ZENDAS Version 6.0, 10 February 2025

Contract on Data Processing on Behalf of the Controller

Between

the**[higher education institution XY, street, city]**,

represented by [authorized representative]

**- Controller -**

and

the**[company ABC, street, city]**,

represented by [authorized representative]

Representative in accordance with Article 27 of the General Data Protection Regulation (GDPR): [Indicate representative, otherwise delete section]

**- Processor -**

# Subject Matter and Duration, Compensation, Precedence of this Contract, Terminology

1. The Processor processes personal data on behalf of the Controller on the basis of [exact title of the underlying contract including the date, for example an SLA etc.] (hereinafter referred to as “underlying contract”).

The subject matter of this order is determined in the underlying contract. [Additions, if applicable, such as: “The data processing on behalf of the Controller is only conducted via remote maintenance or on-site, using the Controller’s resources.”]

*or*

The subject matter of this contract is [definition of the order in keywords, e.g. “maintenance of the locking system XY”]; the specific processing activities are described in section 2 subsection 2.

1. The provisions of this contract apply to any data processing activities relating to the underlying contract and performed by the Processor on behalf of the Controller.
2. The term of this contract is based on the regulations of the underlying contract. If applicable, this contract continues to apply until the data are erased or returned in accordance with section 4 subsection 14.
3. The Controller has the right to extraordinary termination of this contract and the underlying contract if the Processor does not properly execute the contractually agreed services (if required by law, despite a written request) or violates obligations under this contract, in particular the obligations set forth in section 4.
4. Unless specifically agreed upon, no separate compensation is paid.
5. Where this contract determines regulations which differ from the regulations of the underlying contract, the regulations of the Contract on Data Processing on Behalf of the Controller take precedence.
6. The terminology regarding data protection in this contract is in line with the General Data Protection Regulation (GDPR) of 27 April 2016.

# Specification Regarding the Nature and Purpose of the Data Processing on Behalf of the Controller, the Type of Personal Data and the Categories of Data Subjects

The nature and purpose of the processing performed by the Processor for the Controller are described in detail in [insert exact name of the document here, including the date, version number or similar and, if applicable, the exact source of the information; e.g. “SLA of...”]

*or*

Nature of the processing:

[Description of the activities to be carried out]

Purpose of the processing:

[Description]

The type of data used is described in detail in [insert exact name of the document here, including the date, version number or similar and, if applicable, the exact source of the information; e.g. “SLA of...”]

*or*

The following types of data are subject to processing:

[Description, e.g. master data related to individuals, communication data]

The categories of data subjects whose data are processed in the context of this contract are described in detail in [insert exact name of the document here, including the date, version number or similar and, if applicable, the exact source of the information; e.g. “SLA of...”]

*or*

Personal data from the following categories of data subjects are processed in the context of this contract:

Students

Applicants for a degree program

Employees

Business associates

Test subjects

[Description]

[Description]

The contractually agreed data processing performed by the Processor without engaging other processors within the meaning of Art. 28 paragraph 2 GDPR (subcontractors) exclusively takes place in a member state of the European Economic Area (member states of the EU, Iceland, Liechtenstein, Norway).

The contractually agreed data processing performed by the Processor without engaging other processors within the meaning of Art. 28 paragraph 2 GDPR (subcontractors) takes place in the third countries stated in Annex 1 (if applicable, in addition to a member state of the European Economic Area).

Any data processing activities performed by the Processor without engaging subcontractors may only be transferred to a country outside of the European Economic Area (third country) if the Controller gives prior consent and the provisions set forth in Articles 44 et seqq. GDPR are fulfilled.

# Right to Issue Instructions and Right to Audit

1. The Controller remains responsible for the compliance with the regulations on data protection, in particular those of the data protection act of the Land of Baden-Württemberg (LDSG) and the GDPR.
2. The Controller has the right to issue instructions to the Processor regarding the processing of the personal data. These instructions must be documented.
3. On the part of the Controller, the following persons are authorized to issue instructions:

[Name, phone, e-mail, function (if required), organizational unit (if required)]

On the part of the Processor, the following persons are authorized to receive instructions:

[Name, phone, e-mail, function (if required), organizational unit (if required)]

1. In case of changes or long-term absence of the persons stated in subsection 3, the other party to the contract must be informed about the successor or substitute in writing and without undue delay.
2. The Processor informs the Controller immediately if, in the Processor’s opinion, an instruction infringes the GDPR or other data protection regulations of the European Union or national law.
3. Instructions that amend, revoke or supplement the regulations set forth in sections 1 and 2 of this contract must be agreed upon in writing in order to be binding.
4. The Controller has the right to audit compliance with the regulations on data protection and the regulations of the contract as needed in the context of the contract or to authorize another person to do so, particularly by obtaining information and inspecting the stored data and the data processing software. The Processor assists with the auditing activities. The Processor is obligated to provide the information requested by the Controller and, in particular, provide proof that the technical and organizational measures were implemented.

# Obligations of the Processor

1. The Processor will provide the Controller with any information required to prove compliance with the obligations set forth in Art. 28 GDPR.
2. The Processor processes personal data only as agreed upon in this contract and in accordance with the instructions of the Controller. This also applies to the transfer of personal data to a third country or international organization, unless the Processor is obligated to transfer the data under the law of the European Union or national law; in this case, the Processor informs the Controller of this processing requirement before the processing takes place, unless the respective law prohibits such a notification due to an important reason of public interest.
3. Processing the data for other purposes is not permitted. The Processor must rectify or erase personal data or restrict the processing of personal data if requested by the Controller in the contract or by instruction.
4. The Processor guarantees the execution of all contractually agreed measures within the scope of the contractual relationship.
5. The Processor assists the Controller in creating and maintaining a record of processing activities, in particular by making the required information available.
6. The Processor maintains a record of processing activities in accordance with Article 30 paragraph 2 GDPR.
7. If the Controller’s data are located on data storage devices of the Processor, the following agreements are concluded:
   1. If the data storage devices are suitable to be handed over, the Processor transfers the data storage devices to the Controller for the purpose of transfer by way of security. The data storage devices must be specifically marked. The Processor is obligated to keep at least one data storage device on which all data of the Controller can be stored and that is suitable for transfer. The Processor stores the data storage devices free of charge until they can be handed over to the Controller.
   2. If the data storage devices are not suitable to be handed over and if, due to actions of third parties (such as seizure) or in case of bankruptcy or insolvency proceedings or other events, the data are in danger of falling into the hands of a third party, the Processor is obligated to copy the data onto the data storage device specified in subsection 7 letter a sentence 3 and erase the data from the storage devices affected by actions of the third party or the events in accordance with data protection regulations.
8. The Processor notifies the Controller immediately if the Controller’s property or the confidentiality of the Controller’s data stored with the Processor are compromised by actions of a third party (such as seizure), in case of bankruptcy or insolvency proceedings or other events.
9. The Processor notifies the Controller immediately of any major disturbances in operating procedures, any suspected personal data breaches, other irregularities in the processing of data and any inspections and actions by a supervisory or investigative authority. The Processor notifies the Controller immediately if the security measures taken by the Processor do not meet the Controller’s requirements (anymore).
10. In case of a personal data breach, the Processor takes appropriate measures in consultation with the Controller in order to secure the data as well as mitigate possible adverse effects on the data subjects. The Processor assists the Controller in ensuring compliance with the obligation to notify the supervisory authority of personal data breaches and the obligations to communicate such breaches to the data subject.
11. The Processor assists the Controller in taking the required technical and organizational measures, in particular those determined in Article 32 GDPR, taking into account the nature of the processing and the information available to the Processor. [If possible, list specific assistance measures here. Otherwise, delete this text.]
12. Taking into account the nature of the processing and the information available to the Processor, the Processor assists the Controller in conducting a possible assessment of the impact of the processing on the rights and freedoms of natural persons, especially in the case of a data protection impact assessment required in accordance with Article 35 GDPR as well as in the prior consultation of the supervisory authorities, if the conditions of Article 36 paragraph 1 GDPR are fulfilled. [If possible, list specific assistance measures here. Otherwise, delete this text.]
13. Taking into account the nature of the processing, the Processor assists the Controller by taking appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Controller’s obligation to respond to requests for exercising the data subject’s rights laid down in Chapter III of the GDPR (such as transparent information, access, rectification, erasure and restriction of processing). [If possible, list specific assistance measures here. Otherwise, delete this text.]
14. Upon completion of the data processing, the personal data processed on behalf of the Controller must not remain with the Processor. Therefore, the Processor must erase or, upon the Controller’s request, return all documents obtained that are the subject of the data processing, as well as the results of the data processing and the results of the use of the data, unless European Union or national law requires the storage of the personal data. The Processor must provide the Controller with an unsolicited confirmation (at least in text form) stating that none of the personal data processed on behalf of the Controller remain with the Processor. If the data are erased, the Processor must explicitly confirm that all personal data processed on behalf of the Controller have been erased. The Processor does not have any right of retention concerning the personal data processed or the respective data storage devices.

The Processor has adequate liability insurance coverage or comparable insurance in a member state of the European Union and provides proof of insurance to the Controller. The Processor undertakes to remain under this insurance coverage for the term of the contract and until the end of the period of limitation of claims.

# Subcontracts

The Processor does not engage any subcontractors at the time the contract is concluded.

*or*

The Controller agrees to the engagement of the subcontractors listed in Annex 1 at the time the contract is concluded.

*(Version 1)* The Processor may only engage subcontractors other than those listed at the time the contract is concluded in individual cases and upon prior written authorization by the Controller.

*or*

*(Version 2)* Besides subcontractors specified at the time the contract is concluded, the Processor may engage the following subcontractors on condition that a contract in accordance with Article 28 paragraphs 2 to 4 GDPR is concluded:

The subcontractors

* have their registered office with a legal personality in a member state of the European Economic Area (member states of the EU, Iceland, Liechtenstein, Norway) or
* are covered by an adequacy decision of the European Commission (Art. 45 paragraph 3 GDPR) or

have agreed on standard contractual clauses with the Processor in accordance with Module 3 of the Annex of the Commission Implementing Decision (EU) 2021/914.[[1]](#footnote-2)

The Processor informs the Controller of any intended changes concerning the addition or replacement of subcontractors at least four weeks before the implementation of the changes. The Controller has the right to object to such changes within three weeks of receiving the notification. If an objection is made, no subcontractors may be engaged.

1. Where a subcontractor is engaged, the Processor ensures by means of a contract that the regulations of this contract (in particular, monitoring and audit rights of the Controller) also apply to the subcontractor. Furthermore, sufficient guarantees must be provided that the appropriate technical and organizational measures are implemented in such a manner that the processing meets the requirements of the GDPR. The Processor provides proof of these guarantees to the Controller. The Processor audits the subcontractor’s compliance with the regulations on a regular basis.
2. Where a subcontractor fails to fulfill the data protection obligations, the Processor is fully liable to the Controller for the performance of that subcontractor’s obligations.
3. The Processor provides the Controller with all information on the processing performed by the subcontractor that is required for the records of processing activities.
4. Further outsourcing by the subcontractor to additional subcontractors in the service chain

is not permitted;

requires the explicit consent of the Controller and the imposition of all contractually agreed regulations in the chain of contracts on the additional subcontractor.

1. Data may only be forwarded to the subcontractor if all the requirements for outsourcing are fulfilled.

# Confidentiality, Data Secrecy, Data Protection Officer

1. All parties are obligated to treat any trade secrets and data security measures of the other party obtained in the context of the contractual relationship with confidentiality. This obligation continues after the end of the contract.
2. Confidentiality obligations do not apply in cases where confidential information was already in the public domain at the time it was given to the other party to the contract, is made available to the public domain after it was given to the other party to the contract and the publication was not in breach of contractual or legal regulations, where the other party to the contract waives confidentiality restrictions or confidential information must be disclosed to third parties due to an administrative or legal ruling.
3. The party to the contract invoking one of the aforementioned exceptions bears the burden of proof that the invoked exception applies.
4. Persons authorized to process personal data may not process personal data without authorization (data secrecy). The Processor guarantees that these persons have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Where a confidentiality declaration is concluded, the wording must make clear that the declaration continues to apply after the end of this contract or the end of the employment relationship between the Processor and persons employed by the Processor. Upon request, the Controller must be provided with appropriate proof that confidentiality obligations are put in place.
5. The Processor confirms to be aware of the applicable data protection regulations, in particular the GDPR, the LDSG, the Federal Data Protection Act (BDSG) and the German Criminal Code, and guarantees to make the employees tasked with the processing aware of the applicable regulations. The Processor monitors the compliance with data protection regulations.
6. The Processor may only provide information on the personal data processed on behalf of the Controller under this contract to third parties or data subjects upon prior written consent of the Controller. If the Processor is required by law or court order to provide information, the Processor must inform the Controller immediately. The Processor may only give information destined for the Controller to authorized persons (section 3 subsection 3 of this contract).
7. If the Processor is legally required to designate a data protection officer, the data protection officer is to be designated before the implementation of the contract. The Processor provides the data protection officer’s contact details to the Controller. The same applies if the data protection officer is changed.

The Processor does not have an establishment in the European Union and therefore designates the following representative in accordance with Article 27 GDPR:

[Name, organization, phone, e-mail address]

# Technical and Organizational Measures

1. The Processor must not copy or duplicate any of the data processed on behalf of the Controller without the knowledge of the Controller.
2. The Processor processes data in the Processor’s own facilities or off-site in the context of mobile work settings in accordance with section 8.
3. The Processor must destroy any testing materials or discarded materials in tangible form without undue delay and in compliance with data protection regulations or hand them over to the Controller. The Processor must destroy electronic testing data without undue delay and in compliance with data protection regulations. The Processor must confirm in writing that the data have been destroyed and on which date.
4. The Processor guarantees that the Controller’s data are kept separately from other data.
5. The Processor takes all measures to ensure the security of processing required according to Article 32 GDPR. Overall, these measures constitute measures of data security and measures to ensure a level of security appropriate to the risk regarding confidentiality, integrity, availability as well as the resilience of processing systems. The state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons according to Article 32 paragraph 1 GDPR are to be taken into account. The measures are specified in the following document: [Title of the document]. The technical and organizational measures defined in this document are part of this contract.
6. The technical and organizational measures agreed upon in this contract may be adapted to the technical and organizational process during the course of the contract relationship. Changes and amendments to the agreed technical and organizational measures require that the authorized person(s) of the Controller are notified in writing and with explicit mention that changes or amendments to these measures are being made.Substantial changes to the technical and organizational measures require the consent of the Controller. The changes to the technical and organizational measures made by the Processor must not cause the measures to fall below the agreed level of security.

# Mobile Work

1. The Processor may allow their employees who are mandated to process personal data on behalf of the Controller to process personal data off-site in compliance with the following provisions.
2. The Processor must ensure that the contractually agreed technical and organizational measures are also complied with in mobile work settings of the Processor’s employees. Deviations from individual contractually agreed technical and organizational measures must be agreed with the Controller in advance and approved by them in writing.
3. In particular, the Processor must ensure that, where personal data are processed off-site, the storage locations are configured in such a way as to exclude local storage of data on IT systems used by the mobile workforce. If this is not possible, the Processor must ensure that data stored locally is always encrypted and that the employees’ cohabitants do not have access to this data.
4. The Processor must ensure that the Controller may effectively monitor the processing of personal data on behalf of the Controller in mobile work settings. The personal rights of employees and their cohabitants must always be respected.
5. The parties agree that, in order to protect the personal rights of the Processor’s employees and their cohabitants, the main measure for monitoring the processing of personal data in mobile work settings is to confirm that the Processor has taken the measures outlined in subsections 2 and 3. When appropriate, the Processor must also allow the Controller to monitor the mobile working practices of employees. The Processor may require that checks on the employees’ mobile working practices be carried out only in the Processor’s presence.

# Liability

1. The Controller and the Processor are liable to the data subjects in accordance with the provisions of Article 82 GDPR. The Processor must coordinate any fulfillment of liability claims with the Controller.
2. At first request, the Processor exempts the Controller from all claims data subjects assert against the Controller due to the breach of an obligation imposed on the Processor by the GDPR, or due to the Processor’s failure to comply with an instruction outlined in this contract or given separately by the Controller.
3. The parties release themselves from liability if/insofar as one party proves that they are in no way responsible for the circumstances through which the damage occurred to a data subject. Apart from that, Article 82 paragraph 5 GDPR applies.
4. Unless otherwise stipulated above, the liability within the scope of this contract corresponds to that of the underlying contract.

# Further Provisions

1. Changes, additions or supplementary agreements to this contract must be made in writing.
2. Should individual provisions of this contract be or become invalid or unenforceable, the validity of the other provisions remains unaffected. The parties to the contract will replace the invalid or unenforceable provision with a legally admissible replacement which corresponds to the purpose of the invalid provision as far as possible. The same applies for any unintentional omissions.

City, date City, date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Controller Signature Processor

---

Annex

Annex 1 (to section 2 subsection 4 and section 5 subsection 1):

Overview of data processing in a third country and/or subcontractors

Annex 2 (to section 7 subsection 5):

Title of the TOM document as set forth in section 7 subsection 5

Further annexes (if applicable)

1. Only choose the option under version 2 if the higher education institution is aware of the following: When agreeing on so called standard contractual clauses (SCCs), the contracting parties (here: Processor and other processors within the meaning of Art. 28 paragraph 2 GDPR (here: “subcontractor”)) are obliged to conduct a transfer impact assessment, i.e. a comprehensive assessment of the legal situation in the third country to which data are transferred (further information in German is provided at https://www.zendas.de/themen/drittlandstransfer/Standarddatenschutzklauseln.html). The parties are obliged to conduct this assessment according to clause 14 of the SCCs. Depending on the legal situation in the third country, the agreement of SCCs alone may not suffice. In this case, the contracting parties must further assess whether they can implement other measures to remedy shortcomings in the data protection regulations of the third country. In individual cases, this may entail complex assessments and evaluations. If the higher education institution chooses the option under version 2 of the general authorization, it must rely on the Processor and their subcontractors to comprehensively assess and “correctly” evaluate the legal situation in the respective third country. Only then is the transfer of data to the third country considered justified and compliant with data protection regulations. The higher education institution is the controller within the meaning of Art. 4 no. 7 GDPR in the entire chain of contracts. Therefore, the option should only be chosen in exceptional cases. [↑](#footnote-ref-2)