• **consent** – from the data subject

• **public interest or official authority** – exercising a task carried out in the public interest or in the exercise of official authority

• **contract** – entering or fulfilling a contractual obligation to the data subject

• **legal obligation** – fulfilling a legal obligation

• **vital interests** – protecting interests of the data subject

• **legitimate interests**
## Legal bases that are most useful at the university

<table>
<thead>
<tr>
<th>Legal basis:</th>
<th>Meaning:</th>
<th>Examples from the university:</th>
</tr>
</thead>
</table>
| Consent                       | • voluntarily  
• informed  
• documented                      | research  
external collaboration and marketing          |
| Contract                      | to fulfil a contract with a data subject     | employment contracts  
collaboration contracts  
purchasing contracts         |
| Legal obligation              | to follow rules and regulation               | LADOK ordinance  
Archives Act  
Work Environment Act         |
| Task of public interest       | on behalf of the Swedish Government or Parliament | education  
research  
external collaboration         |
| Exercise of public authority  | necessary for the exercise of public authority | examination  
disciplinary matters           |
Regulations concerning consent

To be able to use consent as a legal basis the following must be fulfilled:

• the consent must be voluntary and individual
• it has to be given for a specific process
• it has to be given freely and in a unambiguous manner
• the data subject has the right to get clear and concise information about the purpose of the processing
• the data subject has the right to withdraw his or her consent at any time
The rights of the data subject
The rights of the data subjects include

- access to his or her personal data (transcript)
- correction or completion of incorrect personal data
- erasure of personal data – provided that the data is no longer needed for the specified purpose or is to be archived in accordance with other legislation
- the right to transfer personal data to another (so-called data portability)
- the right to object to the processing of personal data
- receive clear and concise information about the processing of personal data
Information to the data subject

Information submitted to the data subject regarding the processing of his or her personal data should be concise and easy to understand.

The information provided must include:

• what kind of data that is processed
• for what purpose it is processed and on what legal basis
• if the data is to be transferred to a country outside of the EU/EEA
• the Data Protection Officer’s contact details
Safety requirements for personal data
Record of processing activities

As a controller, the university must maintain a record of all processing of personal data within our operations. The record must include:

• the purpose of the processing
• a description of categories of data subjects and personal data
• any transferral of personal data and whether it will be moved outside of the EU/EEA
• contact details to the employee responsible, for example the head of department or the director of research
Keep personal data safe!

It is of great importance to process personal data with adequate security measures to avoid theft, erasure or alteration.

If you process personal data in your work, you need to keep the following in mind:

• stay updated on our policies and guidelines
• only use tools approved by the university
• safety routines – use secure passwords, log out from your computer when leaving it and do not leave mobile units unattended
Incidents must be reported

If the university loses control over personal data, this must be reported to the Swedish Data Protection Authority.

Examples of incidents that must be reported are:

• theft of information
• accidental loss of information
• hacking incidents
• unauthorized access to personal data
Finally: the most important points to keep in mind!
Always follow the basic principles

• do not process more personal data than necessary
• only collect personal data for specific and predefined purposes
• do not keep personal data for longer than necessary
Make sure to have a legal basis for the processing

• consent from the data subject
• to perform duties of general interest or in connection with the exercise of authority
• entering into or fulfilling a contractual obligation with the data subject
• fulfilling a legal obligation
• protecting vital interests of the data subject
• legitimate interests
This is coming

- More information, policies and instructions will be found at [www.medarbetarportalen.gu.se/dataskydd](http://www.medarbetarportalen.gu.se/dataskydd)

- A support organisation for the processing of personal data will be formed. The intended organisation consists of the Data Protection Officer, a data protection group, and contact persons at the faculties

- Training and information relating to different aspects of personal data processing
Who to contact for questions?

Contact the Data Protection Officer at dataskydd@gu.se