

**Statutes on the collection and processing of personal data
by the University of Konstanz
for the purpose of completing university-specific tasks**

dated 22 February 2022

Section I: General provisions

§ 1 Object of the statutes

These statutes regulate the processing of personal data by the University of Konstanz for the purpose of completing university-specific tasks.

§ 2 Reasons for data processing

- (1) The university processes personal data in the context of its statutory duties.
- (2) Involving study, teaching, academic continuing education and the qualification of early career researchers, personal data is processed for the following purposes, in particular:
 1. Student application processes
 2. Study-related processes, in particular,
 - a) The processes for re-registration, applications for a leave of absence, exmatriculation and examinations,
 - b) Course and exam administration,
 3. For admission to and completion of the guest auditor programme,
 4. To maintain ties to the university's graduates,
 5. To conduct doctoral and habilitation procedures,
 6. To provide advice/consultation, especially student advisory services, social services, equal opportunity and anti-discrimination issues, (doctoral) supervision programmes, as well as consultations with ombudspersons,
 7. To use systems in the context of online teaching, especially e-learning systems,
 8. To use videoconferencing services,
 9. For awarding scholarships,
 10. For working with student university groups.

- (3) The university processes personal data during the administration and completion of research projects.
- (4) In the context of academic self-administration, personal data are processed for the following purposes, in particular:
1. To conduct elections for positions in university bodies,
 2. To fill positions and functions in academic self-administration,
 3. During appointment processes,
 4. In the context of work in university bodies.
- (5) The university also processes personal data for the following purposes, in particular:
1. Accreditation,
 2. The collection of fees and contributions as well as the settlement of payments under private law,
 3. Collaboration with other universities or institutions,
 4. Measures in the context of equal opportunity and participation, anti-discrimination, integration and protection against sexual harassment
 5. Completion of public and non-public events and conferences,
 6. For knowledge, design and technology transfer
 7. Support for founding start-ups,
 8. Preparation of applicants for starting their studies,
 9. Completion of the programme "Schülerstudium" for school students at the university as per § 64 para. 2 LHG (Landeshochschulgesetz – state law on higher education),
 10. Public relations work,
 11. Implementation of procedures related to academic integrity,
 12. Structure and development plans,
 13. Generation of official university statistics and for internal and external reporting in the context of data-based strategy development, planning, decision-making and controlling processes,
 14. Use of university facilities (e.g. the University Sports Service and the Communication, Information, Media Centre (KIM)),
 15. Implementation of contracts (under public and private law),

16. Awarding of university positions (e.g. professor (apl. Prof.) or honorary professor), awards and honours,
17. Conducting disciplinary proceedings as per § 62a LHG,
18. Regulating permitted behaviour on campus and access to the university ("Hausrecht").

§ 3 Types of data processing

- (1) Personal data are processed in physical and electronic form.
- (2) Mainly written documents are processed physically and stored using suitable technical and organizational means until the retention period ends.
- (3) Data is collected electronically, for example, via web forms, email, upload or scan. This data is processed further and stored electronically using suitable technical and organizational means until the retention period ends.

§ 4 Generated personal data

- (1) The university is permitted to generate in particular the following characteristics and identifiers and to assign them to an individual person:
 1. Enrolment number,
 2. Personal university ID number (university ID),
 3. Examination number,
 4. Admission number,
 5. Administrative code,
 6. Account for using the university's IT systems,
 7. University email address,
 8. ID card number.
- (2) When students enrol in an additional programme at the university, then the university is permitted to reassign them the same generated data as per para. 1 as in their first programme, in particular, the enrolment number.
- (3) The account for using the university's IT systems consists of a student's personal university ID number and the corresponding password.

Section II: Basic principles for all processing of personal data

§ 5 Lawfulness, transparency

- (1) Whenever personal data is processed, the fundamental right to protection of personal data and the right to informational self-determination in the European Union must be ensured.
- (2) The respective organizational units at the university conducting data processing must ensure it takes place in a lawful manner, in particular, with justification founded on a legal basis within the meaning of Art. 6 General Data Protection Regulation (GDPR), usually in the form of a legal provision, or, in justified cases, with consent.
- (3) As per Articles 13 and 14 GDPR, the corresponding people must be informed when data is collected. The respective university unit must provide corresponding data protection information.
- (4) If personal data is to be shared with third parties, the relevant university unit must first check whether this is permissible. In addition to this, especially for collaboration with other universities or external institutions (e.g. in the context of (study) programmes) and when using external service providers, it has to be checked if a contract as per Article 26 or Article 28 GDPR has to be concluded. This action must be documented.

§ 6 Limitation to specific purposes

Personal data can only be processed for specified, clear and legitimate purposes, as well as for other compatible ones. In any case, data processing can only take place with a corresponding legal basis or the consent of the respective persons. As required by law, the corresponding university unit must inform the respective persons about the use of their data for other purposes.

§ 7 Minimization of data processing

Before processing personal data, a check is required of whether the processing is suitable for achieving the purpose, limited to what is necessary for the purposes of the processing and appropriate after a further overall assessment. Anonymized data must be used if the required effort is proportionate to the purpose and the intended purpose can be achieved. Pseudonymized data must be used in cases where anonymization is impossible, the required effort is proportionate to the purpose and the intended purpose can be achieved. Personal data may not be stored for potential future purposes unless this is required or permitted by law.

§ 8 Accuracy

The personal data must be processed accurately and using up-to-date tools. All reasonable measures must be taken to ensure that incorrect data is deleted or corrected immediately.

§ 9 Limitation of retention period

- (1) The data of applicants who do not afterwards enrol at the university will be deleted by the end of the semester following the semester they submitted their applications.
- (2) The data of students and doctoral researchers will be deleted immediately after their membership in the respective university group ends as per § 10 para. 1 sentence 2 LHG, or, respectively, after their status as affiliated members of the university ends once they receive their doctoral certificates. Deviating from sentence 1, if an examination process (of a performance assessment the student has already registered for) has not yet been completed at this time, the data will only be deleted immediately after this examination process has been completed. The examination process as described in the prior sentence is also considered completed when the respective person has exmatriculated from the university and not continued their studies for a period of three years after the exmatriculation date.
- (3) The data processed for the purpose of maintaining contact with graduates will be deleted 50 years after the exmatriculation date at the latest, unless the respective persons request earlier deletion of this data. The university informs students about the processing of data for these purposes and informs graduates about their right to withdraw consent for such data processing.
- (4) The following data are exempt from the deletion obligation as per para. 2:
 1. Family name, given name(s), birth name, date of birth, place of birth, gender,
 2. Study programme, enrolment number,
 3. Result and date of the final examination including the overall grade, the academic degree and (if applicable) the title of the thesis,
 4. The individual grades the overall grade is calculated from and
 5. Date of enrolment and exmatriculation as well as the reason for exmatriculation, if applicable: date of acceptance as a doctoral researcher and date the doctoral certificate was issued.

The university processes this data for the purpose of validating the documents issued by the university, in particular certificates. The data may also be processed, insofar as this is necessary, for the purpose of revoking a university degree. The

university deletes the data 50 years after the respective person's exmatriculation date or the date their doctoral certificate was issued.

- (5) The data of guest auditors will be deleted after the end of the semester in which they were admitted as guest auditors.
- (6) The data of highly gifted persons as per § 64 para. 2 LHG as well as the data of participants in external students' exams are processed as described in paragraphs 2 and 4.
- (7) The data of external users of university facilities will be deleted immediately after termination of the respective user relationship.
- (8) Unlike in paragraph 2, if former students provide their written or electronic consent, the university can store the following data for a period of 50 years in order to be able to issue replacement documents:
 - 1. Family name, given name(s), birth name, date of birth, place of birth, gender, address, email address,
 - 2. Study programme, enrolment number,
 - 3. Internship semesters, leave of absence semesters, other interruptions,
 - 4. Result and date of the preliminary or intermediate examination,
 - 5. Result and date of the final examination of the study programme including the overall grade and the individual grades the overall grade is calculated from,
 - 6. Date of enrolment and exmatriculation as well as the reason for exmatriculation.

Students will be informed of this option when they enrol and reminded of this fact by their exmatriculation at the latest.

- (9) Written performance assessments, especially written on-campus exams, written assignments, project work and internship reports, including the corresponding evaluations and exam minutes for oral exams, must be kept for at least two years, up to a maximum of five years. The retention period begins at the end of the semester in which the performance assessment was completed. If the results of the performance assessment are contested, the retention period will not end before the corresponding decision has entered into legal effect.
- (10) Bachelor's theses, including the corresponding evaluations, are stored for a period of five years; master's theses, including the corresponding evaluations, are stored for a period of ten years. The retention period begins at the end of the calendar year in which the exmatriculation takes effect. Documents relating to doctoral

examination procedures as per § 19 para. 1 will be stored for 30 years; the retention period begins at the end of the year in which the doctoral certificate was issued.

- (11) Regulations on documentation and storage in examination regulations, in these and other statutes as well as from other laws remain unaffected. If the data to be deleted is relevant for an administrative legal case, it will be deleted immediately only after the corresponding legal decision has gained legal validity. Data that is part of administrative or other legal proceedings must be deleted immediately after the corresponding legal decision has entered into legal effect. Data that has been stored and processed anonymously does not have to be deleted.
- (12) All data, especially data in digital form, must be offered to the corresponding archive before it is deleted.

§ 10 Integrity and confidentiality

- (1) Personal data must be treated confidentially and adequately protected by appropriate technical and organizational measures against unauthorized or unlawful processing and accidental loss, destruction or damage.
- (2) University staff are legally obligated to maintain the confidentiality of data. The university instructs its staff of this obligation, and the Division of Human Resources documents that this instruction has taken place.
- (3) It must be ensured that additional persons involved in the university's processing of personal data are bound to data secrecy or are bound by a comparable legal obligation.

§ 11 Accountability

The university must be able to demonstrate its compliance with §§ 5-10. In particular, the organizational unit responsible for data processing must provide the entry required for the data processing register as per Article 30 of the EU's General Data Protection Regulation (GDPR) to the organizational unit responsible for maintaining this register.

Section III: Particular data processing situations

§ 12 Video communication tools; lecture recordings

- (1) University members and affiliated members use the video communication systems approved by the Rectorate for research, study, teaching, continuing education and academic self-administration purposes. These systems must specifically adhere to

the principle of data protection with regard to their technology design, data protection-friendly default settings and minimization of data processing. Functions of video communication systems that interfere especially intensively with users' general personal rights and right to informational self-determination, in particular attention tracking functions, are not permitted.

- (2) There is no general obligation for participants to activate their audio and video functions during online sessions. However, if this is necessary for conducting a session, especially one that requires the active participation or attendance of students, the organizer(s) can make other arrangements. In this case, it must be documented that participants were informed accordingly before such sessions begin.
- (3) If sessions as per para. 1 sentence 1 are conducted in a hybrid format, the organizer(s) must inform all participants about which audio and video recordings will be made during the event. Participants are only obligated to accept the use of audio and video broadcasts of themselves if these are required for conducting the event; para. 2 sentences 2 and 3 apply. If there is no such obligation, the organizer(s) must provide an option for students to take part in the hybrid event without such use of audio and video broadcasts.
- (4) In-person, online and hybrid events in line with the university's statutory duties as per § 2 LHG can be broadcast to an end device, as long as this is necessary, especially in cases of limited capacity in lecture halls or in order to provide public access to the event(s).
- (5) Sessions as per para. 1 sentence 1 can be recorded in order to fulfil the duties laid out in § 2 LHG, as long as lecturers have consented to lecture recording and technical and organizational measures are taken to reduce the risk of recording the personal data of other participants. In cases where it was not possible to avoid recording the personal data of other participants and the effort to make the person(s) unrecognizable afterwards would be unreasonable, the corresponding parts of the recording can be made available as long as the lecturer has considered the rights of the respective person(s) and concluded that the university's interest in the publication outweighs the respective person(s)' interest in stopping the publication. The lecturers decide, within the framework of the Rectorate's guidelines, how the recordings can be made available and to which group of people.

§ 13 Video-based analysis for teaching and qualification purposes

- (1) Universities are permitted to make video and audio recordings of students, doctoral researchers and post-doctoral researchers pursuing a habilitation as far as this is required to analyze and reflect, jointly with lecturers, on their work with the aim of assessing and improving actions, means of expression or patterns of movement;

course participants must be given the option of whether to consent to being included in audio and video recordings.

- (2) The recordings may only be used in the context of a specific course and must be deleted immediately, once they are no longer required for the purposes stated in paragraph 1.

§ 14 E-learning systems

- (1) The university operates specialized IT systems (e-learning systems) for the purpose of supporting lecturers, students, guest auditors and others, provided it is regulated in a corresponding cooperation agreement, with the study, teaching and continuing education process. In particular, the e-learning systems include components for organizing courses, working groups and everyday study activities, for creating and sharing learning materials and for enabling communication between lecturers and their students/guest auditors as well as among students and guest auditors.
- (2) Course organizer(s) can require students to use e-learning systems approved by the Rectorate if this is necessary for the respective acquisition of skills. The university can require students to use an e-learning system to submit coursework and performance assessments. In such cases, users are obligated to provide the following data:
 - Login data
 - Consent to the e-learning system's terms of use
- (3) If online exams are conducted via the e-learning system, § 9 applies accordingly.
- (4) E-learning systems must especially fulfil the principles of data protection with regard to their technology design, data protection-friendly default settings and minimization of data processing. Data can only be used for the purpose specified in paragraph 1. The provisions of § 6 remain unaffected.

§ 15 Student records

- (1) For each student, the university keeps a file of all study-related records. The purpose is to keep a record of all application, study and examination documents.
- (2) The overall file is split into several portions which are kept by different organizational units. Each student's file includes the following documents in particular:

The portion kept by the Division of Student Affairs and Teaching consists of:

- Application for admission,
- Documentation of periods of study,

- Documentation of higher education entrance qualification,
- Documentation of health insurance,
- Letter of admission,
- Documentation of factors improving the average grade or of a waiting period or of a case of hardship,
- All documents/correspondence related to enrolment, including
 - Official "enrolment request" issued by the university,
 - Documentation of higher education entrance qualification,
 - Proof of payment of required fees and contributions,
- All documents/correspondence related to fees and contributions, including
 - Official notification of fees due,
 - Applications for and confirmation of exemption from fees,
- All documents/correspondence related to university study, including
 - Applications for and confirmation of leaves of absence,
 - Applications for and confirmation of study programme changes,
 - Documents related to admission to module packages, modules and courses,
 - Official documentation of (interim) examination certificates,
 - Official documentation of certificates earned,
 - Other official documentation of degree certificates,
 - Documentation of participation in a mandatory consultation, if required.


The portion kept by corresponding decentralized organizational units and the Central Examination Office, depending on the responsibility defined in the examination regulations, consists of:

- All documents/correspondence related to examination procedures, including
 - Applications for and confirmation of recognition of performance assessments,
 - Exam registration,
 - Applications for withdrawal from exams and corresponding documentation,
 - Applications for and documentation required for preparing examination/degree certificates,
 - Performance assessments, e.g. written on-campus exams, written assignments, theses and minutes of oral exams,
- Exam results including any assessments of reviewers,
- All documents/correspondence related to exmatriculation, including
 - Application for exmatriculation,
 - Official notification of exmatriculation.

The portion kept by the Division of Legal Affairs consists of:

- Documents related to disciplinary proceedings as per § 62a LHG.
- (3) The only persons permitted to access data as per Articles 9 and 10 GDPR as well as data required for disciplinary proceedings as per § 62 a LHG are persons tasked with processing personal data in corresponding contexts, and only where this is necessary.

§ 16 Processing of student data by the Student Advisory Service

- (1) The Student Advisory Service is a university service that students can voluntarily choose to use.
- (2) In contexts where students are required (by law or statute) to consult with the Student Advisory Service, the university processes the following data:
1. Family name, given name,
 2. Study programme,
 3. Study programme semester,
 4. Email address,
 5. List of coursework and academic performance assessments completed so far,
 6. As well as other data and documents required to achieve the specific objective of the consultation.
- (3) The university can evaluate the amount of coursework, performance assessments and exam registrations completed by a student in order to provide them with individually tailored  advisory services. This takes place when a comparison between the work completed and the requirements of the study and examination regulations indicates that a student's successful completion of the study programme is at risk, especially if there is a risk that the student might not complete the required work on time.

§ 17 Student ID card (UniCard)

- (1) The university issues students a student ID card. The student ID can be issued as a printed chip card (UniCard).
- (2) The following data can be printed visibly on the card:
1. Type of ID and issuer,
 2. Family name,
 3. Given names,
 4. Date of birth,
 5. Enrolment number,

6. University ID number,
7. Semester ticket,
8. Study programme,
9. Period of validity,
10. Affiliation to a faculty/department,
11. Passport photo,
12. BWCard number.

(3) For chip cards (UniCard), the following information is stored on the chip:

- 1 Enrolment number,
- 2 Library and university number,
- 3 Serial number of the chip card,
- 4 Start and end date for the current period of validity,
- 5 Electronic wallet,
- 6 BWCard number.

Due to other legal provisions, the storage of additional data on the chip remains unaffected.


§ 18 Campus management system

The university operates a campus management system with self-service functions. In particular, the campus management system must fulfil the principles of data protection with regard to its technology design, data protection-friendly default settings and minimization of data processing.

§ 19 Data processing in the context of the doctoral examination procedure

(1) For each doctoral candidate, the university keeps a file, generally consisting of the following documents:

1. Application for acceptance as a doctoral candidate and the application for commencement of the doctoral examination process including all the corresponding documents required in the Doctoral Regulations,
2. Official notifications from the respective department,
3. Review of the doctoral thesis as well as minutes of the oral doctoral examination,
4. Draft of the doctoral certificate.

- (2) For the purpose of conducting the doctoral examination procedure and fulfilling legal requirements as per § 13 para. 9 in connection with para. 8 LHG and § 38 para. 5 sentence 4 LHG, the university operates a central system with self-service functions within the campus management system.
- (3) The decentralized organizational units (e.g.  Research Training Groups, Graduate Schools) are entitled to operate systems that support the central system as long as
1. They have consulted with the organizational unit responsible for data protection beforehand,
 2. The systems are included in the university's data processing register as per Article 30 GDPR and
 3. The units have received approval at the Rectorate level.

§ 20 Data processing in the context of academic self-administration

The election regulations and other statutes, in particular the codes of procedure, govern the details of data processing in the context of academic self-administration.

§ 21 Student body (Verfasste Studierendenschaft)

The university transmits personal data to the student body (Verfasste Studierendenschaft) that is required for fulfilling its responsibilities as per § 65 LHG.

§ 22 Examination procedures

- (1) In the context of examination procedures, the organizational units responsible within the university, in particular the respective Examination Office and Examination Board, process the data collected as per § 12 para. 6 LHG as well as other data generated by the university or otherwise lawfully obtained.
- (2) The examination records are part of the student file as per § 15.

Section IV: Responsibilities

§ 23 Responsibilities of persons authorized to represent the university

- (1) The Rectorate has overall responsibility for setting up and operating a functioning data protection management system.
- (2) As the university's external representative, the rector is responsible for ensuring adherence to data protection regulations.
- (3) The directors of individual university units are responsible for ensuring adherence to all data protection regulations in their respective organizational units. These directors are also responsible for implementing and upholding existing data protection and data security standards in their corresponding organizational units.

§ 24 Responsibilities of all university staff

It is the responsibility and obligation of all staff members to ensure data protection and data security. The university offers data protection training to all staff.

§ 25 Information and advice

The organizational unit responsible for data protection provides advice to other organizational units. The responsibilities of the data protection officer as per GDPR remain unaffected.

Section V: Final provisions

§ 26 Coming into effect

The German version of these regulations comes into effect the day after its publication in the "Amtliche Bekanntmachungen" (official announcements) of the University of Konstanz.

Note:

The German version of these regulations was published in the "Amtliche Bekanntmachungen" of the University of Konstanz no. 9/2022 on 22 February 2022.