To those who intend to use the slideshow for a presentation

About the slideshow

- Originally produced by the personal data management project (reg. no STYR 2016/1173)
- The aim is to help employees communicate the content of the upcoming data protection regulation and what it means for Lund University.
- The slideshow contains many slides. It is important that you make a selection based on your presentation. To facilitate, we have labelled the slides as follows:
  - General – information which will benefit everyone
  - Discussion – non-essential information, intended to promote discussion
  - Supplementary – probably most suitable for in-depth discussions if you have plenty of time
  - Focused – select the example/s that are most relevant to your target group
- Some slides have notes that explain or exemplify the content, or include discussion points.

Parts

- Part 1: Focuses on general information about the new regulation, complemented by examples related to universities.
- Part 2: Requires an understanding of the content in Part 1. It has an IT and information security perspective, and is mainly intended for employees who are responsible for various IT systems containing personal data.
- Part 3: Explains the project in brief

Disclaimer

- As the General Data Protection Regulation is not yet in effect, some of the information is still uncertain.
- New versions of the slideshow may be published on: http://personuppgifter.blogg.lu.se/pagende-aktiviteter/kommunikationsfragor/

Feedback

- If you have any suggestions for improvements, please contact the project communications officer Jonas.Wisbrant@cs.lth.se.
Introduction to the General Data Protection Regulation

VERSION DECEMBER 2017
Dear Lund University,

My name is *****.

I would like to know what information you have on me...

... Thanks! Could you please delete it?
Content

Part 1: About the GDPR
- Grounds, summary and consequences

General concepts
- Personal data
- Processing of personal data
- Legal basis
- Rights of the data subject
- Information to data subjects
- Documented consent

Part 2: IT perspective
- Responsibilities and roles in the organisation
- Technology
  - Where does the information come from?
  - Information exchange between different systems
  - IT system authorisation
- Managing the rights of data subjects
- Information to data subjects
Cause and effect

General Data Protection Regulation (GDPR) = Dataskyddsförordningen (DSF)
- Valid from 25 May 2018
- Applies to organisations – not private individuals

Aims
• Protect the right to privacy
• Facilitate the free flow of personal data within the EU (but not outside)

Consequences
• We must know what we may and may not do
• Clearer and more information to data subjects
• Stringent and documented organisation
Quiz:
What’s the worst that can happen on 26 May 2017?

1. Heavy administrative workload to ensure the rights of the data subjects…

X. SEK 20 million in fines…

2. Serious criticism from investigative journalism…

3. We cause trouble for a data subject…
Summary
How data is to be processed – in brief

Today
- Data may be processed for certain explicitly stated and legitimate purposes
- The processing of data must be correct and transparent towards the data subject

Principles as of 25 May 2018
- **Data minimisation** – processing of personal data shall be limited to what is necessary
- **Storage limitation** – personal data shall no be stored longer than necessary
- More emphasis on **data integrity** and confidentiality
- **Accountability** – we must be able to demonstrate compliance with the rules
- Transferring of data to a **third country** requires explicit support from the regulation

Your personal right to
- information about when and why your personal data are processed
- prompt **correction** of errors
- to be **forgotten**
- **data portability**
- information regarding **incidents** involving personal data
- decline **automated decisions**
Context: **Data protection officer and list of all personal data processing**

The university is to:

- show the Data Protection Authority our compliance with the regulation
- ensure that we are able to fulfil the data subjects’ rights
- keep a list of all processing of personal data

**6 high-level strategies run by the project as far as possible**

- Major PM3 systems ➔ Administration plans describing the system in relation to the GDPR
- Training for ALL staff and ALL students
- Coordinated organisation for advice and support
- Standardised information to the major data subject groups
- Register of personal data processing that links organisation ➔ legal basis ➔ IT system
- Procedures for managing the rights of data subjects
General Data Protection Regulation – key concepts

NOVEMBER 2017
Personal data – what are they?

“any information relating to an identified or identifiable natural person”*

Name, photo, address, genome, email, description, grades, age, personal identity number…

… hair colour, shoe size, personality, expertise…

We MAY and SHALL process large amounts of personal data

Cats, fictitious or deceased persons do not have rights under the GDPR

* Source: GDPR article 4.1
## Special categories (sensitive) of personal data

<table>
<thead>
<tr>
<th>Information revealing</th>
<th>as well as</th>
</tr>
</thead>
<tbody>
<tr>
<td>• race</td>
<td>• genetic data</td>
</tr>
<tr>
<td>• ethnicity</td>
<td>• biometric data which uniquely identifies a natural person</td>
</tr>
<tr>
<td>• political opinions</td>
<td>• health data</td>
</tr>
<tr>
<td>• religious belief</td>
<td>• information concerning a natural person’s sex life</td>
</tr>
<tr>
<td>• philosophical belief</td>
<td>• information concerning a natural person’s sexual orientation</td>
</tr>
<tr>
<td>• trade union membership</td>
<td>• personal data concerning criminal convictions and offenses</td>
</tr>
</tbody>
</table>

* personal identity number*  

... must NOT be processed at the outset!

* Personal identity number is not mentioned in the GDPR/DSF – but it has the same status
Personal data processing, pursuant to the GDPR

- Collection
- Recording
- Organisation
- Structuring
- Storage
- Adaptation or alteration
- Retrieval
- Consultation

- Use
- Disclosure by transmission, dissemination or otherwise making available
- Alignment or combination
- Restriction
- Erasure or destruction
Personal data in unstructured material – in emails, local registers and online

Personal data in unstructured material cease to be an exception.

➤ We need ensure a legal basis and information for e.g. information and marketing purposes...

• symbolic photos and event photos
• text, news and calendars
• social media
Legal basis for processing personal data

<table>
<thead>
<tr>
<th>Legal basis</th>
<th>Meaning</th>
<th>At the University</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal obligation</td>
<td>Required by other legislation</td>
<td>LADOK ordinance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Archives Act</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Work Environment Act</td>
</tr>
<tr>
<td>Exercise of public authority</td>
<td>Necessary for the exercise of public authority</td>
<td>Grades</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disciplinary cases</td>
</tr>
<tr>
<td>Task of public interest</td>
<td>On behalf of the Swedish Government or Parliament</td>
<td>Education</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Research</td>
</tr>
<tr>
<td></td>
<td></td>
<td>External engagement</td>
</tr>
<tr>
<td>Agreement</td>
<td>To perform a contract with a data subject</td>
<td>Cooperation agreement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Purchasing agreement</td>
</tr>
<tr>
<td>Consent</td>
<td>• Voluntary</td>
<td>Research</td>
</tr>
<tr>
<td></td>
<td>• Informed</td>
<td>Collaboration and communication</td>
</tr>
<tr>
<td></td>
<td>• Documented</td>
<td>Certain sensitive data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other interests</td>
</tr>
<tr>
<td>Following legitimate interests</td>
<td>- - - -</td>
<td>Cannot be exercised by a public authority</td>
</tr>
<tr>
<td>Protection of basic interests</td>
<td>Security policy</td>
<td>E.g. when in collaboration with the Armed Forces</td>
</tr>
</tbody>
</table>
## Legal basis:
Examples of why we may do what we do

<table>
<thead>
<tr>
<th>Purpose of activity</th>
<th>Legal basis</th>
<th>Consequences</th>
</tr>
</thead>
</table>
| Recruiting students to our study programmes and courses | Consent          | - Information depending on the situation  
|                     |                              | - Document consent  
|                     |                              | - Process for withdrawing consent |
| Admission of students | Public interest | **- LU-wide standard information**                             |
| Enrolment of students | Public interest     | - Standard information applies  
|                     | + possibly consent | - E-course for all students  
|                     |                              | + possibly documentation of consent |
| Implementing courses | Public interest     | Standard information applies  
|                     | + possibly consent | + any addition to the standard information  
|                     |                              | + consent in case of any addition** |
| Assessing student performance | Exercise of public authority | Standard information applies |
Processing → legal basis → consequences

Example: Attract and recruit students

- **Processing**
  Attract students externally to study programmes and courses

- **Legal basis**
  Consent

- **Tools**
  - Online form
  - Mailing lists
  - Email
  - List of participants

- **Examples**
  Notices of interest, catalogue mailings, lists of participants and event registrations...

- **Consequence**
  Unique information to the people concerned
  Document consent
  Process for withdrawing consent

GDPR project

Defines 40–50 activities/purposes

Links them to legal grounds

Identifies the systems concerned

Draws conclusions based on the legal grounds
## Rights of data subjects

<table>
<thead>
<tr>
<th>Right to...</th>
<th>Meaning</th>
<th>Conflict</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>Information about the processing of personal data when they are collected and, on request, any incidents</td>
<td>Information security</td>
</tr>
<tr>
<td>Rectification</td>
<td>Have erroneous data corrected and supplemented</td>
<td>Archiving?</td>
</tr>
</tbody>
</table>
| Erasure                         | When the data is not needed
Withdrawn consent
If there are no legitimate ground, for the exercise of public authority, etc. | Archiving
Documented exercise of public authority                                |
| Restiction of processing        | Marked for limited processing – even during investigation                | -                                                                        |
| Data portability                | For consent (not research studies) and agreements                        | -                                                                        |
| Making objections               | Exercise of public authority and information of public interest          | -                                                                        |
| Avoiding automated decision-making and profiling | Admission[^1]                                                        | -                                                                        |

[^1]: UHR is probably responsible for the personal data in the admissions process until the universities take over the communication with the admitted students.
Information to the data subjects

When importing data from other systems:
- NyA → LADOK → Kuben → other local systems

When collecting data from the data subject:
- enrolment of students (already done*)
- recruitment of students
- public events
- research involving personal data

Standard information or templates drawn up for
- new students
- new staff
- research studies
- communication and collaboration
Do more legal obligations result in information management with embedded conflicts?
What to do now?

Read FAQs etc. on personuppgifter.blogg.lu.se

and subscribe...