Guidelines
2022-08-30
Reg. no: ORU 2020/05382
Page no: 1 (4)

This document has been translated from Swedish into English. If the English version differs from the original, the Swedish version takes precedence.

Guidelines for personal data processing at Örebro University

Governance and control of the university's GDPR compliance efforts

This document describes Örebro University's organisation, responsibilities, and the fundamental principles for personal data processing. Support and guidance for personal data processing in practice is provided on the GDPR page on the intranet and on the Swedish Authority for Privacy Protection's website.

The basis of the General Data Protection Regulation (GDPR)

As of 25 May 2018, GDPR (EU) 2016/679 is law in all of the EU's member states.

The fundamental principles of data protection to be observed are:

- Lawfulness – any processing of personal data must have a lawful basis, in a statute or ordinance.
- Purpose limitation – collecting personal data only for specific, explicitly stated and legitimate purposes.
- Data minimisation – not processing more personal data than is necessary for those purposes.
- Accuracy – ensuring that the personal data is accurate.
- Storage limitation – erasing personal data when it is no longer needed (erasure/archiving).
- Integrity – protecting the personal data, ensuring that no unauthorised persons are given access to it, or that data is not lost or destroyed.
- Accountability – not only complying with but also demonstrating how the university complies with GDPR.

The lawful grounds on which Örebro University (ORU) may base their processing of personal data are as follows: **legal obligation**, **exercise of official authority**, **public interest**, **necessary for a contract**, and **consent**.

Prior to each new processing instance, a risk analysis on the use of the personal data is to be undertaken, addressing the various aspects of the data protection principles.

GDPR and other legislation

GDPR is no obstacle to personal data processing that is necessary under legislation governing higher education operations or other regulations. Nor is it an obstacle to personal data processing that is necessary for enabling public authorities to fulfil their obligations under the Archives Act or for releasing official documents under the principle of public access to official records.

Processing record (compilation of the university's instances of personal data processing)

Örebro University has a legal obligation to maintain a record of instances of personal data processing. There is a processing record that to a large extent is based on the description of the university's processes as found in its information management plan. This record includes, notably, a description of process group, purpose, data subject categories and which categories of personal data is used, as well as the lawful ground cited.

Each school and department/office is to make sure that the personal data processing instances that take place within their operations can be found in the processing record. If a personal data processing instance is not accounted for, the data protection officer must be contacted for documentation support.

Division of responsibility

Personal data controller of personal data processing at the authority is Örebro University. This responsibility also covers personal data processing for the research that is conducted as part of university operations, and personal data processing performed by students as part of their studies.

Heads of school/heads of department/heads of office are responsible for ensuring that the rules for personal data processing are adhered to within their respective organisation. The head of school/department/office is the data protection coordinator at the school/department/office. This responsibility may be delegated and divided between the schools and between the departments/offices.

System owners are responsible for ensuring that a system in which personal data is processed is in compliance with the requirements laid down in GDPR. 'Systems' also include purchased system services not operated by Örebro University. The system owner is responsible for ensuring that questions concerning data protection are answered and documented in the systems inventory list *SystemInventeringsLista vid Örebro universitet* (SILOU).

System/service/process end users are responsible for ensuring that any personal data processing they undertake is in compliance with the requirements laid down in GDPR.

Members of staff are responsible for keeping abreast with and acting according to GDPR in relation to their respective duties and responsibilities and, when processing personal data, only using ORU-approved systems and services, as well as independently seek answers to questions concerning data protection in the information available on the intranet. If the relevant information cannot be found, professional services (records office, information security, data protection officer, legal office) should be contacted.

Researchers are responsible for keeping abreast with and acting according to GDPR and approved procedures for research containing personal data. The principal researcher of a project is responsible for signing and registering the necessary GDPR agreements, for ensuring that a risk analysis and any impact assessments are done etc. For all research projects processing personal data, there must be documentation describing that the data protection principles have been considered and in what way.

Teachers/course coordinators/programme coordinators are responsible for informing and referring students to information about GDPR when personal data processing is necessary to meet the intended learning outcomes. Information geared at students is available at oru.se. For all student projects processing personal data, there must be documentation describing that the data protection principles have been considered and in what way.

Students are responsible for keeping abreast with and acting according to GDPR for any personal data processing required during the course of their studies in accordance with the information received from the university.

Data protection officer (DPO)

The overall and most important responsibility of the DPO is monitoring that the organisation complies with GDPR. This includes:

- providing information, training and advice within the organisation, and
- checking that the organisation adheres to provisions and internal governing documents.

The DPO is also to:

- provide advice on risk analyses and impact assessments,
- be the contact person for the data subjects and the staff within the organisation, and
- be the contact person for the Swedish Authority for Privacy Protection and cooperate with them in the event of data breaches and inspections.

Once a year, the DPO is to submit a report to the university board. For the ongoing GDPR compliance efforts at the university, the DPO reports to the head of the Office for Academic Policy.

The DPO can be contacted via dataskyddsombud@oru.se.

Data protection coordinators at schools and departments/offices

The appointed data protection coordinators are listed on the GDRP page on the intranet.

The role of the data protection coordinators involves:

- being responsible for supplying the DPO with data in the event of requests for transcripts of records or requests from individuals under GDPR,
- reporting to DPO (for requests for transcripts of records),
- in the event of personal data breaches, providing support to the person responsible for the processing (e.g. system owner) in the investigation and management of the incident to the extent made possible by the competence offered the data protection coordinator via the training modules available at the university,

- disseminating in their own organisation information prepared/provided centrally at the university about GDPR/personal data processing,
- informing the school/department/office about personal data processing when such processing deviates from documents prepared centrally or if special procedures based on these documents, and which are to apply within the local organisation, have been prepared together with the data protection coordinator,
- coordinating the management of personal data processing instances at the school/department/office in cases when these are not evident from the processing record (see "Processing record" above),
- contributing to the development of Örebro University's data protection efforts by participating in the network for data protection coordinators at the university, and
- being the liaison to the DPO.

For more in-depth advice and complex questions, contracts etc., professional services (DPO/records office/information security/legal office) should be contacted.

Personal data processor

Processes personal data on behalf of Örebro University, as directed by the university in a written agreement.

Obligation to inform data subjects

Örebro University is obliged to inform data subjects of how their personal data will be processed under GDPR, how they can exercise their rights, etc.

In general terms, this information is provided in Örebro University's data protection policy, published on Örebro University's webpage. In addition, each process/system/service at Örebro University is to provide information on how personal data is processed. Information is also to be provided in the event of other data collection, such as via forms, recording of lectures, social media etc.

Personal data breaches

Whoever is responsible for personal data is obliged to have procedures in place to be able to detect, investigate and report personal data breaches. Whoever is responsible for the processing in question must immediately, once a breach has been discovered, report this to the DPO and initiate an investigation, including a risk and impact assessment. Individuals discovering or suspecting a personal data breach, are to report this to the DPO without delay.

If a report is to be made to the Swedish Authority for Privacy Protection, this must be done within 72 hours of the breach coming to the university's attention. All breaches warranting an investigation are to be registered at Örebro University, in Public 360.