

## **Data Processing Agreement ( Art. 28 GDPR)**

between

### **University of Erfurt**

represented by the President  
Nordhäuser Str. 63, 99089 Erfurt

- Responsible party -  
referred to as "client"

and

---

---

---

---

- Processor -  
referred to as "Contractor"

### **§ 1 Subject matter and term of the agreement**

(1) The subject matter of the agreement is set out in the basic contract to which reference is made here.

---

(2) The term of this agreement corresponds to the term of the above-mentioned basic contract.

### **§ 2 Specification of the content of the agreement**

(1) The nature and purpose of the processing of personal data by the Contractor are specifically described in the basic contract.

(2) The provision of the agreed data processing shall take place exclusively in a member state of the European Union or in another state party to the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the client and may only take place if the special requirements of Art. 44 of the GDPR are met.

(3) The object of the commissioned processing of personal data is the following data types/ categories: [Please tick or complete]

- ☐ Personal data
- ☐ Communication data (e.g. telephone, email address)
- ☐ Contract data (contractual relationship, product or contractual interest)
- ☐ Contract billing and payment data
- ☐ Planning and control data
- ☐ User data
- ☐ \_\_\_\_\_

(The categories of data subjects affected by the processing include: [Please tick or complete])

- ☐ Students
- ☐ Employees
- ☐ Doctoral Students
- ☐ Habilitation Students
- ☐ Scholarship holders
- ☐ Sponsors/partner companies
- ☐ Users
- ☐ Interested parties
- ☐ Applicants
- ☐ Subscribers
- ☐ Suppliers
- ☐ Contact person
- ☐ \_\_\_\_\_

### **§ 3 Responsibility**

The Contractor processes personal data on behalf of the Client. Within the scope of this agreement, the Client is solely responsible for compliance with the statutory provisions of data protection law, in particular for the lawfulness of data transfer to the Contractor and for the lawfulness of data processing ("controller" within the meaning of Art. 4 No. 7 GDPR).

### **§ 4 Authority of the Client to issue instructions**

(1) The instructions shall initially be defined by the basic contract and may subsequently be amended, supplemented or replaced by the Client in writing or at least in text form to the office designated by the Contractor by means of individual instructions (individual instructions). The Client shall confirm verbal instructions without delay (at least in text form).

(2) The Contractor may only process personal data of data subjects within the scope of the order and the Client's instructions. It must inform the client immediately if it is of the opinion that an instruction violates data protection regulations. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Client.

## § 5 Technical and organizational measures

(1) The Contractor shall document the implementation of the technical and organizational measures set out and required prior to the award of the contract before the start of processing, in particular with regard to the specific execution of the contract, and submit them to the Client for review. If accepted by the client, the documented measures shall form the basis of the order. If the inspection/audit by the client reveals a need for adjustment, this must be implemented by mutual agreement.

(2) The Contractor must ensure the security of the processing in accordance with Art. 28 para. 3 lit. c, 32 GDPR, in particular in conjunction with Art. 5 para. 1, para. 2 GDPR. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the different probability of occurrence and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR must be taken into account.

The contractor shall take the following technical and organizational measures to ensure the security of the processing:

[Please check or complete]

### a) to maintain confidentiality (Art. 32 para. 1 lit. b GDPR)

*Access control: no unauthorized access to data processing systems, e.g. through*

- ☐ Magnetic or chip cards
- ☐ Keys
- ☐ Electronic door openers
- ☐ Plant security or gatekeeper
- ☐ Alarm systems
- ☐ Video systems
- ☐ \_\_\_\_\_

*Access control: no unauthorized system use, e.g. through*

- ☐ (secure) passwords
- ☐ Automatic locking mechanisms
- ☐ Two-factor authentication
- ☐ Encryption of data carriers
- ☐ \_\_\_\_\_

*Access control: no unauthorized reading, copying, modification or removal within the system, e.g. through*

- ☐ Authorization concepts and needs-based access rights
- ☐ Logging of accesses
- ☐ \_\_\_\_\_

*Separation control: separate processing of personal data collected for different purposes, e.g. through*

- ☐ Multi-client capability
- ☐ Sandboxing
- ☐ \_\_\_\_\_
- ☐ Pseudonymization (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR): the processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures
- ☐ \_\_\_\_\_

b) to maintain integrity (Art. 32 para. 1 lit. b EU GDPR)

*Transmission control: no unauthorized reading, copying, modification or removal during electronic transmission or transport, e.g. through*

- ☐ Encryption
- ☐ Virtual Private Networks (VPN)
- ☐ Electronic signature
- ☐ \_\_\_\_\_

*Input control: Determining whether and by whom personal data has been entered, changed or removed in data processing systems, e.g. by*

- ☐ Logging
- ☐ Document management
- ☐ \_\_\_\_\_

c) to ensure availability and resilience (Art. 32 para. 1 lit. b GDPR)

*Availability control: protection against accidental or willful destruction or loss, e.g. through*

- ☐ Backup strategy (online/offline; on-site/off-site)
- ☐ Uninterruptible power supply (UPS)
- ☐ Virus protection
- ☐ Firewall
- ☐ Reporting channels and emergency plans
- ☐ Rapid recoverability (Art. 32 para. 1 lit. c GDPR)
- ☐ \_\_\_\_\_

d) Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR, Art. 25 para. 1 GDPR)

- ☐ Data protection management
- ☐ Incident response management
- ☐ Data protection-friendly default settings (Art. 25 para. 2 GDPR)

*Order control: no order processing within the meaning of Art. 28 EU GDPR without corresponding instructions from the client, e.g. through*

- ☐ Clear contract design
- ☐ formalized order management
- ☐ Strict selection of the service provider
- ☐ Obligation to convince in advance
- ☐ Follow-up checks
- ☐ \_\_\_\_\_

(3) The technical and organizational measures are subject to technical progress and further development. In this respect, the Contractor shall be permitted to implement alternative adequate measures. In doing so, the security level of the specified measures may not be undercut. Significant changes must be documented and communicated to the client without delay.

**§ 6 Correction, restriction, deletion and return of data**

- (1) The Contractor may not rectify, erase or restrict the processing of data processed on behalf of the Client without authorization, but only in accordance with documented instructions from the Client. Insofar as a data subject contacts the Contractor directly in this regard, the Contractor shall forward this request to the Client without delay, insofar as an assignment to the Client is possible according to the information provided by the data subject. This also applies to requests for information from data subjects. The Contractor shall support the Client in clarifying the data subject's request.
- (2) The Contractor shall not be liable if the request of the data subject is not answered by the Client, is not answered correctly or is not answered on time, if and to the extent that the Contractor is not partly responsible for this.
- (3) If included in the scope of services, the deletion concept, right to be forgotten, rectification, data portability and information shall be ensured by the Contractor in accordance with the Client's documented instructions.
- (4) Copies and duplicates of personal data shall not be created without the Client's knowledge. Excluded from this are backup copies, insofar as they are necessary to ensure proper data processing, as well as personal data required to comply with statutory retention obligations.
- (5) Upon completion of the contractually agreed work or earlier at the request of the Client - at the latest upon termination of this Agreement - the Contractor shall hand over to the Client all documents, processing and usage results and data pertaining to the contractual relationship that have come into its possession or, with prior consent, destroy them in accordance with data protection regulations. The same applies to test and scrap material. The deletion log must be submitted on request.

- (6) Documentation that serves as proof of proper data processing in accordance with the order shall be retained by the Contractor beyond the end of the contract in accordance with the respective retention periods. The Contractor may hand them over to the Client at the end of the contract for the Client's discharge.

## **§ 7 Quality assurance and other obligations of the Contractor**

In addition to complying with the provisions of this Agreement, the Contractor has statutory obligations pursuant to Art. 28 to 33 EU GDPR; in this respect, the Contractor shall in particular ensure compliance with the following requirements: [Please check or complete]

- a) ☐ Written appointment of a data protection officer who performs his or her duties in accordance with Art. 38 and 39 EU GDPR.
- ☐ The contact details of the data protection officer shall be provided to the client for the purpose of direct contact. The client will be informed immediately of any change of data protection officer.

---

*(Mr./Ms please enter: fist name, surname, organizational unit, telephone, email address)*

has been appointed as the data protection officer at the Contractor. The client must be informed immediately of any change of data protection officer.

- ☐ Their current contact details are easily accessible on the Contractor's website.
- ☐ The contractor is not obliged to appoint a data protection officer. The contact person at the contractor is

---

Mr/Mrs [please enter: first name, surname, organizational unit, telephone, e-mail address]

- c) ☐ Since the Contractor is based outside the Union, it appoints the following representative in the Union pursuant to Art. 27 (1) GDPR:

---

[please enter: first name, surname, organizational unit, telephone, e-mail address].

- d) In accordance with Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 EU GDPR, the Contractor shall only use employees who have been obliged to maintain confidentiality and who have previously been familiarized with the data protection provisions relevant to them when carrying out the work. The confidentiality obligation shall continue to apply after the end of the contract. The Contractor and any person subordinate to the Contractor who has access to personal data may only process this data in accordance with the instructions of the Client, including the powers granted in this Agreement, unless they are legally obliged to process it.
- e) The Client and the Contractor shall cooperate with the supervisory authority in the performance of their tasks upon request.

- f) The Contractor shall inform the Client without undue delay of any inspections and measures taken by the supervisory authority insofar as they relate to this order. This shall also apply if a competent authority investigates the processing of personal data in the context of administrative offense or criminal proceedings relating to the processing of personal data by the contractor.
- g) Insofar as the Client is subject to an inspection by the supervisory authority, administrative or criminal proceedings, a liability claim by a data subject or a third party or any other claim in connection with the commissioned processing at the Contractor, the Contractor shall support the Client to the best of its ability.
- h) The Contractor shall regularly monitor the internal processes and the technical and organizational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the data subject is guaranteed.
- i) The Contractor shall provide the Client with evidence of the technical and organizational measures taken at any time within the scope of its supervisory powers pursuant to Section 12 of this Agreement.

#### **§ 8 Notification of breaches by the Contractor**

- (1) The Contractor shall support the Client in complying with the personal data security obligations set out in Articles 32 to 36 GDPR, data breach notification obligations, data protection impact assessments and prior consultations. This includes, among other things
  - a) the obligation to enable the detection of security breaches and relevant breach events
  - b) the obligation to report personal data breaches to the client without delay. The Contractor shall take the necessary measures to secure the personal data and to mitigate possible adverse consequences for the data subjects and shall consult with the Client without undue delay in this regard,
  - c) the obligation to support the Client within the scope of its duty to inform the data subject and to provide it with all relevant information in this context without delay,
  - d) the support of the client in the context of its data protection impact assessment or in the preparation of the list of processing activities,
  - e) supporting the client in the context of prior consultations with the supervisory authority
- (2) The Contractor may claim remuneration for support services which are not the subject of the agreement or which are not attributable to misconduct on the part of the Contractor; the amount of remuneration shall be agreed in advance.

#### **§ 9 Obligations of the Client**

- (1) The Client shall inform the Contractor immediately and in full if it discovers errors or irregularities in the results of the order with regard to data protection regulations.
- (2) In the event of a claim against the Contractor by a data subject with regard to any claims under Art. 82 EU GDPR, the Client undertakes to support the Contractor in the defense of the claim within the scope of its possibilities.

- (3) The Client shall inform the Contractor of the contact person for data protection issues arising within the scope of the basic contract.

## § 10 Subcontracting relationships

- (1) Subcontracting relationships within the meaning of this provision shall be understood as those services that relate directly to the provision of the services in accordance with this agreement. This does not include ancillary services which the Contractor uses, e.g. as telecommunications services and postal/transport services.

/transportation services. However, the Contractor is obliged to take appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security of the personal data for which the Client is responsible, even in the case of outsourced ancillary services.

- (2) The Contractor may only commission subcontractors (additional processors) with the prior express written or documented consent of the Client.

[Please check or complete]

- a) ☐ Subcontracting is not permitted.
- b) ☐ The client agrees to the commissioning of the following subcontractors under the condition of a contractual agreement in accordance with Art. 28 para. 2 - 4 EU GDPR:

Company Subcontractor	Address/Country	Performance

- c) ☐ The commissioning of subcontractors or  
☐ the change of the existing subcontractor

is permissible insofar as

- the Contractor notifies the Client of such outsourcing to subcontractors a reasonable time in advance in writing or in text form and
- the client does not object to the planned outsourcing in writing or in text form to the contractor by the time the data is handed over and
- a contractual agreement in accordance with Art. 28 para. 2-4 GDPR is used as a basis.

- (3) The transfer of the Client's personal data to the subcontractor and the subcontractor's initial activities are only permitted once all requirements for subcontracting have been met.



- (4) If the Contractor places orders with subcontractors, the Contractor shall be responsible for transferring its data protection obligations under this Agreement to the subcontractor.
- (5) If the subcontractor provides the agreed service outside the EU/EEA, the Contractor shall ensure the admissibility under data protection law by taking appropriate measures. The same shall apply if service providers within the meaning of para. 1 sentence 2 are to be used.
- (6) Further subcontracting by the subcontractor [please mark with a cross where applicable]
- ☐ is not permitted
  - ☐ requires the express consent of the main client (at least in text form)
  - ☐ requires the express consent of the main contractor (at least in text form)

All contractual provisions in the contractual chain must also be imposed on the other subcontractor.

## **§ 11 Inspection rights of the client**

- (1) The Client shall have the right to carry out inspections in consultation with the Contractor or to have them carried out by inspectors to be named in individual cases. In addition, it shall have the right to satisfy itself of the Contractor's compliance with this Agreement in its business operations by means of spot checks, which must generally be notified in good time. These inspections shall be carried out during the Contractor's normal business hours without disrupting operations.
- The Contractor may make these inspections dependent on the signing of a confidentiality agreement regarding the data of other customers and the technical and organizational measures that have been put in place. If the auditor commissioned by the Client is in a competitive relationship with the Contractor, the Contractor shall have the right to object to this.
- (2) The Contractor shall ensure that the Client can satisfy itself of the Contractor's compliance with its obligations under Art. 28 GDPR. The Contractor undertakes to provide the Client with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organizational measures.

## **§ 12 Maintenance/remote maintenance**

[to be added only if necessary/ not applicable for Software as a service]

- (1) The statutory provisions on order processing shall apply accordingly to maintenance/remote maintenance, insofar as access by the Contractor to the Client's personal data cannot be ruled out. The remote maintenance software used must be disclosed to the Client in writing.

The client must be informed immediately of any changes or extensions to the remote maintenance software and its basic application options. Access to \_\_\_\_\_ [please enter the name of the IT system] of the client for remote maintenance purposes is only permitted via a state-of-the-art encrypted connection. Exceptions require the written consent of the client. The authorized maintenance personnel must be named to the client.

- (2) If remote maintenance is to be carried out, the client must be informed in advance in a suitable form about the application and implementation. The client is entitled to refuse remote access. The client must be able to terminate the remote maintenance at any time by operator action. The client must be able to trace the remote maintenance work at any time. Once the remote maintenance work has been completed, the connection between the service center and the service center must be disconnected immediately.
- (3) During remote maintenance, personal data may not be viewed, transferred, deleted or modified without the consent of the entity being maintained. In the case of remote maintenance, personal data may not be disclosed without the consent of the entity to be maintained.
- (4) The time, duration of maintenance and the main maintenance activities shall be logged by the Contractor during the term of the basic contract. The Client shall be granted access to the log files upon request. The log files shall be kept at \_\_\_\_\_ [please enter: retention period].

### **§ 13 Liability and compensation**

A liability provision agreed between the parties in the basic contract shall also apply to commissioned processing. In addition, Art. 82 GDPR applies.

### **§ 14 Duty to provide information, written form clause, final provisions**

- (1) Should the Client's personal data be jeopardized by seizure or confiscation, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall inform the Client immediately. The Contractor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the personal data lies exclusively with the Client as the "controller" within the meaning of the GDPR.
- (2) Amendments and supplements to this agreement and all its components - including any assurances made by the Contractor - require a written agreement, which may also be made in an electronic format (at least text form), and an express reference to the fact that it is an amendment or supplement to these terms and conditions. This also applies to the waiver of this formal requirement.
- (3) In the event of any contradictions, the provisions of this agreement on data protection shall take precedence over the provisions of the basic contract. Should individual parts of this agreement be invalid, this shall not affect the validity of the remainder of the agreement.
- (4) German law shall apply. The place of jurisdiction is Erfurt.
- (5) All references to persons and functions in this agreement apply equally to men and women.

---

Location and date

---

Location and date

---

Signature

---

Signature