DATA PROCESSING AGREEMENT LEARNING

Compliance.One GmbH (hereinafter "Contractor" or "Compliance.One") provides the Customer with a web-based learning platform (hereinafter "Platform") and training content. The Customer can use its access to the Platform to provide its employees with training content in areas such as data protection, information security, compliance, occupational/workplace health and safety, etc. Some of the training content also contains examination questions (quizzes), upon successful completion of which participants can receive a certificate confirming successful participation. The Platform also provides evaluations of participation and results. On request and on the basis of a separate order, the Customer can also store its own training content on the Platform and make it available to its users. The Platform processes personal data of the Customer's employees on behalf of the Customer.

This Data Processing Agreement, as part of the main contract between the parties, specifies the obligations of both parties to comply with the applicable data protection law, in particular the requirements of the General Data Protection Regulation ("GDPR").

1. Scope

The Contractor processes personal data on behalf of the Customer. The subject matter of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects are set out in the Service Agreement and in **Annex 1** to this Data Processing Agreement.

If the Customer itself acts as a processor (in particular if the Customer makes the learning platform available to affiliated companies or their employees), the Contractor shall act as a sub-processor of the Customer. In this scenario, the data controller may assert the rights arising from this Data Processing Agreement directly against the Contractor as a sub-processor.

2. Instructions

2.1 The Contractor may only process data of data subjects within the scope of the order and the documented instructions of the Customer. The instructions are initially set out in the main contract and may subsequently be amended, supplemented, or replaced by the Customer in text form, unless they have been issued irrevocably. Verbal instructions must be confirmed by the Customer immediately in text form.

2.2 If the Contractor is obliged to process personal data under the law of the Union or of the Member State to which the Contractor is subject, the Contractor shall inform the Customer thereof in writing prior to the respective processing, unless the law prohibits such information for important reasons of public interest. In the latter case, the Contractor shall inform the Customer immediately as soon as this is legally possible.

2.3 The Contractor shall inform the Customer immediately if it is of the opinion that an instruction violates applicable laws. The Contractor may suspend the implementation of the instruction until it has been confirmed or amended by the Customer.

3. Technical and Organizational Measures

3.1 The Contractor commits himself to the Customer to comply with the technical and organizational measures required to comply with the applicable data protection regulations. This includes, in particular, the requirements of Art. 32 GDPR.

3.2 The status of the technical and organizational measures in place at the time of the conclusion of the contract is documented in **Annex 2** to this Data Processing Agreement. The parties agree that changes to the technical and organizational measures may become necessary, in order to adapt to technical and legal circumstances. The Contractor reserves the right to change the security measures taken, although it must be ensured that the contractually agreed level of protection is not undercut. The Customer can request an up-to-date overview of the technical and organizational measures taken by the Contractor at any time.

4. Data Subject Rights

4.1 The Contractor shall support the Customer within the scope of its possibilities in fulfilling the requests and claims of data subjects in accordance with Chapter III of the GDPR (in particular information,

correction, blocking, or deletion). Insofar as the cooperation of the Contractor is necessary for the protection of data subjects' rights by the Customer, the Contractor shall take the necessary measures in each case in accordance with the Customer's instructions. Where possible, the Contractor shall support the Customer with suitable technical and organizational measures in fulfilling its obligation to respond to requests to exercise data subject rights.

4.2 The Contractor may only provide information to third parties or the data subject with the prior consent of the Customer. The Contractor shall forward any requests addressed directly to it to the Customer without delay.

5. Other obligations of the Contractor

5.1 The Contractor shall inform the Customer immediately, at the latest within 24 hours, if it becomes aware of any breaches of the Customer's personal data protection.

5.2 In connection with the commissioned processing, the Contractor shall support the Customer in drawing up and updating the list of processing activities and, if necessary, in carrying out a data protection impact assessment. All necessary information and documentation shall be made available to the Customer immediately upon request.

5.3 If the Customer is subject to inspection by supervisory authorities or other bodies or if data subjects assert rights against the Customer, the Contractor undertakes to support the Customer to the extent necessary, insofar as the processing in the order is affected.

5.4 The persons employed by the Contractor for processing have committed themselves in writing to confidentiality, have been familiarized with the relevant provisions of data protection, and are appropriately instructed and monitored on an ongoing basis with regard to compliance with data protection requirements.

5.5 The Contractor shall support the Customer in complying with the obligations set out in Articles 32 to 36 GDPR, taking into account the nature of the processing and the information available to it.

5.6 The Customer can contact the Contractor's data protection officer at any time with questions regarding data protection at the Contractor. The Contractor's data protection officer is the lawyer Conrad Graf, e-mail: privacy@compliance.one

6. Rights and Obligations of the Customer

6.1 The Customer alone is responsible for assessing the permissibility of the commissioned processing and for safeguarding the rights of data subjects.

6.2 The Customer shall be entitled to monitor the Contractor's compliance with the data protection regulations and the contractual agreements to an appropriate extent itself or through third parties. The persons entrusted with the inspection shall be granted access and insight by the Contractor to the extent necessary and possible. The Contractor shall be obliged to provide the necessary information, demonstrate processes, and provide the evidence required to carry out an inspection. Inspections at the Contractor's premises must be carried out without any avoidable disruption to business operations. Unless otherwise indicated for urgent reasons to be documented by the Customer, inspections shall take place after reasonable advance notice and during the Contractor's business hours and not more frequently than every 12 months.

7. Sub-processors

7.1 The commissioning of sub-processors by the Contractor is only permitted with the consent of the Customer.

7.2 The Customer agrees to the commissioning of sub-processors in accordance with the overview of sub-processors, attached as **Annex 3**. The overview of sub-processors also defines the process for future changes to the sub-processors.

7.3 The Contractor shall carefully select the sub-processors and check that they can comply with the agreements made between the Customer and the Contractor before commissioning them. In particular, the Contractor shall check that all sub-processors have taken the technical and organizational measures required under Art. 32 GDPR to protect personal data.

7.4 Services that the Contractor uses from third parties as a purely ancillary service in order to carry out the business activity are not to be regarded as subcontracting relationships within the meaning of this agreement on data processing. These include, for example, cleaning services, pure

telecommunication services without any specific reference to services that the contractor provides for the Customer, postal and courier services, transportation services, and security services.

7.5 The commissioning of sub-processors shall not affect the Contractor's contractual and data protection obligations towards the Customer. The Contractor shall be liable for any poor performance of a subcontracted processor as if it were its own fault.

8. Data Transfer to Third Countries

The data processing takes place exclusively within the European Union or the EEA and/or in third countries for which an adequacy decision has been issued by the EU Commission. Any relocation of the order processing to an "unsafe" third country requires the express approval of the Customer.

9. Deletion and Return of Personal Data

9.1 Copies or duplicates of the data are not created without the knowledge of the Customer. Excluded from this are backup copies, insofar as they are necessary to ensure proper data processing, as well as data required to comply with statutory retention obligations.

9.2 After termination of the service agreement or earlier at the request of the Customer, the Contractor must hand over the personal data processed in the order to the Customer or delete it in accordance with data protection regulations.

9.3 Documentation that serves as proof of proper data processing in accordance with the order must be retained by the contractor beyond the end of the contract in accordance with the respective retention periods.

ANNEX 1: DESCRIPTION OF DATA PROCESSING

Controller and Processor

The Customer is the controller within the meaning of the GDPR and uses the Contractor's learning platform to make training content available to its employees and, under certain circumstances, to third parties. As the processor, the Contractor provides the learning platform to the Customer as Software-as-a-Service (SaaS).

Data Subjects

The personal data processed in the order concerns the employees invited to participate in certain learning content via the learning platform and, under certain circumstances, third parties invited by the Customer to participate in certain learning content (e.g. freelancers or employees of affiliated companies).

Categories of Data

Within the scope of data processing, the following personal data may be processed by the Contractor on behalf of the Customer:

- First name, surname of the employees or participants;
- E-mail address of employees or participants;
- Login information for employees and participants;
- Department or area in which the person concerned works (e.g. HR department for specific training for employees of the HR department);
- Personal/identification number;
- Training courses assigned to the person concerned for participation;
- Invitations to participate sent by e-mail or reminders in the event of late participation;
- technical information required for the provision of the landing page or the user interface of the learning platform, including the assigned training courses (user ID, IP address, device information, timestamp);
- Participation in trainings (progress of participation, if applicable, participation in quizzes and results);
- Successful completion of participation including the award of a certificate if applicable.

Special Categories of Data

The processing of special categories of personal data is not intended and is not necessary for the use of the learning platform.

Subject and Duration of Processing

The personal data processed in the order are processed for the performance of the contractor's services agreed in the main contract or the data processing agreement. The data is processed on the instructions of the Customer, as defined in the data processing agreement.

The data will be deleted at any time at the instruction of the Customer, as defined above. The Customer can also define specific retention and deletion periods. The data will be deleted upon termination of the contract.

The Customer can export the data at any time.

The term of this Data Processing Agreement is based on the term of the main contract.

ANNEX 2: TECHNICAL AND ORGANIZATIONAL MEASURES

With regard to the technical and organizational measures, please refer to the ISO 27001 certification of Compliance.One GmbH. The certificate is available at www.compliance.one/legal. In addition to the ISO 27001 certification, an overview of the technical and organizational measures is provided below:

1. CONFIDENTIALITY

1.1 Physical Access Control

The software is hosted in Hetzner Online GmbH's data centers in Germany.

The technical and organizational measures taken in the data centers of the sub-processor Hetzner Online GmbH are described in detail here: https://www.hetzner.com/AV/TOM.pdf

1.2 System Access Control

The following measures have been taken by Compliance.One for system access control:

In order to gain access to IT systems, users must have the appropriate access authorization. For this purpose, appropriate user authorizations are assigned by administrators.

Access to IT systems is granted exclusively through the use of SSH keys with a minimum key length of 4096 bits. Each key is additionally protected by a secure passphrase. Key pairs are regularly reviewed and are rotated at least once per year.

Access to production systems is only possible via designated jump hosts. Direct connections from external networks to servers are strictly prohibited to ensure the highest level of security.

This architecture ensures that only authorized users with preconfigured access keys and through centrally managed access points are able to reach internal systems.

Remote access to Compliance.One IT systems always takes place via encrypted connections.

An intrusion prevention system is used on Compliance.One's servers. All server and client systems are equipped with anti-virus software that guarantees a daily supply of signature updates. All servers are protected by firewalls that are constantly maintained and supplied with updates and patches.

The access of servers and clients to the Internet and the access to these systems via the Internet is also secured by firewalls. This also ensures that only the ports required for the respective communication can be used. All other ports are blocked accordingly.

All employees are instructed to lock their IT systems when they leave them. Passwords are always stored in encrypted form.

1.3 Data Access Control

Authorizations for Compliance.One IT systems and applications are set up exclusively by administrators.

Authorizations are always assigned according to the need-to-know principle. This means that only those people who maintain and service these data, applications, or databases or are involved in their development are granted access rights to them.

The prerequisite is a corresponding request for authorization for an employee by a supervisor.

There is a role-based authorization concept with the option of assigning differentiated access authorizations, which ensures that employees receive access rights to applications and data depending on their respective area of responsibility and, if necessary, on a project basis.

Employees are generally prohibited from installing unauthorized software on IT systems.

All server and client systems are regularly updated with security updates.

1.4 Separation

All IT systems used by Compliance.One for Customers are multi-client capable. The separation of data from different Customers is always guaranteed.

1.5 Pseudonymization and Encryption

Administrative access to server systems is always via encrypted connections. In addition, data on server and client systems is stored on encrypted data carriers. Appropriate hard disk encryption systems are in use.

2. INTEGRITY

2.1 Input Control

The entry, modification and deletion of personal data processed by Compliance.One on behalf of the Customer is always logged.

Employees are obliged to always work with their own accounts. User accounts may not be shared or used jointly with other persons.

2.2 Transfer Control

Personal data that is passed on on behalf of Customers of Compliance.One may only be passed on to the extent that this has been agreed on with the Customer or is necessary for the provision of the contractual services for the Customer.

All employees working on a Customer project are instructed on the permissible use of data and the modalities of data disclosure.

As far as possible, data is transmitted to recipients in encrypted form.

The use of private data carriers is prohibited for employees at Compliance.One.

Employees at Compliance.One receive regular training on data protection issues. All employees are obliged to handle personal data confidentially.

3. AVAILABILITY AND RESILIENCE

Data on Compliance.One server systems is backed up incrementally at least daily and "fully" weekly. The backup media are encrypted and moved to a physically separate location.

The import of backups is tested regularly.

The IT systems have an uninterruptible power supply. There is a fire alarm system and a CO2 extinguishing system in the server room. All server systems are subject to monitoring, which immediately triggers messages to an administrator in the event of errors.

Compliance.one has an emergency plan that also includes a restart plan.

4. ORDER CONTROL

Data processing takes place exclusively in the European Union.

Compliance.One appointed a data protection officer.

When subcontracted processors are involved, a data processing agreement is concluded in accordance with the provisions of the applicable data protection law following a prior audit by Compliance.One's data protection officer. Contractors are also regularly monitored during the contractual relationship.

5. PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

At Compliance.One, care is taken during the development of the software to ensure that the principle of necessity is already taken into account in connection with user interfaces. For example, form fields and screen masks can be designed flexibly.

The Compliance.One software supports input control with a flexible and customizable audit trail that enables unalterable storage of changes to data and user authorizations. Authorizations for data or applications can be set flexibly and granularly.

6. PROCEDURES FOR REGULAR REVIEW, ASSESSMENT AND EVALUATION

A comprehensive data protection management system is implemented at Compliance.One. There is a guideline on data protection and information security and policies to ensure the implementation of the guideline's objectives.

The guideline and the policies are regularly evaluated and adjusted with regard to their effectiveness.

A Data Protection and Information Security Team is in place to plan, implement, evaluate and make adjustments to data privacy and information security measures.

In particular, it is ensured that data protection incidents are recognized by all employees and reported to the team without delay. The team will investigate the incident immediately. If data processed on behalf of customers is affected, care is taken to ensure that they are informed immediately about the nature and scope of the incident.

ANNEX 3: OVERVIEW OF SUB-PROCESSORS

Compliance.One uses the following sub-processors to provide the services under the main contract:

Sub-processor	Services of the sub-processor	Location of the DP
Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen, Germany	Hosting of the learning platform	EU
Sendinblue GmbH Köpenicker Straße 126, 10179 Berlin, Germany	Sending transactional emails (Brevo email sending platform)	EU
Friendly Captcha GmbH Am Anger 3-5, 82237 Wörthsee, Germany	Fraud and bot prevention and defense	EU
BunnyWay d.o.o. Dunajska cesta 165, 1000 Ljubljana, Slovenia	Content Delivery Network (CDN)	EU

The Contractor may terminate the commissioning of individual sub-processors or commission additional sub-processors. When commissioning additional sub-processors, the Contractor shall inform the Customer of the planned deployment of the additional sub-processor by electronic means at least 30 days prior to the deployment of the additional sub-processor. If the Customer has a material reason to object to the use of a sub-processor, the Customer shall notify the Contractor of this in writing no later than 15 days after being informed of the planned use of the sub-processor, stating the material reason. If the Customer does not object within this period, the use of the additional sub-processor shall be deemed to have been approved by the Customer.

Should the Customer object, the Contractor may cure the objection as follows: (1.) the Contractor shall not use the additional sub-processor to process the Customer's personal data, or (2.) the Contractor shall take measures to remove the substantial ground for the Customer's objection, or (3.) the Contractor may temporarily or permanently cease providing the aspect of the service to the Customer affected by the use of the additional sub-processor and refund to the Customer any remuneration paid in advance for the provision of the aspect of the service. If none of these three options is feasible and the objection has not been remedied within 15 days of receipt of the objection, either party may terminate the contract extraordinarily with reasonable notice.