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

Data protection/GDPR

Policy document Örebro University

Category: Guidelines

Reg. no: ORU 2024/02826

Adopted by: Vice-Chancellor

Last revised: 2024-05-14

Adopted: 2022-08-30

Document owner: Legal Office

ÖREBRO UNIVERSITY

Contents

Introduction

This document describes Örebro University's organisation, responsibilities, and the fundamental principles for data protection/GDPR. Support and guidance for personal data processing in practice are provided on the intranet, Inforum.

These guidelines are based on the EU General Data Protection Regulation (GDPR), which has been implemented as Swedish law.

The fundamental principles of data protection to be observed are:

- Lawfulness – any processing of personal data must have support in statutes or ordinances.
- Purpose limitation – collecting personal data only for specific, explicitly specified 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 data protection/GDPR.

Data protection/GDPR at Örebro University

All processing of personal data must have support in one of the legal grounds to be lawful. The legal grounds that the university can use to support the processing of personal data in its operations are as follows:

- Legal obligation – in its operations, the data controller must process certain personal data to comply with laws or rules.
- Exercise of official authority – the data controller must process personal data to carry out its duties as a public authority.
- Public interest – the data controller must process personal data to perform tasks in the public interest that are supported by law or other regulations. Examples include education and research.
- Necessary for a contract – personal data processing that may be necessary to fulfil a contract, such as personnel administration systems.
- Consent – as a rule, consent cannot be used as a legal ground for processing personal data of employees and students, as they are in a position of dependence relative to the university.

Legitimate interests – when the data controller's interests outweigh those of the data subject, and if the processing is necessary for the specific purpose. However, as a public authority, the university cannot apply legitimate interests as a legal ground.

Örebro University must maintain a processing record of its 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 the process group, purpose, data subject categories and which categories of personal data are used, as well as the legal 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. For personal data processing instances that are specific to an individual school or department/office, any specific circumstances must be documented by the respective school or department/office. These must be reported to the data protection officer, who compiles Örebro University's joint processing record.

Prior to each new processing instance not already included in Örebro University's processing record and/or the information management plan, a risk analysis on the use of personal data must be conducted, addressing the various aspects of the data protection principles.

Data protection/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.

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 oru.se. 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 types of data collection, including via forms, recording of lectures, and social media.

Roles and responsibilities

Örebro University is the personal data controller of all personal data processing at the university. This responsibility also covers personal data processing within research that is conducted as part of university operations and personal data processing performed by students as part of their studies. Various roles have different areas of responsibility within data protection/GDPR.

Data protection officer

According to the law, the university must appoint a Data Protection Officer (DPO). The DPO's overall and most important responsibility is monitoring that the organisation complies with data protection/GDPR. This includes:

- providing information, training and advice within the organisation on matters such as risk analyses and impact assessments,
- checking that the organisation adheres to provisions and internal governing documents,
- being the contact person for the data subjects and the staff within the organisation,
- being the contact person for the Swedish Authority for Privacy Protection and cooperating with them in the event of data breaches and inspections, and
- submitting an annual report on data protection efforts to the university board.

Data protection coordinators at schools and departments/offices

Each school and department/office must have a data protection coordinator. The appointed data protection coordinators are listed on Inforum. This responsibility may be delegated and divided between the schools and between the departments/offices.

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 other 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 to 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 data protection/GDPR,
- informing the school/department/office about data protection/GDPR when such processing deviates from documents prepared centrally or if local procedures based on these documents 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,
- contributing to the development of the data protection/GDPR 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. For research matters, there are also research data advisors at each faculty.

Personal data processor

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

Other roles

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 and for developing local procedures for the specific processing activities of their operations, if necessary. 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 responsible for systems in which personal data is processed must ensure that data protection/GDPR is complied with. 'Systems' also include purchased system services not operated by the university. System owners are responsible for ensuring that questions concerning data protection are addressed and documented as specified by the university.

Information owners responsible for processes where personal data is processed must ensure that data protection/GDPR is complied with. Information owners are responsible for ensuring that questions concerning data protection are addressed and documented as specified by the university.

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 accordance with data protection/GDPR, as well as the guidelines and procedures of the university.

Members of staff are responsible for keeping up to date with and acting according to data protection/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 seeking answers to questions concerning data protection in the information available on Inforum and within support functions.

Researchers are responsible for keeping up to date with and acting according to data protection/GDPR and approved procedures for research containing personal data. The principal researcher of a project is responsible for signing and registering the necessary data protection/GDPR agreements, for ensuring that a risk analysis and any impact assessments are performed 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 before the personal data processing is performed.

Teachers/course coordinators/programme coordinators are responsible for informing and referring students to information about data protection/GDPR when personal data is necessary for meeting 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/GDPR principles have been considered and in what way.

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