

MANUAL DATA PROTECTION

Handling Personal Data at
TU Graz



Imprint

Graz University of Technology
Quality Management, Evaluation & Reporting
Rechbauerstraße 12
8010 Graz

Authors

Mag.iur. Daniel Kurzmann, BA MA LL.M.
daniel.kurzmann@tugraz.at

Mag.iur. Christof Plaschke
christof.plaschke@tugraz.at

Last updated

2023

Layout/Typesetting

Nina Eisner, polycoon e.U.

You can find the online version of the manual
by scanning the QR code below:



Contents

1. Definitions	8
1.1. General Data Protection Regulation	8
1.2. Personal Data	9
1.3. Special Categories of Personal Data	9
1.4. Health Data	10
1.5. Processing	11
1.6. Pseudonymised Data	11
1.7. Anonymised Data	12
1.8. Distinction Between Anonymised and Pseudonymised Data	12
1.9. Data Subjects	13
1.10. Controller	13
1.11. Joint Controller	14
1.12. Processor	14
1.13. Material Scope of Application	15
1.14. Territorial Scope	15
2. Principles and Internal Implementation	17
2.1. Internal Implementation Measures	17
2.1.1. TU Graz Staff Data Protection Advisory Committee	17
2.1.2. TU Graz Extended Data Protection Advisory Committee	18

2.1.3. TU Graz Statute Part Data Protection Policy	18
2.1.4. Company Framework Agreement “On the Automated Processing of Personal Data of Staff”	18
2.1.5. Application Request for Personal Data Processing	19
2.1.6. TU Graz Data Protection Officer	19
2.2. Principles and Legal Bases for Personal Data Processing	20
2.2.1. Lawfulness, Fairness, Transparency	21
2.2.2. Purpose Limitation	23
2.2.3. Data Minimisation	24
2.2.4. Accuracy	25
2.2.5. Storage Limitation	25
2.2.6. Integrity and Confidentiality	26
2.2.7. Accountability	26
2.2.8. Data Protection Information	27
2.2.9. Rights of the Data Subjects	28
2.2.10. Information Security	31
2.2.11. Data Protection Incident/Data Breach	31
2.2.12. Processing Directory (Proventor Tool)	33
2.2.13. Data Protection Impact Assessment	34
3. Teaching	35
3.1. Fulfilment of the Requirement to Inform Students	35
3.2. Retention Periods for Teaching Purposes	35

3.2.1. Assessment Documents	36
3.2.2. Bachelor Theses, Seminar Papers	36
3.2.3. Retention of University Specific Data (Examination Data)	36
3.2.4. Room Assignments	38
3.3. Data Published in the Context of Oral (Final) Examinations	38
3.4. Data Published in the Context of Written Examinations	39
3.5. Signature Lists And Attendance Lists	39
3.6. Photos and Videos Taken in the Context of Courses/Excursions	39
3.7. Sending Interim Results	40
3.8. Homework/Inspections	40
3.9. Data Protection and Confidentiality Requirement for Theses	41
3.10. Data Published in the Context of Graduation Ceremonies	42
3.11. Virtual Teaching	42
4. Research	43
4.1. Data Protection in Research	43
4.2. Distribution of Roles	44
4.3. Legal Bases	45
4.3.1. General Data Protection Regulation (GDPR)	45

4.3.2. Data Protection Act (DSG)	46
4.3.3. Research Organisation Act (FOG)	46
4.4. Principles of the GDPR	47
4.5. Retention Periods for Research Data	50
4.6. Processing of Children's Personal Data	51
4.7. Recommended Procedure	52
4.7.1. Clarification of the Organisational and Legal Framework	52
4.7.2. Clarification of Implications of the Data Protection Regulation	52
5. Administration	53
5.1. Introduction	53
5.2. Staff	53
5.2.1. Applications	53
5.2.2. Unsolicited Applications/Keeping Records of Applications	54
5.2.3. Data Protection Information for (New) Staff Members	55
5.2.4. Birthday Calendar	55
5.2.5. Staff Appraisals	55
5.2.6. Obligations of Secrecy	56
5.2.7. Retention of Personal Staff Data	56
5.2.8. Publishing Data of Former Staff Members on the (Institute's) Website	57

5.2.9. Processing of Children's Personal Data	57
5.2.10. Video Surveillance	58
5.3. Events and Public Relations	58
5.3.1. Events	58
5.3.2. Websites	59
5.3.3. Social Media (Facebook, Instagram, X, LinkedIn etc.)	59
5.4. Handling Contact Details	60
5.4.1. Contact Databases	60
5.4.2. Sending Invitations and Newsletters	61
5.4.3. Writing to New Contacts	62
5.4.4. Communication with TU Graz Staff and Students	62
6. Archive Material	63
7. Contact Details	64
8. Selected Links	66





A summary of the most important points and, in particular, the legally binding requirement to notify responsible parties in the event of a data protection violation (data breach), can be found on the **Fact Sheet for TU Graz Employees on Information Security and Data Protection** (see [Selected Links](#)).

¹ Regulation 2016/679/EU of the European Parliament and of the Council dated 27.04.2016, established to support the protection of individuals with regard to the processing of personal data, the free movement of such data, and to repeal Directive 95/45/EC (General Data Protection Regulation), OJ L 201/37.

² Directive 95/46/EC of the European Parliament and of the Council dated 24.10.1995, established to support the protection of individuals with regard to the processing of personal data and the free movement of such data, OJ L 281/31.

³ Federal Act Concerning the Protection of Personal Data (Data Protection Act, in German: Datenschutzgesetz or DSG), BGBl I 165/1999 idF I 148/2021.

⁴ Federal Act on General Matters relating to Article 89 GDPR and Research Organisation (Research Organisation Act, in German: Forschungsorganisationsgesetz or FOG), BGBl I 341/1981 idF I 116/2022.

1. Definitions

1.1. GENERAL DATA PROTECTION REGULATION


The General Data Protection Regulation¹ (hereinafter referred to as the GDPR) has been in force since 25 May 2018 and is directly applicable as an EU regulation in the member states of the European Union (EU). It has also been an applicable law in the member states of the European Free Trade Association (EFTA) since 20 July 2018. Thus, the GDPR replaces the Data Protection Directive² and contributes to the harmonisation of data protection law in the EEA. Numerous opening clauses allow national legislators to make independent regulations that reference various individual issues or sub-areas.

By passing the 2018 Data Protection Amendment Act, the Austrian legislators amended the Data Protection Act³ (previously referred to in German as the *Datenschutzgesetz* or DSG 2000) along with several other material laws (including the Research Organisation Act⁴, see further information).

Unless explicitly stated as otherwise, the term “data” in this manual always refers to “personal data” as defined in the GDPR.

1.2. PERSONAL DATA

For the purposes of the GDPR, the term “personal data” means any information relating to an identified or identifiable natural person (hereinafter referred to as a “data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person (Article 4(1) GDPR).



Examples: First name, surname, address, date of birth, gender, IP address, identification number by which a person can be identified.

1.3. SPECIAL CATEGORIES OF PERSONAL DATA

Special categories of personal data for the purposes of the GDPR (colloquially referred to as “sensitive data”) are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. In addition, genetic data, biometric data for the purpose of uniquely identifying a natural person, health data, or data



concerning a person's sex life or sexual orientation is considered sensitive data (Art. 9 para. 1 GDPR).

The processing of aforementioned data is only permissible if one of the exceptions listed in Art. 9 para. 2 GDPR applies (e.g. explicit and voluntary consent, processing for the purposes of preventive health care or occupational medicine, if a legal basis for this exists). Furthermore, when processing sensitive data, higher requirements must be put in place when implementing technical and organisational measures (see also 2.2.1. – Lawfulness, Fairness, Transparency).

Whether the data is sensitive can be determined by defining the purpose of the processing. If the processing is done for purposes of preventative health care, for example, the data are usually health data (see also the following point) and, therefore, is sensitive data.



Examples: Processing of brainwave measurements as part of research projects, where these are or can be assigned to a person (e.g. via an ID number); processing of the national insurance number in a health-related context.

1.4. HEALTH DATA

Health data is personal data related to the physical or mental health of a natural person, including the provision of health services, and reveal information about their health status. Whether the data is health data depends in particular on the purpose of the processing. For example, the national insurance

number constitutes health data if it is used for the purposes of providing health services.

1.5. PROCESSING

“Processing” refers to any operation or set of operations which is performed on personal data, whether or not this is by automatic means, such as the **collection, recording, organisation, filing, storage, adaptation or alteration, retrieval, querying, use, disclosure by transmission, dissemination or the otherwise making available, alignment or combination, restriction, erasure or destruction** of data (Art. 4 para. 2 GDPR).

This definition clearly shows that the term “processing” should be interpreted very broadly. If in doubt, therefore, processing is assumed to occur.



1.6. PSEUDONYMISED DATA

The personal data (e.g. identification number/code) is processed in such a way that the data can no longer be attributed to a specific data subject without using additional information (e.g. addresses, names), provided that this additional information is kept separately and appropriate technical and organisational measures are implemented (e.g. control of entry, access, and storage periods) which ensure that the personal data cannot be attributed to an identified or identifiable natural person (Art. 4 para. 5 GDPR).

If the names of persons are replaced by codes, the data is normally considered as pseudonymised.

Although it is more difficult to establish the person's identity, the connection between a person and their data can be re-established. Therefore, the person is at least identifiable.



Examples: One-way/hash function; nickname; participating individuals can be identified by pre-existing conditions combined with age despite the removal of data.

1.7. ANONYMISED DATA

If it is impossible to attribute the data to a person, i.e. if it is impossible to establish a connection between the person and the data, the data is considered as anonymised or anonymous. Such data is not personal data, and, for this reason, the data protection law does not apply.



Example: Aggregated data that is used for statistical purposes and cannot (or can no longer) be attributed to a person.

1.8. DISTINCTION BETWEEN ANONYMISED AND PSEUDONYMISED DATA

Anonymised: It is impossible to attribute data to a person. It is no longer possible to establish a connection between the data and a person, so the data protection law does not apply.

Pseudonymised: For example, a person's name is replaced by a code (e.g. QR code). It is more difficult to establish the person's identity, but the connection between a person and their data can be re-established. The person is identifiable, and the data is considered as personal data; therefore, the data protection law applies.

1.9. DATA SUBJECTS

Data subjects or “the subjects” are natural or legal persons whose personal data is processed by a data controller or processor.



1.10. CONTROLLER

For the purposes of the GDPR, a controller is any natural or legal person, public authority, agency, or other body who/which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Processing activities carried out by employees based on work instructions are attributed to the employer. In this case, the employees are not data controllers as defined in the GDPR. This also applies to employee-like persons and to relationships and to executive employees as part of their requirement to follow instructions. The situation is different if employees act in ways that conflict with or deviate from the employer's instructions and, thus, indicate that they are, for example, pursuing their own interests. For this reason, the actions of the employees can no longer be attributed to the employer, and the employees take on the

⁵ Leitinger, Gosch, *Die Zurechnung unterstellter Personen zum Verantwortlichen mit besonderem Fokus auf das Verhältnis zwischen "Mitarbeiter" und "Arbeitgeber"*, *jusIT* 2021/46, 115 (122).

⁶ Leitinger, Gosch, *Die Weisung im Datenschutzrecht – Konsequenzen aus Datenschutzverößen durch Mitarbeiter*, *jusIT* 2022/9, 23 (28).

role of the controller.⁵ Such processing, therefore, could not be attributed to the employer.⁶

1.11. JOINT CONTROLLER

If two or more controllers jointly determine the purposes and means of the processing of personal data, they are jointly responsible for the data processing. In this case, the joint controllers must conclude an agreement in which they transparently regulate who is responsible for fulfilling the obligations under data protection law (e.g. obligation to inform, data subject rights, data breach). This agreement must be in writing.

Use cases: TU Graz and (research) partners who jointly process personal data, e.g. BioTechMed, Digital University Hub, scholarship programmes, NAWI Graz.

1.12. PROCESSOR


A processor is any natural or legal person, public authority, agency, or other body which processes personal data on **behalf of the controller**. If data will be processed, a data processing agreement must be concluded (DPA; in German: *Auftragsverarbeitungsvertrag* or *AVV*). If TU Graz commissions a service provider, it is advisable to refer to the data protection law and clarify whether the commissioned processing will take place under certain circumstances.

If personal data is transferred to third parties (i.e. processing is not commissioned or data processing

is jointly controlled, for example, by a company that destroys hard disks as a service, or sends letters (by post), it may be necessary in individual cases to conclude a confidentiality agreement.

1.13. MATERIAL SCOPE OF APPLICATION

The GDPR applies to the **wholly or partly automated processing** of personal data as well as to the **non-automated processing** of personal data that is **stored or intended to be stored** in a **filing system (and card index system, e.g. documents in a physical file)** (Art. 2 GDPR).

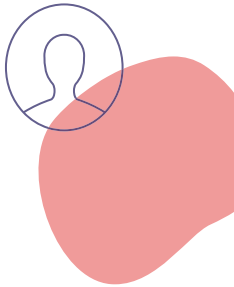


Example: A staff member has a conversation with the works councillors about supervisors. The personal data exchanged in the oral conversation is not covered by the scope of the GDPR. However, the fundamental right to data protection (§ 1 of the Data Protection Act) still applies in this case.

1.14. TERRITORIAL SCOPE

The territorial scope of the GDPR covers all data processing that takes place in the context of the activities carried out when establishing a controller or processor in the EU. Whether the data processing takes place in the EU does not play a role.

If a controller or processor is not established in the EU, but still processes the personal data of



individuals in the EU, the GDPR applies, if:

- these provide goods or services in the EU, or
- the conduct of individuals is observed, provided this conduct takes place in the EU (Art. 3 GDPR).



Example: In the context of an international research project jointly carried out by TU Graz and a Chinese university, the health data of the individuals participating in the project is jointly analysed. Both universities are obliged to comply with the GDPR, especially as the participating individuals are EU citizens.



© Kinn Studio – AdobeStock

2. Principles and Internal Implementation

2.1. INTERNAL IMPLEMENTATION MEASURES

In order to meet the requirements of the data protection regulation, TU Graz has amended the data protection section of the Statutes and adopted a company framework agreement to regulate data protection aspects related to processing the personal data of staff members.

In the data protection regulations section of the Statutes, the Data Protection Advisory Committee for staff was set up to pass resolutions, and the extended Data Protection Advisory Committee was set up to advise the Rectorate on data protection issues (see 2.1.1. and 2.1.2.).

2.1.1. TU GRAZ STAFF DATA PROTECTION ADVISORY COMMITTEE

The Staff Data Protection Advisory Committee (<https://tu4u.tugraz.at/go/dsb-a>) deals with all issues that arise related to the processing of staff members' personal data, and in particular with the introduction, operation, and modification of ICT systems (see 2.1.4.).



2.1.2. TU GRAZ EXTENDED DATA PROTECTION ADVISORY COMMITTEE

If not only personal data of staff members but also those of students, other university members (e.g. private lecturers, research fellows), and external persons (e.g. applicants for positions and degree programmes, as well as staff members of third parties) is affected, this processing falls under the responsibility of the Extended Data Protection Advisory Committee (<https://tu4u.tugraz.at/go/dsb-e>).

Furthermore, the competence area of the Advisory Committee extends to confidential data without making reference to natural or legal persons, e.g. to data from contracts, work results, etc., and to data from research projects (taking into account the FAIR data principle).

2.1.3. TU GRAZ STATUTE PART DATA PROTECTION POLICY

The TU Graz Statute Part Data Protection Policy is available in TU4U.

2.1.4. COMPANY FRAMEWORK AGREEMENT “ON THE AUTOMATED PROCESSING OF PERSONAL DATA OF STAFF”

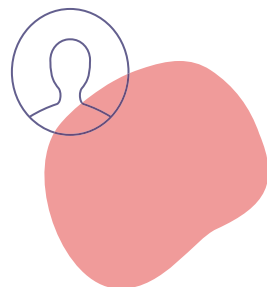
⁷ Federal Act enacted on 14 December 1973 on the Labour Constitution (Labour Constitution Act; in German: - Arbeitsverfassungsgesetz or ArbVG), Federal Law Gazette I 22/1974 as amended by I 115/2022.

In implementing the provisions of the labour and data protection regulations, TU Graz and the Works Councils have adopted a company framework agreement (in the sense of §§ 96, 96a, and 97 ArbVG⁷), which applies to the planning, introduction, use, and modification of existing and

future information and communication systems with reference to staff members' personal data.

2.1.5. APPLICATION REQUEST FOR PERSONAL DATA PROCESSING

To ensure compliance with the legal and internal requirements for existing and future information and communication systems, an application to carry out personal data processing is available. This application is available in TU4U and contains three parts: a general part, a technical part, and a part on the specific technical and organisational measures associated with the ICT system. The applications can be submitted by the applicants to the Data Protection Advisory Committee for Staff after a data protection assessment has been carried out by the Data Protection Coordination Team and the IT Security Team. The application is evaluated by the members of the Staff Data Protection Advisory Committee. Decisions made by this body are made based on resolutions passed by the Rectorate, the Works Councils, and the Service Committees. The completed applications or questions that remain should be submitted in advance to the meeting coordinator (datenschutz@tugraz.at).



2.1.6. TU GRAZ DATA PROTECTION OFFICER

In order to be able to guarantee sufficient neutrality, an external data protection officer, x-tention Informationstechnologie GmbH, Römerstraße 80a, 4600 Wels, was appointed by TU Graz. This appointment was made on 14 May 2018.

The tasks of the external data protection officer are to:

- inform and advise the Rectorate regarding the obligations arising from implementing the GDPR and other data protection regulations;
- monitor and review compliance with the GDPR and other data protection regulations as well as the data protection strategy, including assigning responsibilities, raising awareness, and training staff involved in the operational application;
- review and document reports made to the competent supervisory authority;
- train staff members regarding the obligations arising from the implementation of the GDPR; and
- cooperate with and serve as a contact point for the competent supervisory authority.

2.2. PRINCIPLES AND LEGAL BASES FOR PERSONAL DATA PROCESSING

The Data Protection Coordination Team recommends referring to the following principles when processing data. If these principles are followed, the data processing is generally allowed.

2.2.1. LAWFULNESS, FAIRNESS, TRANSPARENCY

Processing personal data is generally prohibited, unless an exception (legal grounds found in Art. 6 GDPR) to this prohibition exists (“obligation to seek permission”).

To process data fairly, the data subjects must be able to become aware that their data will be processed. This principle prevents the personal data of data subjects from being processed secretly. The principle of transparency is closely related to that of fair processing. Accordingly, data subjects must be informed in plain language and comprehensively that their personal data will be processed (e.g. information must be provided about the scope of the data processing, the identity of the controller, the purposes of the data processing, the rights of the data subjects, etc.).

This information needs to be presented to the data subjects in the form of a privacy statement. Transparency regarding personal data processing can also be established, among other things, by means of providing data protection with technology (privacy by design) and by using data protection-friendly default settings (privacy by default).

The processing is lawful if all the principles (see 2.2.) are applied, and one of the following legal bases exists:

- the data subject has given their voluntary consent to the processing (Art. 6 para. 1 lit. a GDPR) (the consent can be revoked at any time and without giving reasons);

- the processing is necessary for the performance of contract or the application of precontractual measures (Art. 6 para. 1 lit. b GDPR);
- the processing is necessary for compliance with a legal obligation (Art. 6 para. 1 lit. c GDPR);
- the processing is necessary in order to protect the vital interests of the data subject (Art. 6 para. 1 lit. d GDPR);
- the processing is necessary for the performance of a task carried out in the public interest (exercise of official authority) (Art. 6 para. 1 lit. e GDPR);
- the processing is necessary for the purpose of protecting the legitimate interests pursued by the controller or a third party (Art. 6 para. 1 lit. f GDPR).

Detailed information about the legal bases can be found in Art. 6 and Art. 7 GDPR regarding consent.

A template for a declaration of consent (according to Art. 6 para. 1 lit. a GDPR) is available in TU4U, (<https://tu4u.tugraz.at/go/ds-vorlagen>) which should be used exclusively together with a data protection statement. The purposes that are based on the legal basis of consent must be listed in the template for the declaration of consent. These

must correspond to the information in the data protection statement (e.g. consent to receiving sent newsletters; consent to data processing for a specifically designated research project or a specific research area – see 5.). Therefore, the purposes listed in the data protection statement must correspond to those in the consent form.

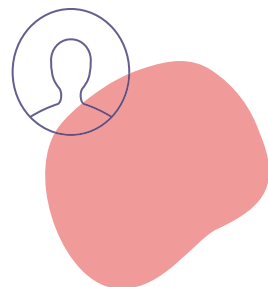
Please note: The declaration of consent is only necessary for purposes for which consent is given in accordance with Art. 6 para. 1 lit. a GDPR. A declaration of consent is NOT necessary for other legal bases! If the processing is based on other legal bases (such as public/legitimate interest, contract, etc., that is not based on consent), it is sufficient to bring the information in the data protection statement to the attention of the data subjects.

2.2.2. PURPOSE LIMITATION

The purposes for collecting personal data and the subsequent data processing must already be defined at the time of data collection. The collection and processing may only be carried out for **specified, clear, and legitimate purposes** (relevant legal basis, no violation of applicable standards). Furthermore, the purpose must be specified in sufficient detail.

The definition of the purpose determines which personal data is truly necessary (Data minimisation – what data is needed to achieve the purpose?) and how long these data may be stored (storage limitation – how long is the data needed?).

Due to these requirements and the controller's obligation to provide evidence, it is recommended



to document the purpose of the data processing in writing in any case (e.g. in the form of the application for personal data processing and/or by including the data processing in the data processing directory).

A defined, clear, and legitimate purpose is often based on legal provisions, contractual agreements, and/or from practical considerations.

Asking the following questions may help to clarify whether there is a sufficient purpose for processing:

- For what purpose is the data processed?
- Is this purpose lawful?
- Is the data to be collected sufficiently well-defined?


If these questions can be answered, there is normally a defined, clear, and legitimate purpose for processing.

2.2.3. DATA MINIMISATION

As already described in the context of data appropriation, only the personal data may be processed that is necessary to achieve the specific purpose. The principle of data minimisation, therefore, complements the principle of data appropriation. If data is also processed that is not urgently needed to achieve the purpose (e.g. data is not related to the processing purpose; the defined purpose cannot be supported by the processed

data, as there are alternative means), this represents a violation of the principle of data minimisation.

It is also always necessary to check whether purpose of the data processing can also be achieved with anonymised data.



Example: Only data that are necessary to achieve a clear and required identification of the data subjects is processed. In this case, no violation of the principle of data minimisation occurs.

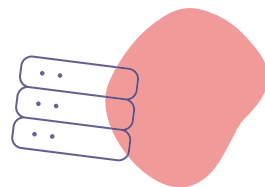
2.2.4. ACCURACY

The personal data processed must be factually accurate (corresponding to reality) and, if necessary, up to date. If the specified processing purpose requires the data to be up to date, this must also be ensured accordingly (e.g. data for access authorisations).

2.2.5. STORAGE LIMITATION

The principle of storage limitation states that data subjects may only identified for as long as necessary to achieve the specified purpose of the processing. If the purpose of the data processing no longer requires the storage of the data, these must be deleted. Thus, a time limitation for processing personal data exists. It should be ensured that deadlines for the deletion of data are defined and that regular reviews take place.

Whether legal retention periods or a specific processing purpose exist can often be clarified by



referring to the respective material laws (e.g. the *Bundesabgabenordnung* (BAO or Austrian Federal Tax Code), *Universitätsgesetz* 2002 (UG or Universities Act), or *Bildungsdokumentationsgesetz* 2020 (BilDokG 2020 or Education Documentation Act). To clarify any time limitations, it is recommended to contact the responsible department.



Example: If a data set includes information that enables the identification of a person, and some data that can be used to identify the person is no longer needed to fulfil the specified processing purpose, the reference to the data subject must be removed. This means that the identifying characteristics must be deleted from the data set. If the data is available in a pseudonymised form, therefore, it may be sufficient to simply delete the allocation lists.

2.2.6. INTEGRITY AND CONFIDENTIALITY

The security of the personal data processed must be ensured at all times. The data must be protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage by taking appropriate technical and organisational measures (TOM – state-of-the-art technical and organisational measures) (e.g. authorisations, admission control, access control, recoverability).

2.2.7. ACCOUNTABILITY

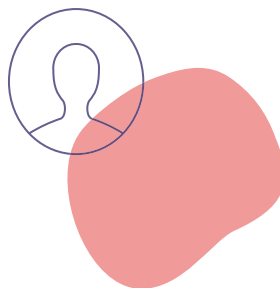
The controller is obliged to comply with the principles described above and must also be able to

prove this compliance (e.g. in the event of an audit by the data protection authority, in legal proceedings). Written documentation includes documentation in the form of the processing directory, of the principles, and of appropriate technical and organisational measures.

2.2.8. DATA PROTECTION INFORMATION

The controller is required to inform the data subjects about the processing of personal data. The information that should be provided is listed in Art. 13 and 14 GDPR and includes the following:


- Name and contact details of the responsible person
- Contact details of the data protection officer
- Information about the categories of data processed (e.g. staff, students) and type of personal data (e.g. first name, surname, title, address, IP address;)
- Legal basis and purpose of processing
- Information about any recipients (recipients should be defined as specific as possible) or information about the data transfer to a third country (outside the EU/EEA)
- Information about the storage period (specific time limitations or criteria for determining the storage period)



- Rights of the data subjects
- Right of the data subject to appeal to the competent supervisory authority (in Austria, this is the Austrian Data Protection Authority)

Templates with the descriptions of the required information that can be individually adapted can be downloaded from TU4U. Once they have been adapted, these can be used as data protection statements for a wide range of data processing activities, such as events, newsletters, excursions, and surveys.

2.2.9. RIGHTS OF THE DATA SUBJECTS



Data subjects have certain rights under the data protection regulation which they can exercise towards the data controller. In principle, the rights of the data subject can be communicated informally or as part of the internal process. If data subjects contact an OU of TU Graz directly, they are asked to forward their requests to datenschutz@tugraz.at, as stated on the official website (<https://security.tugraz.at/datenschutz/dsgvo/rechte/welcome.en.shtml>). TU Graz is legally obliged to respond to requests from the data subject within a **period of one month**. Data subjects have the following rights:

- **Right to be informed and right of access to the data processed**
The former right enables the data subject to request information about the personal data (and, in particular, about the purpose of processing, categories of data, and

recipients). If this request interferes with the rights of third parties, is excessive, or manifestly unfounded, we may refuse to provide the information or demand the reimbursement of costs. Regarding the latter right, the information will be provided within one month of filing the request, whereby a justified extension of the deadline is possible.

■ **Right to rectification of the data**

This right enables the data subject to request the rectification of inaccurate or incomplete data concerning them.

■ **Right to restrict data processing**

This right enables the data subject to restrict processing:

- for the duration of the period in which the disputed accuracy of the data is determined;
- for the duration of period in which the overriding legitimate/public interest is examined if an objection is raised; or
- in the event of unlawful processing, if the Data subject does not wish the data to be erased.

■ **Right to data portability**

This right enables the data subject to obtain and reuse data they personally have given to TU Graz, and which is processed by TU Graz with automated systems on the basis of consent or to fulfil a contract concluded with the data subject. The rights and freedoms of third parties must not be affected by this.



■ Right to erasure

The right enables the data subject to have personal data erased:

- if the data is no longer necessary for the purposes for which they were processed;
- if the consent on which the processing is based is withdrawn, and no other legal basis for the processing exists;
- if an objection to the processing is raised, and no legitimate grounds for processing exist;
- if the processing of the personal data is unlawful; or
- if the deletion of the personal data is performed to fulfil legal obligations.

■ Right to object to data processing

This right enables the data subject to object to the processing of their personal data because of specific circumstances. Based on these circumstances, the data subject can object at any time to the processing of personal data, when this processing is carried out to fulfil legitimate or public interests.

■ Right of revoke consent to data processing:

The revocation of this right, however, does not affect the lawfulness of the processing that was carried out up until the consent is revoked. This right can be exercised at any time and without justification (only applicable where a legal basis for consent exists).

2.2.10. INFORMATION SECURITY

In addition to the legal components, ensuring the security of the information is a central aspect of data protection (e.g. Art. 32 GDPR). The scope of application extends beyond the processing of personal data and also includes non-personal data. Ensuring the confidentiality, integrity, and availability of data is of central importance. In addition, Art. 25 GDPR must be observed, which provides standards for considering privacy by design (i.e. data protection through technical design) and privacy by default (i.e. data protection through user-friendly default settings) when processing personal data.

Please refer to the guidelines for ensuring data security at TU Graz. More information on this topic is available at <https://security.tugraz.at/informationssicherheit/policy/>.

2.2.11. DATA PROTECTION INCIDENT/ DATA BREACH

A data breach or data protection incident occurs when there is a violation of the protection of personal data processed in the course of activities carried out at TU Graz (student contact data, examination data, data of people participating in events, data of staff members, etc.).

Possible scenarios:

- Theft/loss of laptops, storage media (USB sticks), or similar items upon which personal data is stored (regardless of who owns the terminal device/data carrier)

- Breaking into premises and stealing documents containing personal data
- Sending an e-mail to several persons in the CC without having a clear, defined, and legitimate purpose for placing these people in CC
- Hacker attack
- Login by a foreign/unauthorised person to access an account.

As soon as a (possible) data breach has been recognised, it must be reported immediately to databreach@tugraz.at or via the online form (<https://security.tugraz.at/datenschutz/dsgvo/databreach/>), providing all known information. If there is any uncertainty regarding whether a relevant incident has occurred, it is still recommended to file an internal report.

**Tip: Better to report once too often
than once too little.**

Immediate reporting is extremely important, as TU Graz must **report** a potential incident to **the data protection authority within 72 hours** (the deadline is not suspended on weekends or public holidays). In this period, an internal evaluation of the incident will be carried out by the Data Protection Coordination Team, the IT Security Team, and the data protection officer. During this process, an examination can be carried out to determine whether the

incident poses a risk to the rights and freedom of the people concerned and thus whether TU Graz is actually obliged to report the incident to the Austrian Data Protection Authority.

Further information is available at <https://security.tugraz.at/datenschutz/dsgvo/databreach/>.

2.2.12. PROCESSING DIRECTORY (PROVENTOR TOOL)

Controllers and processors are legally required to keep a data processing directory (in German: *Verarbeitungsverzeichnis* or *VVZ*) (Art. 30 GDPR). The VVZ provides an overview of all activities carried out for personal data processing.

In this way, TU Graz ensures that it is accountable to the supervising authority, which can then – if a complaint is filed or as a result of an ex officio action – exercise its right to perform data controlling. At TU Graz, the “PROVENTOR” tool is used to document the processing procedures. Entries are made at the process level. The central organisational units have access to this tool, and the entries made should be evaluated by the organisational units on an ongoing basis and updated accordingly if changes are made.

Further information about the VVZ can be found at <https://tu4u.tugraz.at/go/vvz>.



2.2.13. DATA PROTECTION IMPACT ASSESSMENT

⁸ Ordinance of the Data Protection Authority on processing operations for which a data protection impact assessment should be carried out (in German: *Datenschutz-Folgenabschätzung-Verordnung* or *DSFA-V*), BGBl. II, No. 278/2018.

⁹ Data Protection Impact Assessment Exemption Ordinance (in German: *Datenschutz-Folgenabschätzung-Ausnahmenverordnung* or *DSFA-AV*), BGBl. II No. 108/2018.

If processing personal data is likely to pose a high risk to the rights and freedom of data subjects, data controllers and processors are legally required to carry out a data protection impact assessment (DPIA) (Art. 35 GDPR). The Austrian Data Protection Authority has issued two regulations in this context, namely the “Blacklist-VO”⁸ and the “Whitelist-VO”⁹. While the blacklist outlines processing operations for which a DPA must be carried out in any case (e.g. when using new technologies), the whitelist contains a catalogue of exceptions for processing operations for which a DPA is not required (e.g. for processing research data).



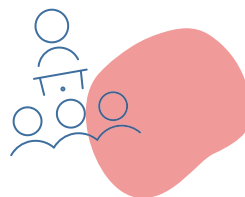
© Kinn Studio – AdobeStock

3. Teaching

3.1. FULFILMENT OF THE REQUIREMENT TO INFORM STUDENTS

The requirement to inform students is fulfilled during admission or through the collected data protection declarations on the OU Registrar's Office website (<https://www.tugraz.at/en/tu-graz/organisational-structure/service-departments-and-staff-units/registrars-office/>). In addition, information about data protection is provided in individual cases before the specific tools are used (e.g. TeachCenter).

If personal data of students will be processed in ways that are not covered in the general data protection declarations (e.g. photos taken during excursions in courses), it is recommended to inform the students in advance or, if these will be published via external media, to obtain their voluntary consent according to Art. 6 GDPR. To publish data on social media platforms, the voluntary consent of the student(s) is required in accordance with Art. 49 GDPR. The information can be provided by using the templates available in TU4U (<https://tu4u.tugraz.at/go/ds-vorlagen>) and can be implemented, e.g. in the TeachCenter.



3.2. RETENTION PERIODS FOR TEACHING PURPOSES

Please refer to the information provided in the booklet: Teaching at the TU Graz¹⁰.

¹⁰ TU Graz,
Vice Rectorate for
Academic Affairs,
BOOKLET: TEACHING
AT TU GRAZ (2021)
69 (70).

3.2.1. ASSESSMENT DOCUMENTS

¹¹ *Federal Act on the Organisation of the University and its Studies (Universities Act 2002 - UG), BGBl I 120/2002 idF I 177/2021.*

¹² *Statute Part Legal Regulations for Academic Affairs at TU Graz, SA 92000 STSR 124-03, § 22 para. 4.*

¹³ *TU Graz, Vice Rectorate for Academic Affairs, BOOKLET: TEACHING AT TU GRAZ (2021) 80 (81).*

¹⁴ *Statute Part Plagiarism at TU Graz, SA 91000 PLAG 150-02, § 2; Statute Part Legal Regulations for Academic Affairs at TU Graz, SA 92000 STSR 124-03, § 22.*

¹⁵ *Federal Act on Documentation in Education (Education Documentation Act 2020 - BilDokG 2020), BGBl I 20/2021 idF I 227/2022.*

Assessment documents (particularly, corrections of written examinations and examination papers) must be kept for at least six months and for a maximum of one year, unless they are handed back to the students (§ 79 para. 5 UG¹¹, Statute Part on Legal Regulations for Academic Affairs¹²). The examination record must also be kept for at least six months. This usually remains with the examiners themselves and contains information about the subject of the examination, the exam location or format, and the beginning/end times of the examination, the names of the examiner or the names of the members of the examination committee, the names of the students, the questions asked, the assessments given, the reasons for the negative assessment, and any special incidents.

3.2.2. BACHELOR THESES, SEMINAR PAPERS

In order to detect academic misconduct, bachelor's¹³ theses and seminar papers may be stored to examine these for evidence of plagiarism by using electronic means beyond the time limitations specified for the retention of assessment documents¹⁴.

3.2.3. RETENTION OF UNIVERSITY SPECIFIC DATA (EXAMINATION DATA)

The BilDokG¹⁵ lists those personal data of students that is necessary to collect for keeping records, such as the matriculation number, name,

date of birth, nationality, gender, home address, or e-mail address.¹⁶

¹⁶ § 9 BilDokG 2020.

According to the UG, the examination data must be kept in an appropriate form for at least 80 years. The following data is included:¹⁷

¹⁷ § 53 UG in conjunction with § 9 line 15 BilDokG 2020.

- 1.) Designation of examinations or the subject of scientific or artistic work
- 2.) The ECTS credits awarded
- 3.) The assessment
- 4.) The names of the examining or assessing persons
- 5.) The date of the examination or assessment
- 6.) The name and matriculation number of the student
- 7.) University Entrance Qualification Examination
- 8.) Dates of the aptitude test or admission and selection procedure

In compliance with this legal requirement, the aforementioned data is stored centrally by TU Graz by using the information and administration system TUGRAZonline.



3.2.4. ROOM ASSIGNMENTS

Basically, room assignments contain personal data in most cases (e.g. matriculation number), which is why the associated data processing falls within the scope of the application of the GDPR and the Data Protection Act. Therefore, it is recommended that room assignments be made in a digital form insofar as technically possible, whereby the principles of privacy by design and privacy by default should be observed (see 2.2.10.). It is not recommended to publish room assignment.

3.3. DATA PUBLISHED IN THE CONTEXT OF ORAL (FINAL) EXAMINATIONS

The UG as well as the Statute Part Legal Regulations for Academic Affairs at TU Graz stipulate that oral (final) examinations need to take place publicly as a matter of principle. This regulation aims to ensure that a certain level of objectivity is maintained and that a check-and-balance system exists regarding examination decisions (purpose of the provision)¹⁸. Therefore, there are no grounds for objection to a public announcement of the examination result in the context of oral examinations from a data protection perspective.

¹⁸ Vcf. BOOKLET:
TEACHING AT
TU GRAZ, 66.

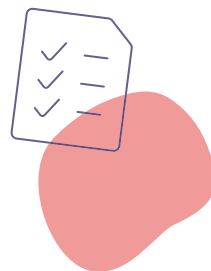
If a defined, clear, and legitimate purpose is not specified, the publication of the **names** of examination candidates (e.g. through public posting) is not recommended from a data protection perspective.

3.4. DATA PUBLISHED IN THE CONTEXT OF WRITTEN EXAMINATIONS

Examination results for written examinations can only be made accessible to the specific person examined. Therefore, the publication of examination results in combination with, e.g. the name/matriculation number should be avoided. Publishing examination results in the TU Graz TeachCenter (i.e. accessible to all participants) or sending lists of examination results (e.g. in the form of a PDF) violates the data protection regulation.

3.5. SIGNATURE LISTS AND ATTENDANCE LISTS

In courses with compulsory attendance, students' attendance must be proven and documented. There are no grounds for objection to the use of signature or attendance lists that fulfil this purpose from a data protection perspective. However, please note that only relevant data should be collected, and the list should be deleted after six months at the earliest or one year at the latest (see storage limitations for assessment documents).



3.6. PHOTOS AND VIDEOS TAKEN IN THE CONTEXT OF COURSES/EXCURSIONS

If you would like to take photos and/or videos in individual cases during a course or excursion,

please make sure – as explained in more detail under the item Events (see 5.3.) - that the following essential points are observed: Inform the people concerned (usually students) that photos and/or videos will be taken; whether and where they will be published; that they have a right to object to data use or processing, and that they should exercise this right ideally before the course/excursion takes place by letting the course/excursion head know that they do not wish to be photographed and/or filmed.

It is recommended that you fulfil the requirement to inform your students by means of issuing your own data protection declaration as early as possible. You can find a template for this in TU4U titled “Privacy Policy for Excursions” (in German: *Datenschutzerklärung für Exkursionen*).

If you wish to share photos and/or videos of students with external parties or publish them on social media channels, it is necessary to obtain the voluntary consent of the students ahead of time.

3.7. SENDING INTERIM RESULTS

Interim results can be sent out by using the program “Serienbrief” (mail merge). More information about the technical procedure can be found at <https://bigmail.tugraz.at/verteiler/faq.shtml>.

3.8. HOMEWORK/INSPECTIONS

Please refer to the information found in the booklet: Teaching at TU Graz¹⁹.

¹⁹ BOOKLET: TEACHING AT TU GRAZ, 69.

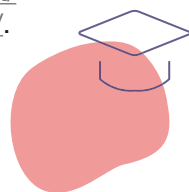
The inspections should be made in such a way that the information is only made available or communicated to the students concerned. It is also advisable to have a lockable post box or a letter box located at the secretary's office where the students can hand in their homework.

3.9. DATA PROTECTION AND CONFIDENTIALITY REQUIREMENT FOR THESES

If theses will be reviewed by external experts, it is recommended that a data protection and confidentiality agreement be concluded between the involved parties.

For example, if the dissertation will be submitted to external reviewers by staff in the dean's office or the institute, the reviewers should submit a data protection and confidentiality agreement that should be signed prior to the submission. If the dissertation is submitted to the reviewers independently by the dissertation candidate, it is advisable to inform them of their obligation to submit the (signed) data protection and confidentiality agreement.

More information about this process and a template for the data protection and confidentiality agreement that can be used for external reviewers can be found in the TU4U at <https://tu4u.tugraz.at/en/students/finishing-my-studies/doctoral-theses/>.



3.10. DATA PUBLISHED IN THE CONTEXT OF GRADUATION CEREMONIES

In general, the data protection regulation allows for the publication of the names of the participants in graduation ceremonies as well as the reading out loud of certain data, such as the birth date or graduation date. However, it is recommended to inform the students that this data will be read out loud when they register for the graduation ceremony by means of a short data privacy declaration. You can request a template by sending an e-mail to datenschutz@tugraz.at. In this case, obtaining the consent of the participants is not required.

If personal data is passed on to external parties (e.g. newspapers, other universities) with respect to graduation or graduation ceremonies, the voluntary consent of the graduates must be obtained in advance.

3.11. VIRTUAL TEACHING

Guidelines for handling personal data collected in the context of virtual teaching can be found in Section IV of the TU Graz Statutes.

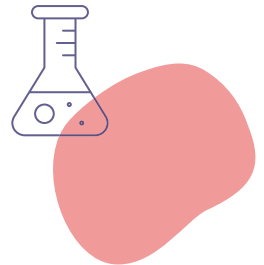


4. Research

4.1. DATA PROTECTION IN RESEARCH

Data plays a central role in research. The legal provisions to be observed in a specific research project depend first of all on whether the data processed is personal or non-personal data (see 1.2.). Non-personal data or anonymous data does not (or no longer) allow conclusions to be drawn about a natural person; therefore, it does not fall under the provisions of the GDPR. Nevertheless, in this case, we recommend checking whether certain other legal provisions must be observed and, if so, which ones (e.g. law, regulation, contract, or directive). If personal data will be processed, the GDPR rules need to be applied to the specific research project. The same applies to mixed data sets, i.e. when personal and non-personal data is inextricably associated with one another. In the research context, two groups of personal data can be distinguished, namely:

- 1.) those processed for the administration of a research project (e.g. timesheets, accounts, payroll accounts, service contracts, which are referred to as “administrative research data”) and
- 2.) those that are the subject of the scientific research project (e.g. subject data, results, publications, which are referred to as “substantive research data”).



4.2. DISTRIBUTION OF ROLES

In the context of processing data collected in the context of research, the GDPR basically distinguishes three different roles, each of which has different legal obligations:

1.) The data controller is anyone who determines the purposes (the “why”) and the means (the “how”) of the data processing. If researchers – and thus TU Graz – make decisions regarding the direction, conception, goal, and topic of a research project, as well as the (allocation of) funding or subsidies, TU Graz should be seen as the data controller in the sense of the GDPR. Accordingly, it must ensure compliance with the legal bases of the processing and the requirement to inform data subjects, as well as ensure that the rights of data subjects are respected.

2.) A data processor is anyone who processes personal data on behalf of and based on the instructions of the data controller. On the one hand, if TU Graz commissions a company to perform a service in a research project, the company acts as a data processor for TU Graz. On the other hand, if TU Graz is commissioned by a company to perform a service, it serves as a data processor for the company. In these cases, a data processing agreement should be concluded according to Art. 28 GDPR (see the German and English templates in TU4U at <https://tu4u.tugraz.at/go/ds-forschung>).

3.) Joint responsibility exists if two or more controllers jointly determine the purposes and means of the processing of personal data (i.e. joint controllers). Thus, if two universities (e.g. TU Graz



and University of Graz) make decisions about the orientation and funding in a joint research project, they assume joint responsibility. In this case, it is advisable to conclude an agreement regarding the joint responsibility in accordance with Art. 26 GDPR (see the German and English templates in TU4U at <https://tu4u.tugraz.at/go/ds-forschung>).

4.3. LEGAL BASES

4.3.1. GENERAL DATA PROTECTION REGULATION (GDPR)

If personal data (administrative and/or content-related research data) is processed in the course of the specific research project, then the legal provisions of the GDPR as well as those of the Data Protection Act (DSG) and the Research Organisation Act (FOG) will always be taken into consideration. Since the processing of personal data is generally prohibited (see 2.2.1.), an exception must first be made. With respect to research data used for administrative, one basis for an exception or the lawfulness of the processing that is listed in Art. 6 GDPR applies.

The GDPR contains a clause that enables exemptions to be made for the purpose of 'academic expression', enabling a balance between the fundamental right to academic freedom and the right to data protection to be found. Therefore, the exception referred to in Art. 89 GDPR, which must always be read together with § 7 of the Data Protection Act, applies to research data, provided that appropriate data security measures are taken (e.g. data access restrictions and encryption).

4.3.2. DATA PROTECTION ACT (DSG)

If the aim of the specific research project is not to obtain personal results, this data may be processed under the DPA in three cases, namely, first, if the data is publicly accessible; second, if the data has already been permissibly obtained for other studies or other purposes; and, third, if the data is pseudonymised data (see 1.6.) and the researchers can no longer establish the personal reference by legally permissible means (§ 7 para. 1 DPA).

If the above-mentioned prerequisites do not apply to the specific research project, the next step that should be taken is to determine whether a special legal provision applies to the specific example of processing (e.g. from the FOG, see 4.3.3.), whether the consent of the data subjects or test persons must be obtained, or, if applicable, whether the approval of the Austrian Data Protection Authority must be gained (§ 7 para. 2 DSG).

4.3.3. RESEARCH ORGANISATION ACT (FOG)

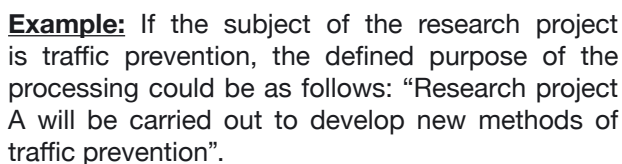
If none of the legal bases listed in § 7 of the Data Protection Act is relevant to the specific research project, § 2d FOG may be considered. This provision states that, in principle, universities may process personal data for research purposes. The prerequisites for this processing are that the data must either be pseudonymised, data may not be published, or data can only be published in an anonymised or a pseudonymised form (§ 2d para. 2 no. 1 FOG).

To find out which legal basis applies to your research project, please contact the Data Protection Coordination Team by sending an e-mail to datenschutz@tugraz.at.

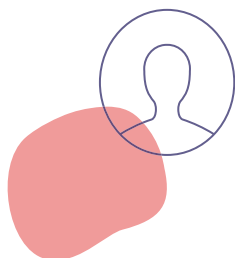
4.4. PRINCIPLES OF THE GDPR

The principles of the GDPR are explained in 2.2., and these must also be generally observed in the research context. At the same time, some "deviations" from the strict GDPR principles are allowed with respect to the processing of research data:

According to the **principle of the purpose limitation**, personal data may only be processed if the purpose defined for this processing is unambiguous and does not violate any legal provisions. Additional processing of personal data is generally possible in the research context (Art. 5 para. 1 lit. b GDPR).



Example: If the subject of the research project is traffic prevention, the defined purpose of the processing could be as follows: "Research project A will be carried out to develop new methods of traffic prevention".




According to the **principle of data minimisation**, only the personal data that is absolutely necessary to achieve the defined purpose may be processed. This results in an evaluation of the purpose on three levels (Art. 89 para. 1 in conjunction with Art. 5 para. 1 lit. c and Art 6. para. 4 GDPR):

Level 1: If the purpose of the specific research project can also be achieved by using non-personal data, only anonymised data should be processed.

Level 2: If the purpose cannot be achieved with anonymised data, an evaluation must be carried out to determine whether the purpose can also be achieved with personal data in a pseudonymised form.

Level 3: Personal data can only be processed in a non-pseudonymised form if the purpose can not be achieved by using either anonymised or pseudonymised data.





Example: The purpose of a specific research project is to develop new methods of traffic prevention. For this reason, 20 project participants fill out questionnaires and take part in test drives on a test site. The purpose cannot be achieved with anonymised data, because the information provided by the participants in the questionnaires is linked to their respective test drives (level 1). Since the purpose cannot be achieved with anonymised data, we recommend documenting the reasons for this. After examining level 2, researchers conclude that the purpose they have defined can be achieved by using pseudonymised data.

For example, the subjects can each be assigned a code, which the researchers write down on a list (e.g. “John Doe” = code 1234/5). On another list, the researchers associate the code with the participant’s respective questionnaire and test drive. This allocation list is stored in an encrypted form to restrict access, so that only the researchers involved in the project or selected staff can identify the personal reference for evaluation purposes. As soon as the researchers no longer need the personal reference, they delete the allocation list. The anonymised data is then made available.

According to the **principle of storage limitation**, personal data may only be stored for as long as it is necessary to achieve the defined purpose of the processing. If the data is processed in the context of research, they may be stored for a longer period of time if appropriate technical and organisational measures are taken, e.g. by restricting data access and encrypting data (Art. 5 para. 1 lit. e GDPR).

4.5. RETENTION PERIODS FOR RESEARCH DATA

The GDPR does not refer to any specific data storage periods, but only provides general principles in this regard (see 2.2.5.). If nothing to the contrary is stipulated in the legal provisions, internal guidelines, or in contracts (e.g. funding agreement, consortium agreement), the following applies:

Administrative research data must be deleted at TU Graz after a maximum period of 15 years.

Content-related research data may also be stored for longer periods due to the exemption clause in the GDPR related to ‘academic expression’, provided that appropriate technical and organisational measures are applied (e.g. access concept). According to the TU’s internal guidelines on safeguarding good scientific practice, “Unless provided otherwise by law, data that form the basis of scientific publications must be preserved and archived securely on durable media in the institution in which they were generated, for at least 10 years, insofar as this is feasible and reasonable.”²⁰

²⁰ TU Graz, Guidelines on Safeguarding Good Scientific Practice, RL 92000 SGWP 050-04, § 4.



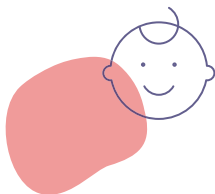
Example: Unless otherwise specified, we recommend deleting administrative research data (i.e. timesheets, accounts, payroll accounts, service contracts) 15 years after the specific research project has ended. Content-related research data – in the above example, this would be the completed questionnaires, evaluations, allocation lists, records of the test drives for the participants, their consent forms and information, etc. – should be stored for at least 10 years as proof of good scientific practice, insofar as this is feasible and reasonable.

4.6. PROCESSING OF CHILDREN'S PERSONAL DATA

The processing of personal data of minors (children up to the age of 14) is only lawful if the responsible parent(s) or guardian provides their consent to the data processing (Art. 8 GDPR in conjunction with § 4 DSG). Minors who have reached the legal age (children over the age of 14) can consent to data processing themselves. However, these age limits only refer to the data protection regulation, which is why they do not, for example, apply to underlying contractual relationships. In this case, the legal norms of Austrian civil law continue to apply regarding the legal capacity or capacity of insight and judgement.

In order to obtain the consent of the responsible parent(s) or guardian, the controller must make reasonable efforts, insofar as the available technology allows, to ensure that their consent has actually been given (e.g. in the online context, authentication by the electronic signature of the parent(s) or guardian; confirmation link sent to the e-mail address of the parent(s) or guardian).

In this context, information about data protection (see 2.2.8.) that will be provided to data subjects should be prepared and formulated by the controller using simple and comprehensible language and, insofar as possible, in a child-friendly manner (Art.12 para. 1 GDPR).



4.7. RECOMMENDED PROCEDURE

4.7.1. CLARIFICATION OF THE ORGANISATIONAL AND LEGAL FRAMEWORK

If your research project touches on aspects relevant to labour law (e.g. because TU Graz staff members will participate as test persons), we recommend contacting the **Vice Rector for Human Resources and Finance** to seek clarification. To clarify general legal matters (e.g. civil law, insurance), please contact the **OU Legal Matters and Insurance Management**.

4.7.2. CLARIFICATION OF IMPLICATIONS OF THE DATA PROTECTION REGULATION

If your planned research project involves the processing of personal data (see 1.2.), please contact the **Data Protection Coordination Team** by sending an e-mail to datenschutz@tugraz.at.



© Kinn Studio – AdobeStock

5. Administration

5.1. INTRODUCTION

The instructions for taking action and procedures when carrying out various administrative activities are described in the TU4U sections for the responsible departments or in the internal guidelines and regulations. The processes described there generally comply with the provisions of the data protection regulation (e.g. accounting for business trips, travel expenses for guest lecturers, short-term sick leave, archiving).

TU Graz staff can find a short and compact information sheet covering some important points of data protection and data security In TU4U (<https://tu4u.tugraz.at/bedienstete/organisation-und-administration/datenschutz-und-datensicherheit/forschung-lehre-und-verwaltung/verwaltung/datenschutz-informationsblatt-fuer-arbeitnehmerinnen>).

5.2. STAFF

5.2.1. APPLICATIONS

The HR department informs applicants about the processing of personal data that takes place during the application procedure in its data protection policy.

Personal data provided on an application are automatically deleted or anonymised in the system



seven months after the application procedure has been completion. Application data in a physical form must be destroyed in accordance with this deadline and in compliance with the data protection regulation. Storing data for a longer period is only possible if the prior voluntary consent of the applicant is obtained for the purpose of keeping records (18 months).

Why should application data be kept for seven months?

Applicants may assert claims under § 29 para. 1 of the Equal Treatment Act (in German: *Gleichbehandlungsgesetz* or *GlBG*)²¹ (violation of the principle of equal treatment on the grounds of ethnic background, religious beliefs, age, or sexual orientation) in court within a period of six months. The application documents, therefore, need to be kept to provide evidence. The seven-month period is designated to account for extra time needed for the physical or postal delivery of this evidence during the judicial assertion of claims.

²¹ Federal Equal Treatment Act (*Gleichbehandlungsgesetz – GlBG*), BGBl I 66/2004 idF I 16/2020.

5.2.2. UNSOLICITED APPLICATIONS/KEEPING RECORDS OF APPLICATIONS

Regarding unsolicited applications that are not relevant, their immediate deletion is generally recommended.

Unsolicited applications that are considered as relevant or application documents used in an ongoing application process that are of interest for future positions can be kept for the purpose of record keeping, if the consent of the applicant is obtained. After the agreed-upon period has

expired, it is advisable to obtain a new consent to either keep the records or to delete the application data.

5.2.3. DATA PROTECTION INFORMATION FOR (NEW) STAFF MEMBERS

(New) staff members are informed about the processing of personal data in the employment relationship when they begin their employment. The data protection policy for (new) staff members at TU Graz is available in the TU4U section of the Human Resources Department.

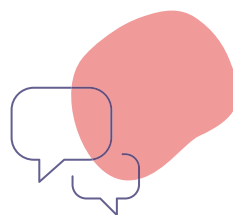
5.2.4. BIRTHDAY CALENDAR

Keeping digital and analogue birthday calendars is generally not recommended.

5.2.5. STAFF APPRAISALS

The minutes of the staff appraisals can be kept for two to three years. This should make it possible for the participants to retrospectively view the goals that have been discussed and the agreements that have been made. The steps agreed upon in previous years can thus be evaluated in the annual staff appraisals.

The content of the conversation is confidential; therefore, this content should only be known to the parties who have conducted the conversation (manager and the respective staff member). Therefore, it is not recommended to store any related



documents centrally in the secretary's office. Similarly, these can be kept in a paper form in locked cabinets in the manager's or staff member's office space. These can also be scanned by staff and kept in a digital form, then stored in the cloud and shared with the manager. Another option would be to store the documentation on a personal hard drive.

5.2.6. OBLIGATIONS OF SECRECY

Staff and employee-like persons who process personal data as part their professional employment are obliged by the employer to maintain the secrecy of such data (unless such secrecy already exists by law). As a rule, staff and employee-like persons are obliged to maintain data secrecy according to § 6 of the Data Protection Act in their employment or service contracts.

If there is any doubt as to whether a person is bound to secrecy by such a clause, it is recommended to clarify the matter with the Human Resources Department.

5.2.7. RETENTION OF PERSONAL STAFF DATA

In general, personnel files are kept in the OU Human Resources, and no personnel files should be kept in decentralised locations, such as at the institutes or other OUs.

This does not include two types of documents that are to be managed in decentralised locations:

- 1.) Original travel receipts
(storage limitation period
of seven years), and
- 2.) Employment contracts
for project staff
(the storage limitation period
depends on the guidelines or
contractual agreements with
the respective funding bodies).

5.2.8. PUBLISHING DATA OF FORMER STAFF MEMBERS ON THE (INSTITUTE'S) WEBSITE

Due to the provisions of the data protection regulation, it is recommended that consent be obtained when the personal data of former staff members will be processed (with the exception of former heads of staff and people cited in the context of historical reports or outstanding achievements).

Since TU Graz must prove the existence of consent if any doubt exists, it is recommended to obtain this consent in writing. In order to make it easier to obtain the written consent, the Data Protection Coordination Team will provide a template that can be used for the consent and the accompanying data protection declaration upon request.



5.2.9. PROCESSING OF CHILDREN'S PERSONAL DATA

See 4.6.

5.2.10. VIDEO SURVEILLANCE

Legal questions regarding video surveillance basically touch on aspects of labour law; therefore, these should be clarified in advance with the Vice Rector for Human Resources.

In addition to labour law, the data protection law must also be observed, which is why a comprehensive list of recommendations for taking action with respect to data protection issues related to video systems is available for download at TU4U (<https://tu4u.tugraz.at/go/videoueberwachung>).

5.3. EVENTS AND PUBLIC RELATIONS

5.3.1. EVENTS

Several data protection issues arise in connection with events. Questions that arise include how to deal with registration and attendance lists or whether photos of participants/speakers can be taken and published. TU4U (<https://tu4u.tugraz.at/go/datenschutz-bei-veranstaltungen>) provides a comprehensive list of recommendations regarding data protection and copyright issues associated with events.

In addition, various templates for data protection declarations and information signs for photo taking and/or video recording are available for download.

5.3.2. WEBSITES

FAQs about legal issues associated with websites are available in TU4U (<https://tu4u.tugraz.at/go/webseitenerstellung-recht>) These serve as recommendations for the creation and maintenance of websites at TU Graz.

5.3.3. SOCIAL MEDIA (FACEBOOK, INSTAGRAM, X, LINKEDIN, ETC.)

According to the current legal situation, the publication of personal data (first and last name, photographs, etc.) on the TU Graz social media channels is generally only permitted after obtaining the explicit consent of involved parties according to Art. 49 GDPR. In this case, the consent is required for the transfer of data to a non-secure third country (USA)²².

²² ECJ 16.06.2020,
C-311/18 (Schrems II).

A template for the declaration of consent as well as for the data protection declaration can be downloaded from TU4U (<https://tu4u.tugraz.at/go/ds-vorlagen>).




5.4. HANDLING CONTACT DETAILS

5.4.1. CONTACT DATABASES

While maintaining contact databases, the principles mentioned above must be observed. For this purpose, consistent maintenance of these databases is recommended, which particularly ensures that:

- the contact details are processed lawfully and transparently (duty to inform – data protection policy);
- contact details that have already been collected or are being newly collected are only processed for the purposes for which they were/are being collected (consistency between the information in the data protection declaration and the actual processing purposes);
- only the data is processed (e.g. recorded) that is absolutely necessary to achieve the purpose;
- the accuracy and timeliness of the data is ensured at all times;
- technical and organisational measures have been taken which correspond to the state of the art and ensure data security; and
- the rights of the data subjects can be safeguarded at any time and thus mailings, e.g. after consent is revoked, can no longer be made.





Examples: The purpose limitation does not apply if you send research partners – whose contact data you have collected for the purpose of networking and professional exchange as part of the research – invitations to association events that have no connection with the research activity.

5.4.2. SENDING INVITATIONS AND NEWSLETTERS

To send invitations and newsletters per e-mail, it is strictly necessary to put the receiving persons in BCC (Blind Carbon Copy)²³. Contact databases must be maintained to ensure that the data is up to date, taking into account undeliverable messages (by post or by e-mail).

²³ DSB 11.05.2020, 2020-0.288.477 (open mailing list).

The receiving persons must be given the opportunity to unsubscribe from mailings sent by TU Graz or to request the deletion of their data from the contact databases maintained by TU Graz. These requirements can be met by including an unsubscribe button or a corresponding (e-mail) address in every electronic or postal message, whereby the person can easily unsubscribe by using the address.

In compliance with the principles of the GDPR, for example, it is possible to send invitations to events to contacts who have already participated in the same or a similar event (e.g. same research topic) or who have given their consent to receive event invitations or newsletters from TU Graz (§ 174 TKG 2021²⁴).

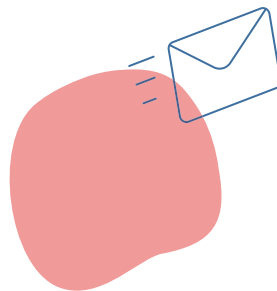
²⁴ Federal Telecommunications Act (in German: Telekommunikationsgesetz 2021 – TKG 2021), BGBl I 190/2021 idF I 180/2022.

5.4.3. WRITING TO NEW CONTACTS

If you plan to contact a natural or legal person who has been identified through internet research, attention should be paid to the purpose for which the natural or legal person has published their contact data on the internet. If this purpose is compatible with the purpose of contacting the person, it is generally possible to contact the person by citing the source of the data (e.g. company website). Depending on the individual case, it is necessary to subsequently ensure that the duty to inform is fulfilled, and the principles are observed.

5.4.4. COMMUNICATION WITH TU GRAZ STAFF AND STUDENTS

In order to communicate with TU Graz staff and students, it is recommended to use only the TU Graz e-mail address available for this purpose (both sender and recipient).



6. Archive Material

If the data are archival material, e.g. according to the Federal Archives Act (in German: *Bundesarchivgesetz*)²⁵, the Federal Archives Ordinance (in German: *Bundesarchivgutverordnung*)²⁶, or the TU Graz archive regulations, a legal basis exists that potentially legitimises the storage of the personal data. The storage according to these legal provisions would also be a clear, defined, and legitimate purpose according to the GDPR, which corresponds to the data protection regulation provision on storage limitation (see 2.2.5.). More detailed information about the storage of documents in the archive is available in the TU4U section of the relevant department.

²⁵ Federal Act on the Protection, Preservation, and Use of Federal Archival Records (Federal Archives Act), BGBl I 162/199 idF I 32/2018.

²⁶ Ordinance of the Federal Chancellor on the Marking, Offering, and Archiving of Federal Written Records (Federal Archives Ordinance), BGBl II 367/2002 idF II 305/2017.



7. Contact Details

Data Protection Officer

x-tention Informationstechnologie GmbH
Römerstraße 80A
4600 Wels
datenschutzbeauftragter@tugraz.at

Data Protection Coordination Team

Mag.iur. Daniel Kurzmann, BA MA LL.M.
datenschutz@tugraz.at
+43 316 873 - 6003

Mag.iur. Christof Plaschke
datenschutz@tugraz.at
+43 316 873 - 6047

Anna-Maria Henögl
(Data Processing Directory)
datenschutz@tugraz.at
+43 316 873 - 6067

IT Security Team

DI Reinfried O. Peter, MSc

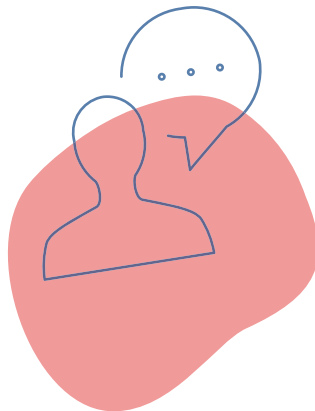
it-security@tugraz.at

+43 316 873 - 6390

Mag.iur. Marcel Schudi

it-security@tugraz.at

+43 316 873 - 7697



8. Selected Links

Templates for data protection declarations, an authorisation to use works, and a declaration of consent according to Art. 49 para. 1 lit. a GDPR
<https://tu4u.tugraz.at/go/ds-vorlagen>

Booklet: Teaching at TU Graz. Questions and Answers about Legal Matters Related to Teaching at TU Graz
<https://tu4u.tugraz.at/bedienstete/lehre/booklet-lehre-an-der-tu-graz/>

Data protection and obligation of secrecy for external reviewers of dissertations
https://tu4u.tugraz.at/fileadmin/Studierende_und_Bedienstete/D-E_Formulare_Forms/Datenschutz-und_Geheimhaltungsverpflichtung_Diss_Externe.pdf

Declaration of consent according to Art. 6 para. 1 lit. a GDPR
<https://tu4u.tugraz.at/go/ds-vorlagen>

TU Graz Statute Part Data Protection Policy
https://tu4u.tugraz.at/fileadmin/public/Studierende_und_Bedienstete/Satzung_und_Geschaeftsordnungen_der_TU_Graz/Datenschutzordnung_Satzungsteil_7.8.2019.pdf

Company framework agreement for the automated processing of personal data of staff
https://tu4u.tugraz.at/fileadmin/user_upload/redaktion/Betriebsvereinbarungen/Datenschutz_Rahmenbetriebsvereinbarung.pdf

Video surveillance and recording systems at TU Graz
<https://tu4u.tugraz.at/go/videoueberwachung>

Information sheet for TU Graz staff about information security and data protection
<https://tu4u.tugraz.at/bedienstete/organisation-und-administration/datenschutz-und-datensicherheit/forschung-lehre-und-verwaltung/verwaltung/datenschutz-informationsblatt-fuer-arbeitnehmerinnen>

Request to perform the processing of personal data
<https://tu4u.tugraz.at/bedienstete/organisation-und-administration/datenschutz-und-datensicherheit/forschung-lehre-und-verwaltung/verwaltung/antrag-zum-einsatz-einer-personenbezogenen-datenverarbeitung/>



