Data processing agreement (DPA) based on the standard contractual clauses of the commission according to ART. 28 (7) GDPR

between

_____
_____
_____

hereinafter referred to as **“Controller”**

lawpilots GmbH
Am Hamburger Bahnhof 3
10557 Berlin
Germany

hereinafter referred to as **“Processor“**

Inhaltsverzeichnis

Preamble

A contractual relationship within the meaning of Art. 28 of the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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, “GDPR”) exists between the controller and the processor.

This data processing agreement including all annexes (hereinafter jointly referred to as the “Agreement”) specifies the data protection obligations of the parties arising from the underlying contract, the service agreement and/or order description including all annexes (hereinafter jointly referred to as the “Main Contract”). Where reference is made to the provisions of the German Federal Data Protection Act (hereinafter referred to as “BDSG”), this refers to the Act on the Adaptation of Data Protection Law to Regulation (EU) 2016/679 and on the Implementation of Directive (EU) 2016/680 in the version applicable as of May 25, 2018.

The processor undertakes vis-à-vis the controller to fulfill the main contract and this agreement in accordance with the following provisions:

General Provisions

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with [choose relevant option: OPTION 1: Article 28(3) and (4) of 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, in the following: GDPR).

(b) The controllers and processors listed in **Annex II** have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) GDPR.

(c) These Clauses apply to the processing of personal data as specified in **Annex III**.

(d) **Annexes I** to **V** are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of GDPR.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of the GDPR.

Invariability of the Clauses

The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

Interpretation

(a) Where these Clauses use the terms defined in the GDPR, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of the GDPR.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Hierarchy

(a) In the event of a contradiction between this Data Processing Agreement and the provisions of any related agreements between the Parties existing or subsequently entered into or concluded (such agreements hereinafter also referred to as **"Principal Agreement"**), the provisions of this Data Processing Agreement shall prevail.

(b) In the event of a conflict between the supplementary clauses in Annex I and other provisions of this Data Processing Agreement, the other provisions of this Data Processing Agreement shall take precedence over the supplementary clauses in Annex I.

Obligations of the parties

Beschreibung der Verarbeitung

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex III.

Description of processing(s)

6.1 Instructions

(a) 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 this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe the GDPR or the applicable Union or Member State data protection provisions.

6.2 Purpose limitation

(a) The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex III, unless it receives further instructions from the controller.

6.3 Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex III.

6.4 Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex IV to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). 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 and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. 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.

6.5 Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

6.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from the GDPR. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) 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.

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

6.7 Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least four weeks in advance, thereby giving the controller sufficient time (within 2 weeks of receipt of the information) to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) The list of sub-processors authorised by the controller can be found in Annex V. The Parties shall keep Annex V up to date.

(c) 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 contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to the GDPR.

(d) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(e) 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.

(f) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

6.8 International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of the GDPR.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 6.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data or not exclude within the meaning of Chapter V of the GDPR, the processor and the sub-processor can ensure compliance with Chapter V of the GDPR by by using either the adequacy decision or the standard data protection clauses adopted by the Commission pursuant to Article 46(2) of the GDPR (also referred to as "standard contractual clauses"), provided that the conditions for the application of these standard data protection clauses are met.

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) 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. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), 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:

(1) 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') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) 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 obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 GDPR.

(d) The Parties shall set out in Annex IV the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 GDPR, taking into account the nature of processing and the information available to the processor.

4.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) GDPR, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 GDPR, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

4.2 Data breach concerning data processed by the processor

(a) In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(1) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(2) the details of a contact point where more information concerning the personal data breach can be obtained;

(3) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

(b) Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) The Parties shall set out in **Annex III** all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 GDPR.

Final provisions

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of the GDPR, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under the GDPR;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to the GDPR.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

Annex I. Supplementary provisions

General Provisions

(a) **Scope:** The clauses contained in this Agreement shall apply to all services involving processing of personal data by the Processor on behalf of the Controller within the meaning of Art. 28 GDPR.

(b) **Form:** Any amendments or additions to this Agreement shall be made at least in text form and must expressly state that they amend and/or add to these provisions. This also applies to a waiver of this text form requirement. Insofar as this Agreement stipulates the written form, the written form as defined by Sect. 126b of the German Civil Code ("Bürgerliches Gesetzbuch", "BGB") shall be sufficient.

(c) **Choice of law:** This Agreement is subject to German law.

(d) **Place of jurisdiction:** The place of jurisdiction shall be Berlin.

Special Provisions

(a) **Designation of Processing Instruction Recipients:** Insofar as the Processor deems it necessary, the Processor may designate specific persons on the Processor's side (including specific contact details) to whom the Controller shall exclusively address its instructions regarding the processing of personal data. The Processor shall inform the Controller of these persons and contact details in writing. Insofar as the Processor makes use of this right, the Controller shall be obliged to address all instructions in accordance with the provision in Clause 7.1 (a) exclusively to the persons designated by the Processor and their respective contact details. In the event that these persons on the Processor's side or their respective named contact details change, the Processor shall notify the Controller of this, specifying the new person or the respective new contact details.

(b) **Unlawful Instructions:** If the Controller issues any instruction to the Processor which the Processor considers to be in breach of the GDPR or applicable EU or EU Member State data protection legislation (Clause 7(1)(b)), the Processor shall be entitled to suspend execution of such instruction until it is confirmed or amended by the Controller. This right is in addition to the right of termination provided for in Clause 10(c) of this Agreement.

(c) **Security of Processing:** The Processor may update and amend the technical and organisational measures set out in Annex IV, provided that such updates and/or amendments do not substantially reduce the overall level of protection afforded by the measures.

(d) **Subprocessors:** The following shall apply in addition to Clause 7(7)(a): In the event of a refusal of the authorisation or an objection, the Processor may, at its own discretion, provide the service without the intended change or propose an alternative subprocessor and agree on engagement of such subprocessor with the Controller. If it would be unreasonable to expect the Processor to provide the service without the intended change – for example because this would entail disproportionate expenses for the Processor – or if it is not possible to agree with the Controller on another subprocessor, then the Controller and the Processor shall be entitled to terminate this Agreement as well as the Principal Agreement, subject to a notice period with one month's notice to the end of the month.

(e) **Industry-Specific Confidentiality Obligations:** Insofar as the Controller is subject to particular mandatory statutory obligations, it shall inform the Processor accordingly.

(f) **Liability:**

(1) The Processor's liability shall be excluded in all cases where the Processor acts in accordance with this Agreement and in accordance with the processing instructions issued by the Controller.

(2) The Controller's liability towards the Processor shall also extend to any fines imposed on the Processor, insofar as such fines are attributable to the culpable breach of Controller's obligations under data protection law by the Controller, its employees or its agents. If, as a result of such breach, an order imposing a fine on the Processor becomes final, the Controller shall indemnify the Processor, and hold the Processor harmless, from the fine imposed, with the amount of such release determined in accordance with the internal proportion of liability in relation between the Parties.

The proportion of the fine to be borne by the Controller shall depend on its share of responsibility for the breach sanctioned by the fine. In any event, the aforementioned liability on the part of the Controller shall be subject to the condition precedent that the Processor notifies the Controller in writing without undue delay of any such case, does not acknowledge the alleged breach, and conducts any judicial or extrajudicial dispute, including any out-of-court settlement, only in consultation with the Controller.

The Controller may in particular request that the Processor have any fine notices judicially reviewed by all available competent bodies, in which case the Controller shall be obligated to indemnify the Processor, and hold the Processor harmless, from the legal costs incurred in the amount of the statutory fees.

(3) The Controller shall indemnify the Processor, and hold the Processor harmless, from any claims for damages by data subjects in connection with a breach of data protection provisions which they assert against the Processor, unless such claims are based on the fact that the Processor is in breach of obligations specifically directed to it as a Processor, or has processed personal data on the Controller's behalf without or contrary to a processing instruction from the Controller. The provisions in the above Clause 13(b)(2) Sentence 4 and 5 of this Annex I shall apply accordingly.

(g) **Fee:** To the extent permitted by law, the Processor shall be entitled to remuneration and reimbursement of its own costs for assisting with any inspections carried out by or on behalf of the Controller.

Annex II. List of parties

Controller: *[Name and contact details of the Controller(s) and, if applicable, of the Controller's data protection officer]*

Name:

_____

Address

_____

Name, role and contact details of the contact person:

_____

Processor: *[Name and contact details of the Processor(s) and, if applicable, of the Processor's data protection officer]*

Name: lawpilots GmbH
Anschrift: Am Hamburger Bahnhof 3
10557 Berlin
Germany

Name, role and contact details of the contact person:

Data Protection Officer:
Nina Ostrerova ISiCO Datenschutz GmbH
Am Hamburger Bahnhof 4
10557 Berlin,
pursuant to Section 38 of the Federal Data Protection Act (BDSG) and Art. 37 of the General Data Protection Regulation (GDPR).

_____
Place, Date

_____
Signature (responsible person)

_____
Place, Date

_____
Signature (processor)

Annex III. Description of the processing

Object of the data processing on the Controller's behalf:
The subject of the order includes the training of employees within the scope agreed with the order processor in accordance with the main contract.

Categories of data subjects whose personal data is processed:

- Interns / working students who are authorized to use the service by the person responsible.
- Employees (permanent staff, trainees, temporary workers, freelancers) who are authorized to use the service by the person responsible.

Categories of personal data processed:

- Personal master data of employees of the controller (surname, first name, form of address, title/academic degree, date of birth)
- Contact details (e-mail address, business telephone number*, address)
- Other employee data (position and department*)
- Training participation data (time, title and language of the training course completed)
- Electronic communication data (IP address, websites accessed, details of the end device used, operating system and browser)

*This personal data of employees is only obtained by booking the Cyber Security Awareness Training.

Nature of data processing:
Transfer, processing and storage of the data listed above.

Purpose(s) for which the personal data is processed on behalf of the Controller:

In order to fulfill the purpose of processing, the controller shall provide the processor with the personal master data and contact data of the employees and, if necessary, other employee data for the provision of documentation of the training services, as described in the main contract.

Duration of processing:
The duration of this agreement corresponds to the duration of the main contract.

In the case of **processing by (sub)processors**, please also indicate the object, nature and duration of the processing (see Annex V).

Annex IV. Technical and organisational measures

Technical and organisational measures

Encryption measures:

Measures or processes by which a clearly readable text / information is converted into an illegible, i.e. not easily interpretable, sequence of characters (ciphertext) with the aid of an encryption process (cryptosystem):

- Symmetric / asymmetric encryption
-

The passwords for Management Cockpit access are encrypted and cannot be interpreted or read.

Pseudonymisation measures:

Measures that reduce the direct reference to a person during processing in such a way that an assignment to a specific data subject is only possible with the use of additional information, which is kept separate from the pseudonym / ID by means of appropriate technical and organisational measures:

If required, participation in the training course can be carried out using pseudonymous TANs. Within this procedure, TANs are generated for each training participant. The assignment of TANs to employees is only possible for the client; it is therefore not possible for lawpilots to draw conclusions about the individual course participants.

Measures to ensure confidentiality

Physical access control:

Measures that physically prevent unauthorised persons from accessing IT systems and data processing equipment with which personal data are processed, as well as confidential files and data carriers:

- Controlled key allocation (chip cards / transponder systems)
- Security locks
- Monitored key issuance, transponder system / code locks

Further measures:

In addition, keys are only issued to managing directors; the locking systems are opened for employees using access chips. The network room is additionally and separately secured with keys.

Equipment access control:

Measures that prevent unauthorised persons from processing or using data protected under data protection law:

- Login with username and password

Further measures:
lawpilots uses a password procedure in which each user receives a personal and individual log-in to the system. The passwords must have a minimum length and contain special characters. In addition, lawpilots uses a password manager so that every account and every log-in can be accessed via an individual and secure password.

Accounts are also automatically locked and can only be accessed again using the password. An authorization concept limits the number of authorized employees and determines which employees have access to which data. Data carriers are encrypted.

Data access control:
Measures to ensure that those individuals authorised to use a particular data processing procedure can only access exclusively such personal data subject to their access authorisation, so that other personal data cannot be read, copied, modified or removed by the respective individual without authorisation during processing, use and storage:

- Use of authorisation concepts (regulations for setting up, classifying user IDs, user groups and rights profiles)
- Processing of personal data complies with the authorisation concept
- Documentation of assigned user IDs, user groups and rights profiles
- Logging of accesses to applications (input, modification and erasure of data)

Further measures:
lawpilots has an integrated authorization concept. Employees are assigned a profile or role depending on their authorization. There is also documentation of which employee has carried out which steps.

Separation control::
Measures to ensure that data collected for different purposes are processed separately and are segregated from other data and systems in such a way that unplanned use of these data for other purposes is excluded:

- A written identity and authorisation management system is in place.
- Authorisation management supports the principle of separation of functions.
- Restrictive assignment of database rights to user and group IDs
- Separate physical storage of clients and the databases used by clients
- Separation of live and test environment (development)

Further measures:
The authorization concept regulates the separation. The customers of lawpilots are separated from each other on the software side of the learning platform. The productive system is also separated from the test system.

Measures to ensure integrity:

Data integrity:
Measures to ensure that stored personal data is not damaged by system malfunctions:

- Installation of new releases and patches with (release/patch management)
- Functional testing during installation and of releases

Transport control:
Measures to ensure that the confidentiality and integrity of personal data are protected during the process of transmitting personal data as well as during the transport of data carriers:

- Email communication is transport-encrypted (TLS).
- Use of an encrypted communication protocol on the web server (https)

Weitere Maßnahmen:
lawpilots übermittelt die Daten über verschlüsselte Verbindungen.

Eingabekontrolle:
Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind:

- Dokumentation, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Aufbewahrung von Formularen, deren Daten in automatisierte Verarbeitungen übergegangen sind

Further measures:
lawpilots transmits the data via encrypted connections.

Input control:
Measures to ensure that it is possible to document and establish retrospectively whether and by whom personal data have been entered into, modified or removed from data processing systems:

- Documentation of which programs can be used to enter, modify or erase which data
- Technical logging of the entry, modification and erasure of data

Further measures:
lawpilots stores and logs the activities of lawpilots employees on the learning platform and keeps these logs for at least three years.

Measures to ensure availability and resilience:

Reliability:
Measures to ensure that all functions of the system are available and any malfunctions that occur are reported:

- Emergency plans and emergency management (restoration of availability)
- Employees are made aware of emergency management

Measures for regular evaluation:

Regular evaluation measures:
Measures to ensure data protection-compliant and secure processing:

- Data protection management software
- Formalised processes for data protection breaches
- Conclusion of the necessary agreements on processing on behalf of the Controller or EU standard contractual clauses
- Documentation of processing instructions to the Processor
- Obligation of the Processor's staff to maintain confidentiality
- Formalised order management

Further measures:
lawpilots has a data protection management system and is also regularly re-certified. Data protection incidents are mapped in formalized processes if they occur. In addition to this, instructions from clients are documented.

Processing instruction enforcement:

Measures to ensure that personal data processed on behalf of the Controller can only be processed in accordance with the Controller's processing instructions:

- Data protection management software
- Formalized processes for management of data protection incidents
- Verification of the measures taken by the Processor
- Conclusion of the necessary agreements on commissioned processing or EU standard contractual clauses
- Written instructions to the processor
- Obligation of the employees of the Processor to maintain data secrecy
- Formalised management of processing instructions

Annex V. List of subprocessors

The processor currently works with the following other processors in the performance of the contract, with whose commissioning the controller agrees. Data processing takes place exclusively within the European Union or the European Economic Area.

If the data processing takes place outside the European Economic Area or is accessed from outside the European Economic Area, an adequate level of data protection is ensured during processing in accordance with Art. 44 et seq. GDPR with the help of e.g. EU standard contractual clauses, BCR or adequacy decision of the EU Commission.

Telekom Deutschland	Landgrabenweg 151 53227 Bonn, Germany	Database of participant data for online training courses
Userlike	Probsteigasse 44-46 50670 Köln Germany	Customer service via chat
Mailjet SAS	13-13 bis, rue de l'Aubrac 75012 Paris France	Transactional emails for the learning platform
Hornetsecurity GmbH	Am Listholze 78, 30177 Hannover, Germany	Provision of services in the context of cyber security awareness training