DIRECTIVE OF THE RECTORATE FOR THE DATA PROTECTION MANAGEMENT AT THE UNIVERSITY OF INNSBRUCK

1. Preamble

This directive forms the basis for the internal data protection management at the University of Innsbruck, which ensures compliance with legal requirements and the protection of processed personal data at the University of Innsbruck.

Data protection is of essential importance for the University of Innsbruck in research operations, student and staff administration—the University endeavors to fulfill the legal requirements in handling personal data.

In particular, the directive:

- Ensures that appropriate measures are implemented to comply with the GDPR,
- raises awareness of the need for strategic, technical, and organizational measures to ensure compliance with data protection requirements and
- defines core processes and priorities for the implementation of data protection issues at the university and assign appropriate responsibilities for their implementation

2. Principles

2.1. Management Commitment

The Rectorate considers responsible, measured, secure, and legally compliant handling of personal data an essential core value and will support the objectives and principles of data protection regulations in line with the University's strategy and objectives.

2.2. The importance of data protection

To ensure that the requirements for the protection of personal data are met on a long-term and university-wide basis, a data protection management system is operated at the University of Innsbruck, which - concerning relevant legal, technological, and organizational issues - is actively provided with appropriate time, technical and financial resources by the Rectorate.

2.3. Scope

This directive applies to the entire University of Innsbruck.

It applies to all employees and staff members who are entrusted with the implementation of data protection at the University of Innsbruck per the assigned roles and tasks, unless mandatory legal provisions, in particular regarding freedom from instructions, contradict this.

The implementation of this directive may take the form of technical and organizational measures. This also includes department-specific guidelines, company regulations, or company instructions, with which employees are obliged to comply.

The contents of the directive and all related documents must be communicated to the employees in the respective area of application. This is done via suitable training courses following the internal

training concept and the permanent provision of the relevant information on the University of Innsbruck intranet.

2.4. Objectives of the directive

The overall objective of the University of Innsbruck in introducing data protection management is to ensure compliance with the provisions of the EU General Data Protection Regulation (GDPR) and national data protection regulations in all processes that process personal data. In addition to ensuring compliance with the data protection principles (following Art. 5 GDPR), top priority is given to

- Ensuring excellence in research with personal data
- Handling personal data of students, employees, and other natural persons transparently and securely and limited to what is necessary
- Prompt and fair handling of requests within the scope of the rights of data subjects
- Targeted routines for checking applications (hard- and software systems) that process personal data.

2.5. Consequences of violations

Violations of valid data protection regulations by employees and / or external contractors may result in sanctions under labor, criminal or civil law.

2.6. Legal basis

Concerning the contents of this directive, the following legal standards serve as a basis:

- EU General Data Protection Regulation– GDPR
- Datenschutzgesetz – DSG
- Arbeitsverfassungsgesetz – ArbVG

3. Organization of data protection

The responsibilities regarding the implementation of data protection measures at the University of Innsbruck are defined below.

3.1. Rectorate

The Rectorate is responsible for compliance with the legal provisions of data protection. The Rectorate fulfills this responsibility through the present data protection directive, corresponding processes, the provision of the necessary technical, financial, and personnel resources as well as the subsequent implementation of adequate measures. The management system for data protection is implemented as a process of continuous improvement to coordinate the individual measures in the areas of data protection and information security in a way that the objectives of this directive are achieved.

Through regular checks and reports by the data protection officer and the internal control system, the Rectorate monitors the implementation of the provisions of the directive and promotes awareness of data protection among employees.

Specifically, the Rectorate ensures:

- Compliance with the legal provisions of the GDPR and national data protection regulations;
- appropriate and early involvement of the data protection officer in all matters relating to the protection of personal data;
- appropriate and early involvement of the data protection committee following the framework company agreement on the processing of personal data and the works councils in the cases provided for by law;
- that a register of all processing activities (record of processing activities) is kept following Art. 30 GDPR;

- appropriate support for the data protection officer in the performance of his/her duties, in particular by providing information on personal data and processing operations;
- that the data protection officer does not receive any instructions regarding the performance of his tasks;
- that the contact details of the data protection officer are published and communicated to the supervisory authority; and
- that the data protection officer is not dismissed or disadvantaged because of the performance of his or her duties.

3.2. Data protection officer

The data protection officer is appointed by the Rectorate and reports directly to it. He or she performs the tasks per Art. 39 GDPR.

He or she shall provide ongoing advice and information to the Rectorate, the data protection coordination, all persons responsible for implementation, and employees who carry out processing operations, concerning their obligations under the GDPR and other data protection regulations of the EU or the Member States and about the legal interpretations under the GDPR and all applicable data protection regulations.

In doing so, he or she shall receive appropriate support in the form of financial resources, infrastructure, and, if necessary, personnel.

Data subjects may consult the data protection officer on all matters relating to the processing of their personal data and the exercise of their rights. The data protection officer shall be bound by the obligation of secrecy or confidentiality in the performance of his or her tasks.

In the performance of his or her tasks, in particular regarding supervisory tasks such as audits, the data protection officer shall take due account of the risk inherent in the processing operations, having regard to the nature, scope, context and purposes of the processing.

3.3. Data protection coordination

The data protection coordination established at the University of Innsbruck implements the instructions of the Rectorate concerning data protection management. The data protection coordination supports other persons responsible for implementation in their defined data protection tasks.

The data protection coordination is responsible in particular for:

- Maintaining and regularly updating the record of processing activities following Art. 30 GDPR;
- advice and support in setting up data protection management (tasks, processes, documents);
- advice and support in connection with the processing of inquiries relating to data subject rights;
- planning and implementing the internal data protection training concept in cooperation with other service units.

3.4. Information Technology Services

The information technology services ensure the implementation of data protection requirements relevant to information security in its area of responsibility.

The information technology services must be involved in all projects and processes at an early stage by those responsible for processing activities to take security-relevant aspects into account as early as the planning phase.

3.5. Heads of organizational units, institutes and principle investigators of research projects

The heads of organizational units and institutes as well as the principle investigators of research projects are responsible for the proper processing of data in their area of responsibility. They are therefore obliged to ensure that the legal data protection requirements and those contained in this directive are considered and implemented accordingly.

It is their task to ensure proper data processing in compliance with the internal requirements and to introduce the defined processes through organizational, personnel, and technical measures.

In particular, they must ensure that all employees in their area of responsibility have taken note of the relevant guidelines and specifications.

The responsibility for a processing activity and the complete documentation in accordance with the GDPR lies with the head of the organizational unit responsible for the implementation and design of an internal administrative process / project or with the principle investigator of a research project and cannot be delegated. The respective person ensures, in coordination with the data protection coordination, that the documentation and regular updating of the processing of personal data and the technical and organizational measures (TOM) in the record of processing activities takes place and that the employees to whom this task is delegated have appropriate time resources.

3.6. Data protection delegates

The head of each organizational unit of the University of Innsbruck appoints a data protection delegate. In exceptional cases, smaller, closely interlinked organizational units may appoint a joint data protection delegate. The data protection delegates support the data protection coordination, under their guidance and training, in the implementation of data protection requirements at the level of the organizational units and ensure that important data protection issues are brought to the attention of the data protection coordination and resolved on a cross-institutional basis.

3.7. Data protection committee

The tasks and responsibilities of the data protection committee are described in the framework company agreement on the processing of personal data and are based on the statutory provisions on co-determination and data protection for employees. The data protection committee has general advisory tasks and tasks relating to the inspection of log files.

3.8. Users

Employees are obliged to comply with the specified rules when handling personal data, insofar as this concerns them. They are obliged to actively participate in internal training measures. They must comply with all overarching and department-specific data protection and security measures that have been brought to their attention through appropriate channels.

4. Basic principles for the processing of personal data

All employees, data processors, and other external contractors must fully comply with the provisions of the GDPR and the national data protection regulations in the respective applicable versions. This has to be ensured by the heads of organizational units and institutes as well as the principle investigators of research projects this in their area of responsibility.

All employees must be obliged in writing to maintain data secrecy in accordance with Section 6 DSG when they take up their duties. This obligation must include confidentiality regarding all circumstances that become known to employees as a result of their work. Data secrecy must continue to apply beyond the end of the employment relationship.

5. Record of processing activities

The data protection coordination is responsible for keeping a register of all processing activities (record of processing activities) in accordance with Art. 30 GDPR. Art. 30 GDPR defines the content to be included in the register. The record of processing activities must be kept in writing and made available to the supervisory authority upon request.

New processing activities of personal data (e.g. as part of research projects or new procedures) and changes to existing ones must be reported in advance to the data protection coordination. The notification must be made following the respective guidelines.

Everyone responsible for the establishment, implementation, or modification of processing activities of personal data within the meaning of the GDPR is obliged to carry out these notifications in a timely manner. Corresponding routines in their area of responsibility must be established in coordination with the data protection coordination. All documents for documentation and post-processing in the procedure directory must be provided to the data protection coordinator promptly.

Insofar as the University acts as a processor within the meaning of Art. 30 para. 2 GDPR, the data protection coordination shall also keep a corresponding record of processing activities for processors. This includes all services provided by the University for third parties and in which personal data is processed. Corresponding information must be submitted to the data protection coordination by the responsible organizational unit or research project.

6. Risk assessment and data protection impact assessment

When introducing or significantly changing processing activities of personal data, a risk assessment must be carried out by those responsible for the processing activity. It must be determined whether the activity poses a high risk to the data subjects in terms of type, scope, context, and purpose. The data protection coordination and the data protection officer shall support the risk assessment. If the risk assessment reveals the existence of a medium, high, or very high risk, the risk assessment, must be submitted to the responsible member of the Rectorate for a decision. Depending on the risk identified, appropriate technical and organizational measures to reduce the risk must then be defined and implemented.

If a processing activity is likely to pose a high risk to the rights and freedoms of natural persons due to the nature, scope, circumstances and purposes of the processing, data protection impact assessment must be carried out in advance. The data protection officer and the data protection coordination must be consulted and the data protection committee must be informed. The result must be recorded in writing and documented in the record of processing activities.

7. Awareness

The data protection coordination works with HR development to ensure that a training concept is drawn up and that training courses are held regularly.

8. Data breaches

In the event of a personal data breach, the University is obliged to respond immediately and take appropriate notifications and measures in accordance with Art. 33 and 34 GDPR. The handling of data breaches is regulated in a separate process.

Immediate reporting is ensured by communicating the university's internal guidelines and by training and sensitizing employees.

9. Rights of data subjects

The University of Innsbruck is obliged to safeguard the rights of data subjects and to ensure that they are fulfilled promptly when asserted.

This applies in particular to the following data subject rights:

- Right of access (pursuant to Art. 15 GDPR)
- Right to rectification (pursuant to Art. 16 GDPR)
- Right to erasure / right to be forgotten (pursuant to Art. 17 GDPR)
- Right to restriction of processing (pursuant to Art. 18 GDPR)
- Right to data portability (pursuant to Art. 20 GDPR)
- Right to object (pursuant to Art. 21 GDPR))

As legal deadlines start at the time of incoming requests that address the rights of data subjects, those responsible for the processing activity must ensure that such requests are forwarded to the data protection coordination immediately upon becoming aware of them. The data protection coordination will take over the processing, if necessary in coordination with the department heads, the data protection officer, and the responsible member of the rectorate.

10. Information obgliations

The persons responsible for processing personal data in their area of responsibility must ensure, together with the data protection coordination, that all necessary information is made available to the data subjects in an appropriate manner. This applies in particular to the transmission of information in accordance with the following articles:

- Art. 13 GDPR (obligation to provide information when collecting personal data from the data subject)
- Art. 14 GDPR (obligation to provide information if the personal data was not collected from the data subject):

11. Technical and organizational measures (TOMs) Privacy by Design / Privacy by Default

In coordination with the information technology services and the data protection coordination, the persons responsible for a processing activity must take suitable technical and organizational measures (TOMs) to secure the personal data processed in their respective areas of responsibility, depending on

- the state of the art,
- the costs of implementation,
- the nature, scope, context, and purposes of the processing, and
- the different probabilities of occurrence and severity of the risk to the rights and freedoms of natural persons.

In any case, these measures must meet the requirements of Art. 32 GDPR and ensure a level of protection appropriate to the risk. The definition of the state of the art is based on the guidelines of the European Data Protection Board, (inter)national standards and best practice approaches such as ISO/IEC 27001 or BSI IT-Grundschutz.

Furthermore, the responsible persons must ensure that data protection requirements are incorporated into the overall design of data processing from the outset (e.g. when introducing new applications) (**privacy by design**) and ensure that products or services are configured to be data protection-friendly by default (**privacy by default**). They are supported in this by the data protection coordination, the data protection officer, and the persons responsible for the IT systems.

12. Conditions for acting as a data processor

The person responsible for the processing activity ensures, if necessary in coordination with the data protection coordination and the authorized signatories, that the framework conditions pursuant to Art. 28 and Art. 29 GDPR are complied with and agreed in documented form when selecting and commissioning data processors. For this purpose, a contract for commissioned data processing must be concluded with each data processor (e.g. service provider) who processes personal data on behalf of the University of Innsbruck.

Responsible persons must report the processing of personal data on behalf of third parties to the data protection coordination in good time before the start of the processing activity so that these are documented and recorded in the register of processing activities of the University as processor.

13. Conditions for joint controllership

If the means and purposes of processing personal data are determined jointly with external partners (joint controllers), the responsible person must, if necessary in cooperation with the data protection coordination and the authorized signatory, organize the conclusion of an agreement in which the tasks and responsibilities pursuant to the GDPR between the contractual partners (joint controllers) are defined, in particular with regard to the data subjects whose data they process. The main provisions of this agreement must be made available to the data subjects. The internal guidelines must be observed.

14. Review and maintenance of the data protection management system

Data protection management at the University of Innsbruck is a continuous process that must be constantly reviewed, maintained and, if necessary, adapted or improved.

In particular, regular audits are to be carried out to check the completeness, correctness and effectiveness of the implemented processes and measures and to report the results to the Rectorate (Jour Fixe, management meetings).