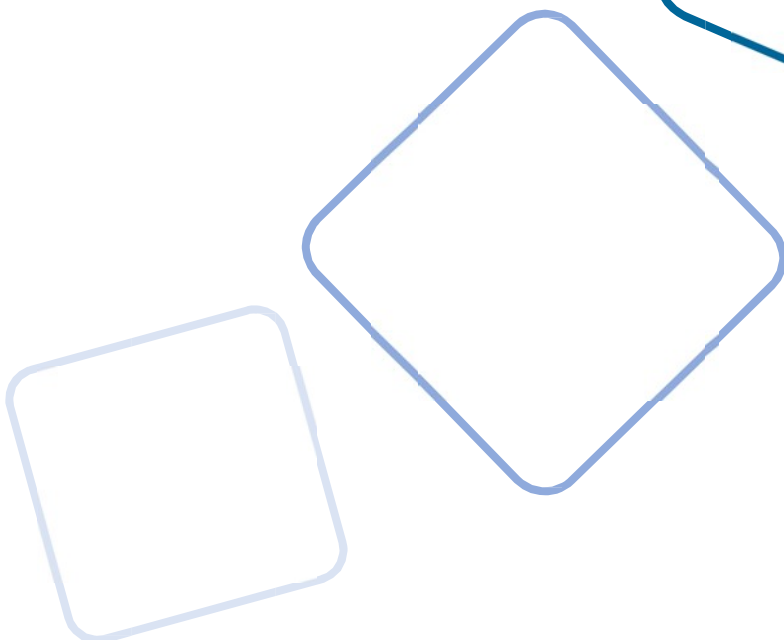
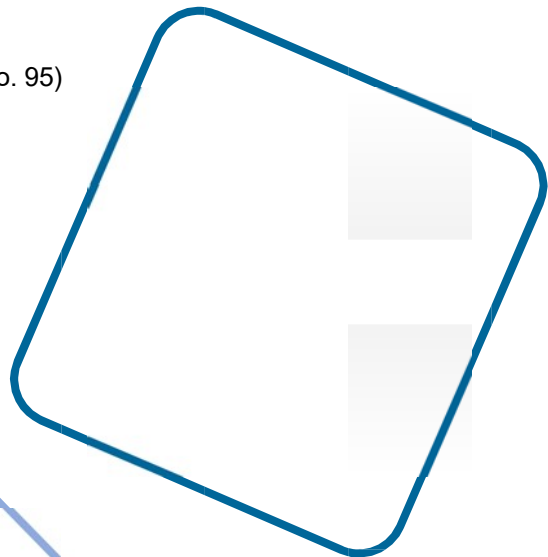


Data Protection Organisation at TU Wien

(online 20 March 2018)
Announcement in Newsletter No. 8/2018 (serial no. 95)

Decided at the Rectorate meeting on 30 January 2018





Contents

I.	How data protection is organised at TU Wien.....	3
II.	Roles in data protection organisation at TU Wien	4
1.	Rectorate	4
2.	Data protection officer/s	4
3.	Data protection coordinator/s	5
4.	Data protection contact persons (if appointed)	6
III.	Professional interfaces	7
1.	Data owners	7
2.	IT and IT security	7
3.	HR Administration	8
4.	Admissions Department, Continuing Education Centre, Deans' Offices	9
5.	Security	9
6.	Internal Audit.....	9
IV.	Data protection by the members of TU Wien.....	9
1.	Immediate supervisors.....	9
2.	Project managers.....	10
3.	All members of TU Wien	10
V.	Consequences of non-implementation	10

Preamble

This document describes how TU Wien organises data protection and defines corresponding roles and tasks. The roles and tasks are adapted or extended as required and represent minimum requirements in the form described.

This document is directed to all members of TU Wien according to Section 94 of the Austrian University Act (UG). Third parties are to be bound by contractual and other agreements in the relevant points. In addition, the organisational regulations contained herein shall apply without chronological or geographical restrictions.

I. How data protection is organised at TU Wien

The way data protection is organised ensures that corresponding responsibilities, documentation frameworks, roles, tasks and competences are defined so that data protection legislation and regulations are complied with. A person can have more than one role, just as a role can be divided among several persons in some cases.

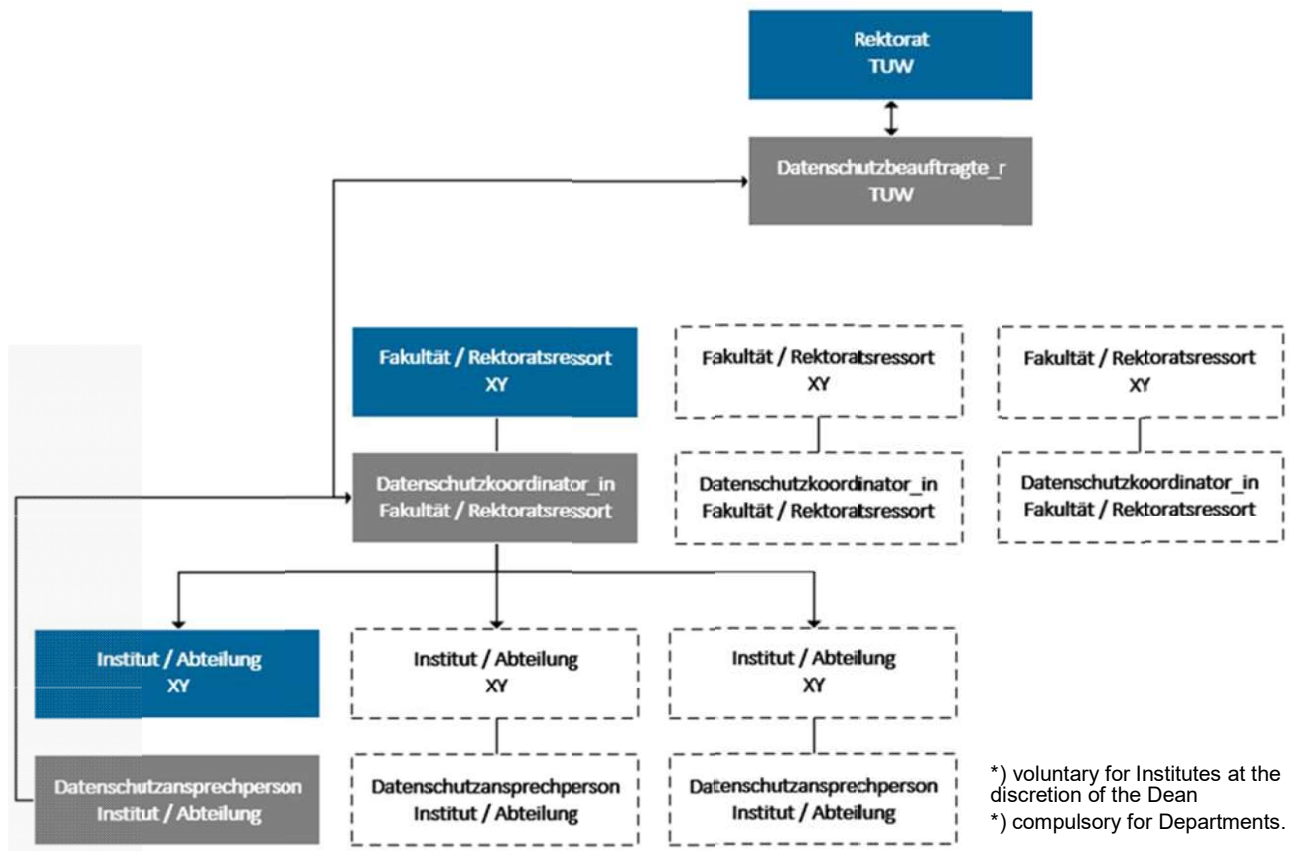


Figure 1: How data protection is organised at TUWien

The organisation of data protection at TU Wien also covers the Vienna Scientific Cluster (VSC) but not the holdings of TU Wien. The Senate, University Council, special interest groups of TU Wien and



Institutions with special tasks according to the applicable organisation chart of TU Wien may nominate a data protection contact person at their own discretion.

II. Roles in data protection organisation at TU Wien

1. Rectorate

The Rectorate of TU Wien is responsible for complying with legal and internal university data protection regulations. The data protection organisation supports the Rectorate in fulfilling its responsibilities and performs the operative handling of processes and tasks related to data protection.

Tasks

- Strategic development of data protection at TU;
- Appointing the data protection officer;
- Appointing the data protection coordinator/s by the competent member of the rectorate in accordance with internal rules of procedure (GO),
- Ensuring that the data protection officer and data protection coordinator are free to issue instructions in the performance of their duties;
- Ensuring availability of human and financial resources for data protection;
- Approval of data protection guideline(s) and other relevant documents;
- Deciding on and implementing measures at university level, e.g. resulting from reviews / audits;
- Promoting the awareness of data protection on the part of all employees of TU Wien;
- Offering training and specific training courses on the subject of data protection;
- Dealing with topics relevant to data protection introduced by the data protection officer.

2. Data protection officer

A data protection officer as defined by the EU General Data Protection Regulation (GDPR) is to be appointed further to both statutory requirement and to internal regulations. According Section 38 of the GDPR, the data protection officer must be duly involved in all activities involving the protection of personal data at an early stage. The data protection officer is not subject to directives in the exercise of his/her duties and may not be dismissed from this position or suffer any disadvantages in the exercise of these tasks and duties. The Data Protection Officer is required to manage the organisational structure of data protection at the University and to identify data protection violations. He/she will report on his/her findings to the Rectorate. In this context, the intensity of reporting is required to take a risk-based approach. By contrast and due to any lack of appropriate authority to issue instructions, active intervention to eliminate or prevent individual data protection breaches will not fall within the scope of duties of the data protection officer. The data protection officer may also perform other tasks and duties but it must be ensured that these do not lead to any conflict of interest.



Tasks

- Primary contact person at TU Wien in data protection matters, in particular responsible for communication with authorities and data subjects.
- According to GO, reporting directly to the Rectorate member responsible (reporting channel); in this context, this is to be done at least once a year. In consultation with the respective data protection coordinators, preparing a comprehensive report for the Rectorate on the data protection issues from the previous financial year and on the planned activities on the subject of data protection.
- Monitoring compliance with the legal requirements of the GDPR and the Austrian Data Protection Act and other statutory framework conditions related to data protection legislation, the regulations enacted further to this legislation and related internal regulations, sensitisation and training of employees and the related reviews.
- Support for data protection coordinators in the performance of their role and compliance with international, national and internal data protection rules including organising regular and appropriate data protection training courses.
- Responsible creation, updating and communication of regulations in the field of data protection which must be applied by all members of TU Wien according to Section 94 of the Austrian University Act (e.g. data protection governance, the data protection organisation manual, data protection guidelines descriptions, etc.).
- Carrying out reviews (supervision).
- Responsible monitoring and coordination of the data protection impact assessment prepared by the data protection coordinator for the introduction of processing activities where a great risk to the rights and freedoms of data subjects may be expected.
- Provide guidelines on how to proceed in connection with the preparation of the register of processing activities, carrying out a data protection impact assessment and arrangements connected with data protection incidents.
- If necessary, introducing data protection-relevant subjects as agenda items to the weekly Rectorate meetings by a responsible Rectorate member as per GO procedure.
- Identifying improvements based on data protection audits ("State of Privacy").
- Holding regular meetings with data protection coordinators, including to ensure that data protection activities, processes, policies and methods are accepted by general agreement.
- Advice on the selection of any contract data processors and on the drafting of the necessary contractual agreements in this regard.
- Sensitisation and awareness-raising.
- Publication of the contents of the data protection guideline/s and regulations, in particular relating to employees working with personal data.
- Coordinating and organising full compliance with processing, recording and storage requirements.

3. Data protection coordinator/s

The data protection coordinators are contact persons for all data protection-related topics within the assigned faculty / sub-rectorate. The data protection coordinators are not subject to instructions in this



capacity. The data protection coordinators are obliged to report data protection breaches.

Tasks

- First contact person for data protection questions in the assigned area.
- Advice and support for staff in the faculties / sub-rectorates.
- Responsible for the dissemination and support in implementing the data protection requirements in their faculties / sub-rectorates and cross-team promotion of the respective data protection processes in order to increase effectiveness.
- Event-related reporting directly to the relevant dean or rectorate member (direct reporting channel) and additionally to the data protection officer as part of data protection organisation.
- Close coordination among each other: with the data protection contact persons and with the data protection officer to ensure the uniform implementation of the data protection regulations.
- Initial assessment and recording of new processing activities.
- Updating documentation when changes are made to processing activities in the assigned area.
- Carrying out an impact assessment and - if necessary - a data protection impact assessment before introducing a new processing activity and periodically for the existing processing activities in coordination with the respective data owners, the data protection officer and TU Information Technology Solutions (TU.it) department.
- Raising the awareness of employees working in their faculty / sub-rectorate.
- Publicising the contents of the data protection directive(s) and regulations, in particular relating to employees working with personal data;
- Supporting the data protection officer in the performance of his or her duties;
- Fulfilling and monitoring data protection requirements in the assigned area.

4. Data protection contact persons (if appointed)

The data protection contact persons are the first point of contact for data protection issues at an institute/department. Establishing this role at institutes is not compulsory but it is at least recommended that this role be established in the departments. In this context, a data protection contact person may look after several departments. The head of an institute / department may assume this task him/herself or assign these tasks to another person in a department of the institute, provided this person consents. The data protection contact persons are obliged to report violations of data protection.

Tasks

- First contact person in the assigned institute / departments for data protection issues.
- Advice and support for employees in the institutes / departments.
- Responsible for dissemination and support in the implementation of data protection requirements in their institutes / departments and cross-team promotion of the respective data protection processes to increase effectiveness.
- Event-driven reporting directly to the relevant head of institute / department (direct reporting channel) and also to the data protection coordinator within the framework of the data protection organisation.



- Notifying the data protection coordinator responsible of new processing activities and changes in processing activities.
- Raising the awareness of employees working in their institute / department.
- Publishing the contents of the data protection directive(s) and regulations, in particular for those employees working with personal data.
- Supporting the responsible data protection coordinator and the data protection officer in the performance of their duties.
- Fulfilling and monitoring the data protection guidelines in the assigned institute / department.

III. Professional interfaces

1. Data owners

The data owners are responsible for the proper implementation of the data protection requirements, in particular the rights of the data subjects, information requirements and data security measures. The data owners are those persons who decide on the processing of personal data.

Tasks

- First-time notification of the processing of personal data and ongoing notification of any changes thereto to the relevant data protection coordinator for the purpose of documenting the processing activities within his/her own area of responsibility.
- Authorising access rights and regular reviews of access rights, defining user rights in coordination with the data protection officer.
- Classifying the data and information for which he/she is responsible, e.g. with regard to confidentiality, availability, integrity and comprehensibility.
- Identifying and dealing with data protection risks.
- Specifying security requirements for the protection of personal data.
- Monitoring the implementation of measures and ensuring that the data protection requirements are at an appropriate level of protection.
- Supporting the data protection contact person – assuming such a position has been established – and the data protection coordinator in each area and the data protection officer in carrying out their duties.

2. IT and IT security

Information and data security are an essential part of data protection. The measures used in information security management and required data security management must also be coordinated in the context of the GDPR and data protection. A structured exchange of these disciplines is therefore to be established.

As the professional expert, TU.it is the main operational contact for the data protection officer for technical IT security issues and for guaranteeing the security requirements necessary to ensure data protection. For this reason, there must be a regular exchange of information.



Tasks of TU.it

- Coordinating the necessary IT security measures with regard to TUNET and for all IT services provided by TU.it.
- Developing IT-specific processes and concepts with regard to data security based on data security requirements.
- Developing, implementing, documenting and monitoring detailed implementation plans for data security measures.
- Supporting TU employees with technical assistance, information and recommendations (use of "owncloud", TU files, email encryption etc.).
- Supporting the data protection officer in performing his/her duties, in particular safeguarding the rights of data subjects, investigating data protection incidents, supervision and audits.
- Immediately reporting critical weaknesses and data protection incidents to the data protection officer.

Decentralised IT contact persons¹ have the following tasks in their immediate sphere of activity:

- Implementing and managing the effectiveness of the (planned) IT security measures during operation time.
- Implementing and managing the effectiveness of the (planned) data protection measures during operation time.
- Sensitisation and awareness-raising.
- Immediately reporting critical weaknesses and data protection incidents to the data protection officer;
- Making practical suggestions/raising practical issues.

The establishment of a responsible role for IT security within TU.it as the central point of contact for all IT security issues at TU Wien is planned for early 2019 at the latest. In addition, the necessity for establishing the position of an information security officer at TU Wien will be examined.

3. HR administration

As a professional expert, the HR Administration department is responsible for implementing and managing employee-related data protection guidelines and measures.

Tasks

- Documenting data protection-related information requirements and consent declarations to do with employees of TU Wien.
- Adapting company agreements with regard to the applicable data protection guidelines.
- Supporting the data protection officer in performing his/her duties.

¹ The group of persons of IT contact persons (role in TISS) has been the main contact for institutes and departments at TU.it for many years.



4. Admissions Department, Continuing Education Centre and Dean's Department

As professional experts, the Admissions Department, the Continuing Education Centre and the Dean's Departments are responsible for implementing and managing student-related data protection guidelines and measures.

Tasks

- Documenting data protection-related information requirements and consent declarations to do with students at TU Wien.
- Adapting information on admissions with regard to the applicable data protection provisions.
- Supporting the data protection officer in performing his/her duties.

5. Security

In its role as a technical expert, the Department for Buildings and Engineering (GUT) is responsible for implementing and managing data protection guidelines and measures with regard to the infrastructure areas in the GUT. These cover areas such as building protection, entry systems, employee protection (including workplace medicine), cleaning, events, maintenance, property management and contracting.

Tasks

- Developing, implementing, documenting and monitoring the data protection-related measures of GUT for entry systems, employee protection (including workplace medicine), cleaning, events, maintenance, property management and contracting;
- Supporting the data protection office in performing his/her duties.

6. Internal Audit

The Internal Audit department is responsible for checking and reviewing the data protection processes and measures for compliance with the provisions of internal guidelines, external requirements and industry standards. In addition, the efficiency and effectiveness of these processes must be ensured by means of inspections.

IV. Data protection by the members of TU Wien²

1. Immediate supervisor

The immediate supervisor functions as an example and multiplier in data protection issues TU Wien.

² i.a.w. Section 94 Austrian University Act (UG)



Tasks

- Supports its employees in data protection issues.
- Sensitisation and awareness-raising.
- Functioning as an example for its employees.

2. Project manager

The project manager is responsible for complying with data protection in those projects that he/she manages. This applies to all projects at TU Wien and not solely to research projects.

Tasks

- Identifying data protection relevance in projects.
- Identifying data protection risks in projects.
- Involving and informing the responsible data protection coordinator in and on matters concerning data protection in projects.
- Planning data protection and data security measures and responding to risks in projects in which personal information is processed.
- Coordinating on identified risks, necessary measures, required resources with the data owners and the data protection contact person (if available), otherwise with the responsible data protection coordinator.
- Immediately reporting weaknesses and data protection incidents in projects to the responsible data protection contact person (if available), otherwise to the responsible data protection coordinator;
- Monitoring compliance with data protection guidelines and processes in the project environment.
- Ensuring inclusion of data protection and security-related factors in projects.

3. All members of TU Wien³

Tasks

- Complying with and implementing data protection guidelines and measures.
- Reporting possible risks.
- Making suggestions for improvements.
- Reporting security-related incidents and security deficiencies.

V. Consequences of non-implementation

Fulfilment of duties is monitored – both regularly and as warranted – by the data protection officer. The data protection regulations are to be complied with strictly in order to guarantee data protection and to avoid legal claims.

³ i.a.w. Section 94 Austrian University Act (UG)



>Data Protection: Organisation<



⁴ i.a.w. Section 94 of the Austrian Universities Act