Data Processing Agreement

In order to fulfil the requirements set out in Article 28 of the General Data Protection Regulation (GDPR)[1] , the parties listed in **Annex 1 hereby** enter into this agreement, including its binding annexes.

Annex 1 Names of the contracting parties

Annex 2 Description of the processing

Annex 3 Technical and organisational measures in accordance with Article 32 of the GDPR

Annex 4 Sub-processors

1. Definitions, priority clause

1.1. The definitions set out in the GDPR shall apply.

1.2. In the event of any conflict between this contract and any other contracts between the parties, the provisions of this contract shall prevail.

2. Rights and obligations of the data controller

The controller is responsible, in particular, for the lawfulness of the processing in accordance with Article 6(1) of the GDPR or other relevant legal bases, for compliance with the data protection law of the Member States applicable to and binding upon the controller, and for safeguarding the rights of data subjects under Articles 7, 12 to 22 of the GDPR.

3. Processing in accordance with instructions and the duty to object

3.1. The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of those legal requirements prior to processing, unless such notification is prohibited by the relevant law on grounds of an important public interest. Within the framework of such instructions, the processor may retain a degree of discretion as to the appropriate technical and organisational measures by which the instructions are implemented.

3.2. Instructions shall, as a general rule, be issued by the controller in writing (e.g. by email). Where, exceptionally, an instruction is given orally, the processor shall confirm it in writing (e.g. by email). The data processor shall ensure that all instructions issued by the data controller are communicated to its relevant employees (e.g. by centrally archiving all instructions).

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

3.3. The data processor shall immediately notify the data controller if, in its opinion, compliance with an instruction issued by the data controller would contravene the GDPR or any other data protection regulation (duty to raise objections). In this case, it may suspend implementation of the instruction until the data controller indicates whether it intends to uphold, amend or revoke the instruction.

4. Duty of confidentiality

For the purposes of performing the contract, the processor shall only employ persons whom it has bound to confidentiality or who are subject to an appropriate statutory duty of confidentiality. In this respect, the processor shall ensure that these persons only access personal data relating to the commissioned processing activity to the extent necessary ('need to know'). Where the data controller is subject to statutory confidentiality obligations, the data processor shall oblige the employees engaged to perform the contract, as well as any sub-processors, to maintain confidentiality, taking into account the relevant law, in particular the relevant professional regulations.

5. Technical and organisational measures in accordance with Article 32 of the GDPR

5.1. The processor shall implement all necessary technical and organisational measures in accordance with Article 32 of the GDPR, which shall include, as a minimum, the measures specified in **Annex 3**.

5.2. Technical and organisational measures are subject to technical progress and further development. Throughout the term of this contract, the data processor shall continuously adapt these measures to the requirements of this contract and further develop them in line with technical progress. The adequacy of the measures must be reviewed regularly by the data processor. The level of security provided by the technical and organisational measures set out in **Annex 3** must not be reduced without the written consent of the data controller. Written consent may also be provided in electronic form.

5.3. The processor undertakes to document in writing any changes to the technical and organisational measures that have a significant impact on the guaranteed level of security, as an addendum to **Annex 3** – which may also be in electronic format – and to notify the controller thereof.

6. Use of sub-processors

6.1. The processor may engage sub-processors. Any sub-processors engaged at the time of conclusion of the contract are listed in **Annex 4**.

The data processor must inform the data controller of any intended changes relating to the engagement or replacement of sub-processors. The data controller may object to such changes within a reasonable period.

6.2. Where the processor engages the services of a sub-processor to carry out specific processing activities on behalf of the controller, that sub-processor shall be bound by a contract, which must be in writing (which may also be in electronic form), or by any other legal instrument

under Union law or the law of the relevant Member State, be subject to substantially the same data protection obligations as those set out in this contract, in particular providing sufficient guarantees that the appropriate technical and organisational measures are implemented so that the processing is carried out in accordance with the requirements of the GDPR. Where a sub-processor breaches its resulting obligations, the processor shall inform the controller accordingly. If the sub-processor fails to fulfil its data protection obligations, the processor shall be liable to the controller for the sub-processor's compliance with those obligations.

7. Transfers to third countries

7.1. A transfer of personal data to a third country or an international organisation shall only take place on the basis of documented instructions from the controller and in accordance with Chapter V of the GDPR; such instructions may be issued at the time of conclusion of the contract within the framework of **Annex 4** or in accordance with clause 6.1.

7.2. In the case referred to in paragraph 1, the data processor may enter into the European Commission's Standard Data Protection Clauses (the 'Processor to Processor' module) with any sub-processor in accordance with Article 46(2) of the GDPR.

8. Support for the controller's compliance with its obligations

8.1. The data processor shall respond to the data controller's enquiries relating to the contract promptly and in an appropriate manner.

8.2. The processor shall assist the controller, taking into account the nature of the processing and the information available to it, in complying with the obligations set out in Articles 32 to 36 of the GDPR (ensuring the security of processing; notifying supervisory authorities of personal data breaches; notifying the data subject affected by a personal data breach; data protection impact assessment; prior consultation).

8.3. If the processor becomes aware of a personal data breach, it shall notify the controller without undue delay in writing, taking into account the requirements set out in Article 33(3) and (4) of the GDPR.

8.4 The processor shall, taking into account the nature of the processing, assist the controller with appropriate technical and organisational measures in fulfilling its obligation to respond to requests for the exercise of the data subject's rights set out in Chapter III of the GDPR, and shall in this regard follow the controller's instructions. Where data subjects contact the processor to exercise their rights, the processor shall inform the controller without delay. The processor shall only respond to a data subject's request after authorisation from the controller.

9. Erasure and return of personal data

9.1. Provided that Union law or the law of a Member State does not preclude it, the processor shall – subject to any other obligations towards the controller or the controller's instructions

under clause 3 – erase the personal data used and any existing copies without delay upon termination of the contract, in accordance with data protection requirements.

9.2 Until the data is deleted or returned, the data processor shall continue to ensure compliance with this contract.

9.3 The Contractor must confirm the deletion to the Client in writing. To this end, the Contractor shall provide the Client with suitable evidence (e.g. deletion logs, certificates, audits).

10. Proof of compliance and assistance with audits

10.1. The Data Processor shall, upon request, provide the Data Controller with all necessary information and documents to demonstrate compliance with the obligations set out in Article 28 of the GDPR and in this Agreement, including any contracts with sub-processors. Where necessary to protect trade secrets or other confidential information, including personal data, the processor may redact the text of the agreement before providing a copy.

10.2 The processor shall facilitate audits – including inspections at the processor's premises or physical facilities, where appropriate with reasonable notice – carried out by the controller or another auditor appointed by the controller, and shall cooperate in their conduct. The determination of the nature and method of the audit (e.g. remotely or on-site, via questionnaire or in a face-to-face interview) is subject to the data controller's unrestricted discretion. The data controller may, at its own discretion, also base its audit on an audit carried out on behalf of the data processor, as well as on relevant certifications held by the data processor.

11. Other provisions

11.1. Should the contractual fulfilment of the subject matter of the contract as set out in **Annex 2** by the data processor be jeopardised by attachment or seizure, by insolvency or composition proceedings, or by other events or measures taken by third parties, the data processor shall inform the data controller without delay. The data processor shall immediately inform all parties involved in this context that the authority to dispose of the data lies exclusively with the data controller.

11.2. The data processor shall inform the data controller without delay if it is unable to fulfil its obligations under this contract. Where the data processor fails to fulfil its obligations under this contract, the data controller may instruct the data processor to suspend processing until the data processor ensures compliance with its contractual obligations. Where the data processor fails to ensure compliance with its contractual obligations or with the GDPR within one month, the data controller may terminate the contract with immediate effect. The Data Controller shall also have the right to terminate the contract without notice in the event of a serious breach by the Data Processor of this contract or of its obligations under the GDPR.

The same shall apply if the Data Processor fails to comply with a decision of a court or the competent supervisory authority that is binding on it.

11.3. Should any provisions of this contract be invalid, this shall not affect the validity of the remainder of the contract.

11.4. Any amendment to this contract, including its termination and this clause, must be in writing, which may also be in electronic form.

Annex 1: Names of the contracting parties

Responsible Party / Client

the relevant course instructor

Data Processor / Contractor

Sara Lopes de Almeida, Daniela Reinartz GbR,
Im Mediapark 5

50670 Cologne, Germany

Appendix 2: Description of the processing

Subject matter and purpose of the processing

The subject matter of the processing is: the technical provision and operation of an online platform for the delivery of courses by the Client to end customers, including, in particular, online streaming, chat functions, participant management, the provision of course content and supporting technical platform functions.

The activities of the data processor serve only the following purposes: The processing is carried out for the purpose of technically enabling, conducting and managing online courses and training sessions via the contractor's platform, in particular for the registration and participation of end customers, for communication between course leaders and participants, for the provision of course content, and for ensuring the technical operation of the platform.

Duration of processing

Duration of processing: Processing takes place for the duration of the contractual relationship between the Client and the Contractor.

Categories of personal data

Categories of personal data subject to processing:

- Master data, in particular name, user ID, contact details
- Communication data, in particular email address, chat messages and course-related communication
- Booking and attendance data, in particular booked courses, attendance dates and times, and participant status
- Content data, in particular course materials provided, contributions, etc.
- Technical usage and log data, in particular IP address, log data, device and browser information
- Audio and video data, insofar as these are processed as part of the online stream

Categories of data subjects

In the course of fulfilling the contract, the data processor processes personal data relating to the following categories of data subjects:

- Participants or end customers of the courses and training programmes offered via the platform
- Course leaders or other persons appointed by the client
- Users of the platform, insofar as they are involved in the delivery, administration or communication relating to the courses

Annex 3: **Technical and organisational measures in accordance with Article 32 of the GDPR**

Taking into account the

- state of the art,
- the costs of implementation,
- the nature, scope and context,
- the purposes of the processing,
- the sensitivity of the personal data being processed, in particular with regard to special categories of personal data (see Article 9(1) of the GDPR), and
- the varying likelihood and severity of the risk to the rights and freedoms of natural persons

the processor shall implement appropriate technical and organisational measures to ensure a level of protection appropriate to the risk.

When assessing the appropriate level of protection, particular account must be taken of the risks associated with the processing, in particular those arising from – whether accidental or unlawful – destruction, loss, alteration or unauthorised disclosure of, or unauthorised access to, personal data that has been transmitted, stored or otherwise processed.

The data processor shall take the following measures:

1. Measures to ensure confidentiality
It must be ensured that personal data is processed only by authorised persons.

1.1. Access control
Unauthorised persons must be denied access to data processing facilities used to process or utilise personal data.

- ☐ Access control system, ID card reader (magnetic/chip card)
- ☐ Door security measures (electric door openers, combination locks, etc.)
- ☐ Security doors / windows
- ☐ Security grilles on windows/doors
- ☐ Fencing
- ☐ Key management/documentation of key allocation
- ☐ Site security, gatekeepers
- ☐ Alarm system
- ☐ CCTV
- ☐ Special security measures for the server room
- ☐ Special precautions for the storage of backups and/or other data storage media
- ☐ Irreversible destruction of data storage media
- ☐ Staff and access cards
- ☐ Restricted areas
- ☐ Visitor policy (e.g. collection at reception, recording of visiting times, visitor passes, escorting visitors to the exit after their visit)

1.2. Access control

Measures must be taken to prevent unauthorised persons from using data processing systems.

- ☒ Personal and individual user log-in when logging into the system or company network
- ☐ Authorisation process for access rights
- ☒ Restriction of authorised users
- ☐ Single sign-on
- ☐ Two-factor authentication
- ☐ Biometric scan (fingerprint, iris, face)
- ☐ BIOS passwords
- ☒ Password policies (specifying password parameters regarding complexity and update intervals)
- ☒ Automatic blocking of access for a specified period following repeated incorrect entry of login details
- ☐ Electronic documentation of passwords and protection of this documentation against unauthorised access
- ☐ Personalised smart cards, tokens, PINs/TANs, etc.
- ☐ Logging of access
- ☐ Additional system log-in for specific applications
- ☒ Automatic locking of clients after a certain period of inactivity (including password-protected screen savers or automatic sleep mode)
- ☒ Firewall
- ☒ System-specific protection against attacks / intrusion detection / intrusion prevention

1.3. Access control

It must be ensured that persons authorised to use a data processing system can access only the data covered by their access authorisation, and that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after storage.

- ☐ Management and documentation of differentiated authorisations
- ☐ Analysis and logging of data processing operations
- ☐ Authorisation process for access rights
- ☐ Approval procedures
- ☒ Profiles/roles
- ☒ Regular checks on the validity of access rights in accordance with the 'need-to-know' principle
- ☐ Encryption of CD/DVD-ROMs, external hard drives and/or laptops (e.g. via the operating system)
- ☐ Measures to prevent unauthorised copying of data onto portable storage media (e.g. copy protection, blocking of USB ports, 'Data Loss Prevention (DLP) system')
- ☐ 'Mobile Device Management system'

☐ Dual-control principle
☐ Segregation of duties
☐ Professional destruction of documents and data storage media in accordance with ISO/IEC 21964-1:2018-08
☐ Irreversible erasure of data storage media
☒ Logging/documentation of erasure operations
☐ Privacy films for mobile data processing systems

1.4. Separation control

It must be ensured that data collected for different purposes can be processed separately.

☐ Storage of data records in physically separate databases
☒ Separate systems
☐ Access permissions based on functional responsibility
☐ Separate data processing through differentiated access controls
☐ Multi-client capability of IT systems
☒ Use of test data
☐ Separation of development and production environments

2. Encryption measures

It must be ensured that access to plaintext is only possible using a (secret) key.

☒ Encryption of mobile devices such as laptops, tablets and smartphones
☐ Encryption of portable storage media (CD/DVD-ROMs, USB sticks, external hard drives)
☐ Encryption of files
☐ Encryption of systems/equipment
☐ Encrypted storage of passwords
☐ Encryption of emails and email attachments
☐ Secure data transfer (e.g. SSL, FTPS, TLS)
☐ Secure Wi-Fi

3. Pseudonymisation

Personal data may be processed in such a way that it can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is kept separately and is subject to technical and organisational measures that ensure the unauthorised identification of data subjects is prevented. Pseudonymisation is a technical and organisational measure and may be implemented by the contractor as follows:

☒ separate storage of additional identification information
☐ Use of (staff, customer or patient) identification numbers instead of names
☐ Encryption of additional identification information
☐ Management and documentation of differentiated access rights to supplementary identification information
☐ Authorisation process or approval procedures for authorisations to process supplementary identification information

☐ Copy protection in respect of supplementary identification information
☐ Dual-control principle for identification

4. **Measures to ensure integrity**
It must be ensured that personal data is processed accurately and without manipulation.

☐ Access rights
☒ System-level logging
☐ Document Management System (DMS) with change history
☐ Security/logging software
☒ Functional responsibilities, organisationally defined areas of responsibility
☐ Dual control principle
☐ Tunnelled remote data connections (VPN = Virtual Private Network)
☐ 'Data Loss Prevention (DLP) system'
☐ Electronic signature
☐ Logging of data transmission or data transfer
☐ Logging of read accesses
☐ Logging of the copying, modification or deletion of data

5. Measures to ensure and restore availability
It must be ensured that personal data is protected against accidental destruction or loss.

☒ Security policy for software and IT applications
☒ Back-up procedures
☐ Storage procedure for backups (fireproof safe, separate fire compartment, etc.)
☒ Ensuring data storage within a secure network
☒ Installation of security updates as required
☐ Mirroring of hard drives
☐ Installation of an uninterruptible power supply (UPS)
☐ Suitable storage facilities for paper documents
☐ Fire and/or water damage protection for the server room
☐ Fire and/or water damage protection for the archive facilities
☐ Air-conditioned server room
☒ Virus protection
☒ Firewall
☐ Contingency plan
☐ Successful emergency drills
☐ Redundant, geographically separate data storage (offsite storage)

6. **Measures to ensure resilience**

It must be ensured that data processing systems are sufficiently robust and resilient to cope with the most significant anticipated disruptive events without their functionality being impaired.

☐ Contingency plan for equipment failure
☐ Redundant power supply
☒ Sufficient capacity of IT systems and equipment
☐ Logistically managed process to prevent peaks in demand
☐ Redundant systems/equipment
☒ Resilience and fault management

7. Effectiveness monitoring

It must be ensured that procedures are in place for the regular review, assessment and evaluation of the effectiveness of technical and organisational measures.

☐ Procedures for regular checks/audits
☒ Policy for regular review, assessment and evaluation
☐ Reporting
☐ Penetration tests
☐ Disaster recovery testing

8. Compliance with instructions

It must be ensured that personal data is processed only in accordance with the client's instructions (including where a further sub-processor is involved).

☒ Data processing agreement in accordance with Article 28(3) of the GDPR, setting out the rights and obligations of the data processor and any further ~~sub-processors~~
☐ Guidelines/specifications for defining data protection responsibilities/accountabilities
☐ Process for issuing and/or complying with instructions
☒ Designation of contact persons and/or responsible staff members
☐ Monitoring/review of the execution of orders in accordance with instructions
☐ Training/induction for all contractor staff with access authorisation
☐ Independent audit of compliance with instructions
☒ Employees' obligation to maintain confidentiality
☐ Agreement on contractual penalties for breaches of instructions
☐ Appointment of a data protection officer in accordance with Article 37 et seq. of the GDPR
☒ Data protection manager/coordinator
☒ Maintaining a record of processing activities in accordance with Article 30(2) of the GDPR
☐ Documentation and escalation process for personal data breaches

☐ Guidelines/requirements for ensuring technical and organisational measures for the security of processing

9. Support for the client

The contractor shall provide the necessary support to the client in fulfilling its obligation to assist the controller

- *in responding to requests to exercise the data subject's rights set out in Chapter III of the GDPR,*
- *in reporting data breaches to the competent supervisory authorities and data subjects,*
- *in carrying out a data protection impact assessment, including any necessary consultation with the competent supervisory authority, and*
- *in fulfilling its obligation to ensure the required data quality (factually correct and up to date).*

☐ Guidelines/specifications for defining data protection responsibilities/accountabilities

☐ Guidelines/requirements for ensuring technical and organisational measures for the security of processing

☒ Process for forwarding enquiries from data subjects

☐ Notification of the controller upon becoming aware of inaccurate or out-of-date personal data

10. Approved codes of conduct / certification procedures

Compliance with approved codes of conduct pursuant to Article 40 of the GDPR or a certification scheme approved by the European Data Protection Supervisor ( ) pursuant to Article 42 of the GDPR as evidence of compliance with the above requirements (1 to 9):

☐ [**Please specify**]

11. Recognised certificates

Existence of recognised certificates relating to the above requirements (e.g. the ISO 27000 series):

☐ [**Please specify**]

Appendix 4: Sub-processors

Name and address of the sub-processors	Subject matter, nature and duration of the sub-contracting
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany	Hosting of the web application, cloud server, storage and processing of personal data (website, database, backups). Duration: for the term of the hosting contract.
Stripe Technology Company Limited, One Wilton Park, Wilton Place, Dublin 2, D02 FX04, Ireland	Payment processing for online payments, processing of payment and transaction data, and fraud prevention. Duration: for the duration of use of the payment service.