The Data Protection Regulation for Heads of Department and Administrative Managers

May 24 2018
The Data Protection Regulation replaces the Personal Data Act

May 25, 2018 the new EU regulation for personal data, the General Data Protection Regulation (GDPR) comes into force. The new regulations will entail stricter regulations, severely increased sanction fees for authorities, of SEK 5-10 million, as well as increased compliance control. In other words, the requirements on the University activities will be even higher.

As a manager, you are responsible for the GDPR compliance

From May 25, the compliance responsibility rests on each manager, e.g. including contacting the University’s Data Protection Officer, before changes as well as the introduction of new systems/new research. This may also include current activities for processing personal data, that will be changed in some manner.

READ MORE
The University’s decision and delegation order can be found in the Rules & Regulations
Ny EU-förordning på gång

• The General Data Protection Regulation will come into effect in Sweden May 25.
• The Personal Data Act will be revoked, but since there are national laws referring to the Personal Data Act, it will remain in force for these purposes.

What does this entail?
Processing concluded before May 25, 2018
• The Personal Data Act applies
• Not GDPR
Processing started after May 25, 2018
• GDPR applies
Processing started before May 25, 2018 and thereafter continuing
• GDPR applies
• Not the Personal Data Act

The purpose of GDPR
• To protect the fundamental rights and freedoms of individuals, in particular their right to protection of personal information.
• To create a common and equal level for the protection of personal information within the EU, so the free flow of information within the Union will not be hindered

Personal data
Personal data means any information relating to a natural person.

Sensitive personal data
Sensitive personal data refers to information regarding:
• Race or ethnic origin
• Political views
• Religious or philosophic conviction
• Trade union membership
• Health
• A person’s sex life or sexual orientation

Genetic or biometric data unambiguously identifying a person. Genetic data means personal data relating to the inherited or acquired genetic characteristics which may be concluded, for example through DNA analysis. Biometric data means personal data relating to the physical, physiological or behavioural characteristics of a person, resulting from specific technical processing, for example fingerprint data.
The most important changes in the new EU Data Protection Regulation

- The protection level for personal data is generally increased
- The obligation to inform the registered is extended
- Higher requirements for IT security
- Clearly stated consent and how to recall the consent. Higher learning institutions, which are authorities, must put careful consideration on consent as a legal base. by fulfilling requirements on voluntary participation and purpose qualification.

Personal data processing

Examples of personal data processing:
Registration, organisation, structuring, storage, processing or changing, access, reading, usage; handing out through transfer, distribution, or making available in other ways; adjusting or combining, limiting, erasing, or destruction.

Legal base for personal data processing
1. Consent
2. Fulfilling agreements, e.g. employment agreements
3. Fulfilling legal requirements, e.g. the Accounting Act
4. General interest - if something is necessary for carrying out a task of general interest.
5. Exercising powers as a public authority - work in connection to research or exercising powers as a public authority must be carried out.
6. Protection of fundamental interests, e.g. vital care.

Other
Interest adjustment - not for authorities. The violation rule is revoked.

READ MORE
At the Swedish Data Protection Authority’s web site datainspektionen.se, you will find more information about GDPR. At su.se/gdpr, you will find collected information (in Swedish) about SUs work with GDPR.
Consent must meet certain requirements, (Art. 7)

Voluntary; If there is a compelling part, further consent must be given for the non-compelling part. When being employed, the employee has no real opportunity to deny consent, wherefore consent in employment agreements have very limited value.

In particular: A clearly stated purpose - you must state in what way you are going to use the information. A consent from an employee concerning “information, that the employer needs for their activities”, is not valid.

Informed: Clear information, it must never be a part of general terms. If the personal data is processed by a Processor in a country, where an appropriate level of protection for processing personal data cannot be guaranteed, and if the registered are not informed about this, their consent may not be valid.

Other
- The responsibility of the organisation is to be able to show that consent is given before the processing begins.
- A function for recalling consent must be in place.

Severe consequences for not adhering to the regulations
The consequences for not adhering to the regulations may be huge. The sanction fees may be 5-10 million SEK for public authorities.

Data Protection Officer
The comprehensive and most important task for the Data Protection Officer is to supervise that the organisation adheres to the Data Protection Regulation. It means, e.g. to collect information regarding how the organisation processes personal data, control of the organisation’s adherence to rules and regulations, and the internal control documents, as well as internal information and advisory tasks within the organisation.

The Data Protection Officer shall also give advice regarding consequence assessment, function as a contact to the Swedish Data Protection Authority, function as a contact to the registered, and the staff within the organisation, as well as cooperating with the Swedish Data Protection Authority, e.g. during inspections. Contact the Data Protection Officer at e-mail dso@su.se, if you have any questions or want to report a personal data breach.
GDPR and Research

The Research Data Committee

Processing of personal data for research purposes (SOU 2017:50)

Complementing national legislation is required to avoid cessation of certain types of research.
- Legal base: consent/public interest
- Public/private actors
- Ethical review as a special protective measure
- Other protective measures, (e.g. pseudonymisation)

Legislative adjustment of two registry acts
- The LifeGene Act
- The Act on Research Registers for Forensic Psychiatry

Processor agreement

The Data Protection Officer has the responsibility, according to article 28 in GDPR. If no processor agreement exists, the processor has no grounds for processing personal data. A processor manages (processes) personal data on behalf of the controller, according to Article 4.8.

Examples of instances when a processor agreement is drawn up
- Cloud services
- Outsourcing
- Support services
- Reporting personal data breaches
- Reporting process/routine
- The Supervisory Authority within 72 hours
- Processor to Controller without undue delay.
- To individuals without undue delay (if the leak could lead to, e.g. ID theft).

If a personal data breach has occurred, you report the incident to the University’s Data Protection Officer, dso@su.se.