privacy train

Version 06/21/2022

Data Processing Agreement privacy train (DPA privacy train)

between

datenschutz nord GmbH

Konsul-Smidt-Str. 88, 28217 Bremen

as licensor

(Processor)

and

privacy train Licensee

(Controller)

Preamble

The Processor shall provide the eLearning privacy train to the Controller on the basis of a BASIC license or an LMS license. Since the Processor processes personal data in this context on behalf of and in accordance with the instructions of the Controller, the Parties conclude - in addition to the License Agreement - the present contract for commissioned processing.

1 Subject matter and Term

(1) The Processor shall carry out the data processing listed in **Annex A.1**. It shall describe the subject matter, nature, purpose and duration of the processing as well as the categories of data processed and data subjects.

(2) This Agreement shall enter into force - unless otherwise agreed - upon conclusion of the General Terms and Conditions (privacy train) and shall apply for as long as the Processor processes personal data for the Controller.

§ 2 Instructions by the Controller

(1) The Processor shall process personal data only for the purposes listed in **Annex A.1** or on documented instructions from the Controller, unless the Processor is required to process certain personal data by law of the Union or a Member State to which the Processor is subject. In such a case, the Processor shall notify the Controller of those legal requirements prior to the processing, unless the law in question prohibits such notification on grounds of substantial public interest.

(2) The Processor shall immediately inform the Controller if, in its opinion, an instruction of the Controller infringes the Union or a Member State data protection law.

(3) Processing of the personal data provided by the Controller for other purposes than listed in **Annex A.1**, in particular for its own purpose, is not permitted.

§ 3 Technical and organisational measures

(1) The Processor shall undertake to implement the technical and organisational measures specified in **Annex A.2** to ensure the security of personal data. The measures shall ensure a level of protection appropriate to the risk involved in processing the data in scope of this Agreement. In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context, purposes of the processing and categories of data (in particular pursuant to Article 9(1) or Article 10 of the GDPR), as well as the different probabilities of occurrence and the severity of the risk for the data subjects.

(2) The technical and organisational measures listed in **Annex A.2** are subject to technical progress and further development. They shall be adapted by the processor if the agreed level of security can no longer be guaranteed. The adaptation may only be carried out if they at least provide the same level of protection achieved when previous measures were in force. Unless otherwise stipulated, the Processor shall notify the Controller of the adjustments made willingly and without undue delay.

§ 4 Obligations of the processor

(1) The Processor confirms that it is aware of the relevant data protection regulations. The Processor shall organise the internal operating procedures within its area of responsibility in such a way that it meets the special requirements of an effective data protection management program.

(2) The Processor shall grant access to the personal data undergoing processing to only to those employees familiar with the Data Protection Law in force and to the extent strictly necessary for implementing, managing and monitoring of the Agreement. The Processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(3) To the extent required by law, the Processor shall appoint a data protection officer and provide his/her contact details in **Annex A.1**. The Processor shall inform without delay and unrequested about any change of the Data Protection Officer.

(4) The Processor shall carry out the processing in the territory of the Federal Republic of Germany, in a Member State of the European Union or within the European Economic Area. Any transfer of data to a third country by the Processor shall be done only on the basis of documented instructions from the Controller and shall take place if the specific legal requirements of the GDPR are met.

§ 5 Assistance to the Controller

(1) The processor shall promptly notify the controller of any request it has received from the data subject. The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing.

(2) In addition to the processor's obligation to assist the controller pursuant to Clause 5(1), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

   a. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment');

   b. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

(3) The Processor shall provide assistance in reviewing data breaches and implementing any notification obligations, as well as in complying with the obligation to ensure that personal data is accurate and up to date.

(4) Furthermore, the Processor shall assist with appropriate technical and organisational measures to enable the Controller to fulfil its existing obligations towards the data subject.

§ 6 Use of sub-processors

(1) The Processor has the Controller's general authorisation for the engagement of sub-processors. The Processor shall specifically inform the Controller in writing, of any intended sub-processing or change in sub-processors at least three weeks prior, thereby giving the Controller sufficient time to be able to object to such changes. The Processor shall provide the Controller with the information necessary to enable the Controller to exercise the right to object. The Controller hereby agrees that the Processor will engage the following sub-processor:

Sub-processor (name, legal form, registered office)	**Processing location**	**Type of service**
PLUTEX GmbH, Bremen (Germany)	Bremen (Germany)	Hosting, Managed Services

(2) The Processor warrants that it will only use external hosting service providers that are certified to ISO/IEC 27001 or other equivalent standards at the time of subcontracting. Where the Processor engages a sub-processor for carrying out specific processing activities (on behalf of the Controller), it shall do so by way of a written contract, which may also be concluded in an electronic format, which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with the clauses in this Agreement. At the Controller's request, the Processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the Controller. The Processor shall remain fully responsible to the Controller for the performance of the sub-processor's obligations in accordance with its contract with the Processor. The Processor shall notify the Controller of any failure by the sub-processor to fulfil its contractual obligations without undue delay.

(3) The Processor shall ensure compliance with the provisions of Articles 44 to 50 of the GDPR in the event of a subcontracting involving a transfer of personal data

within the meaning of Chapter V of the GDPR by providing, where necessary, appropriate safeguards in accordance with Article 46 of the GDPR.

(4) Where the Processor engages a sub-processor in processing activities which involves a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the Processor and the sub-processor shall ensure compliance with Chapter V of GDPR by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) GDPR, provided the conditions for the use of those standard contractual clauses are met.

(5) In the case of Section 6(4), the Processor shall carry out the assessment in accordance with Articles 14 and 15 of the Standard Contractual Clauses and make it available to the Controller upon request. If the Processor or the Controller come to the conclusion that further measures need to implemented to ensure an adequate level of protection, these measures shall be implemented by the Processor or the sub-processor respectively. The sub-processor may only be involved in the data processing once an adequate level of protection has been ensured.

§ 7 Documentation and compliance

(1) The Processor shall provide the Controller with all information necessary to demonstrate compliance with the obligations set out in this Agreement and adapted directly from the GDPR. At the Controller's request, the Processor shall also allow and contribute to audits of the processing activities covered by this Agreement, at reasonable intervals or if there are indications of non-compliance of any required regulations. In deciding on a review or an audit, the Controller may take into account relevant certifications within the meaning of Article 28(5) GDPR held by the Processor.

(1) The Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Processor and shall, where appropriate, be carried out with reasonable notice and in a manner that complies with the Processor's business and confidentiality obligations and, where possible, without disrupting operations.

(2) The Parties shall make the information referred to in this Agreement, including the results of any audits, available to the competent supervisory authority/ies on request.

§ 8 Infringements to be notified

(1) The Processor shall inform the Controller without undue delay of any disruptions to operations that entail risks for the Controller's data, as well as when data protection breaches in connection with the Controller's data become known. The same shall apply if the Processor establishes that the security measures taken by the Processor do not meet the legal requirements.

(2) The Processor is aware that the Controller is under an obligation to comprehensively document all breaches of personal data protection and, if necessary, to report them to the supervisory authority/ies or the data subject. The Processor shall notify the Controller without undue delay after the Processor having become aware of the breach. Such notification shall contain, at least:

- Description of the nature of the breach, including, where possible, the categories and approximate number of individuals and data sets affected,
- Name and contact details of contact persons for further information,
- a description of the likely consequences of the injury, and
- a description of the measures taken or proposed to correct the breach or mitigate the resulting adverse effects.

§ 9 Termination

(1) Following termination of the Agreement, the Processor shall delete or return all personal data processed on the behalf of the Controller unless the Union or a Member State law requires storage of the personal data. This shall also apply to any existing copies in accordance with the technical and organizational measures taken. The Processor shall notify the Controller of the deletion and return of the data in writing.

(2) the Controller may terminate the contractual relationship without notice if the Processor commits a serious breach of the provisions of this Agreement or of data protection regulations and the Controller cannot reasonably be expected to continue the contractual relationship until the conclusion of the notice period or until the agreed termination of the Agreement.

(3) The Processor may terminate the contractual relationship without notice if the Controller insists on the fulfilment of its instructions even though such instructions violate applicable legal requirements or this Agreement and the Processor has notified the Controller thereof.

§ 10 Accession to the Agreement

Any entity that is not a Party to this Agreement may, with the agreement of all the Parties, accede to this Agreement at any time as a controller or a processor by means of a declaration of accession. In addition to the declaration of accession, Annexes 1 to 3 shall be completed where necessary. From the date of accession, the acceding entity shall be treated as a Party to this Agreement and have the rights and obligations of a controller or a processor, in accordance with its designation.

§ 11 Final provisions

(1) If the property of the Controller which is held by Processor is at risk by actions of third parties (for example by attachment or seizure), by insolvency proceedings or by other events, the Processor shall notify the Controller immediately. A right of retention is excluded with regard to data carriers and data files of the Controller.

(2) The grounds for the Agreement, amendments to the Agreement and ancillary agreements must be in writing, which may also be in an electronic format.

(3) In the event of any conflict between these contractual clauses and the provisions of related agreements existing between the parties or subsequently entered into or concluded, these clauses shall prevail.

(4) Should any provision of this Agreement become invalid, that shall not affect the validity rest of the Agreement.

A.1. listing of the commissioned services and contact details of the data protection officers

Subject of processing	**LMS License:** Operation of a learning management system to deliver online training to the Controller's employees. **BASIC License:** Operation of password-protected Internet access to the course content ordered and provided on the Processor's server.
Nature and purpose of processing	**LMS License:** User management and documentation of training status in the Processor's LMS. **BASIC License:** Management of a group account for access to the ordered course content in the Processor's LMS.
Type of personal data	**LMS License:** Name, first name, title, e-mail address, learning progress (course not yet started, course started, and course completed), time of last status change, company affiliation, and, if applicable, location and department. IP addresses, insofar as these are required for the technical delivery of the content. Tracking based on IP addresses does not take place. **BASIC License:** E-mail address and, if applicable, surname and first name of the coordinator on the part of the Controller. IP addresses, insofar as these are required for the technical delivery of the content. Tracking does not take place.
Categories of data subjects	**LMS License:** Employees of the Controller as well as self-employed persons (freelancers) used by the Controller (training participants). **BASIC License:** The coordinator on the Controller's side, training participants.

Name and contact details of the Processor's data protection officer	Joanna Maxine Stünkel, office@datenschutz-nord.de

A.2 Technical and organizational security measures

This appendix documents the technical and organizational measures implemented by the Processor to properly fulfil the service provided.

1. Pseudonymization

Personal data is always pseudonymized, insofar as this is possible according to the intended use and does not require a disproportionate effort in relation to the intended protective purpose. If IP addresses are required for the delivery of content, they are not stored or are anonymized immediately.

2. Encryption

The training platform can only be accessed via a connection with https encryption. Administrative access to the server system is also only possible from the Controller's company network.

3. Confidentiality

a) Physical Access

Access control measures (intended to prevent unauthorized persons from gaining access to data processing facilities with which personal data are processed or used):

aa) Data Center:

The entrance door to the data center (particularly resistant) is equipped with an electronic locking system (key card and PIN code). Access is logged on a person-by-person basis. The data center has no windows and is equipped with an intrusion alarm system.

bb) Office Space:

All entrance doors to the offices are equipped with electronic locking systems (RFID chips). Even during business hours, all entrance doors are locked and can only be opened by handle from the inside or with a suitable key. Outside business hours, the offices are monitored by a burglar alarm system (alarms are activated by a security service). Visitors are only allowed on the office floors when accompanied by an employee.

b) System Access

Access control measures (to prevent data processing systems from being used by unauthorized persons):

aa) Administrative access points:

Administrative access to the training platform requires the entry of a username and password. The administrator passwords contain between 11 and 20 characters, consist of upper and lower case letters as well as special characters and numbers. Logged in administrator accounts are automatically logged out after 5 minutes of inactivity at the latest. On the server side, administrative activities can only be performed from the Processor's corporate network

bb) Controller-systems:

When logging in to the system, the username and password are requested. The passwords used must contain at least 8 characters and consist of upper and lower case letters, special characters and numbers. Passwords must also be changed every 90 days. In this case, the last 10 passwords used are locked. After 5 minutes of inactivity,

the system is locked and can only be unlocked using the password. All access control security requirements are enforced by the system

c) Data Access

Access control measures (intended to ensure that those authorized to use a data processing system can only access the data subject to their access authorization, and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage):

Access rights are assigned strictly according to the need-to-know principle based on authorization concepts.

User accounts can only be created, deleted and modified by an administrator.

aa) LMS License

Each user can only view their own learning status (course completed, course in progress, or course not yet completed) and has no access to the other users' data (other users are invisible to them). The learning status is logged as follows: Course Edited (green), Course in Progress (yellow), and Course Not Yet Edited (grey). Each status change is also logged with date and time.

A coordinator can be appointed who is allowed to view the learning status of all users within the Controller with extended rights.

bb) BASIC License

The Controller receives a single user account for the BASIC Controller. This account is configured in such a way that only the ordered course modules are accessible in the system. Neither the own profile data nor the other users can be viewed in the database.

d) Data Transfer

Transfer control measures (Shall ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or during its transport or storage on data carriers, and that it is possible to check and determine to which entities a transfer of personal data is intended by data transmission facilities):

Access to the privacy train training platform is encrypted with https.

e) Data Separation

Measures to implement the separation requirement (Shall ensure that data collected for different purposes can be processed separately):

Separate databases (LMS license) as well as logical data separation (BASIC license) ensure that the data of one Controller is processed separately from the data of other Controllers.

4. Integrity

Input control measures (to ensure that it is possible to check and determine retrospectively whether and by whom personal data has been entered into, modified or removed from data processing systems):

The creation and modification of a user account is logged by the system. The same applies to the learning status of participating users (only relevant for the LMS license, see also access control).

5. Availability

a) Availability Control

Availability control measures (Shall ensure that personal data is protected against accidental destruction or loss):

The training platform's data inventory is backed up incrementally on a weekly basis and fully on a weekly basis. An uninterruptible power supply prevents the data stock from being damaged in the event of a sudden power failure. The data center is air-conditioned and has appropriate fire protection measures. All systems have up-to-date virus protection. Security-relevant software updates are installed immediately.

b) Processor control

Order control measures (to ensure that personal data processed on behalf of the Controller can only be processed in accordance with the Controller's instructions):

Data Processing Agreements in accordance with Art. 28 GDPR have been concluded with all Sub-Processors.

6. Resilience of Systems

Resilient systems (hardware and software) are used that can withstand the expected stresses in terms of storage, access and line capacities.

7. Regular Reviews

The technical and organizational measures are reviewed on an ongoing basis and adapted to the state of the art if necessary.