Data Processing Agreement
pursuant to Art. 28, 29 EUGDPR

Between

***
***
***

(responsible party, hereinafter referred to as "**Controller**")

and

Terra Infinity UG
Adams-Lehmann-Str. 60
80797 Munich, Germany

(contracted processor, hereinafter referred to as "**Processor**")

– hereinafter, each individual party is also referred to as "**Party;"** jointly both parties are also referred to as **"Parties"** –

1 Scope

1.1 In conjunction with the provision of services under the main Agreement from [date] and its Annexes (hereinafter summarily and uniformly referred to as "Agreement"), the Processor will have to be granted access to Controller's or other third parties' personal data (hereinafter summarily and uniformly referred to as "Client Data").

1.2 All terms of this Data Processing Agreement shall be used according to and in the understanding of the European General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and Council).

1.3 In the event of conflicts between the provisions of this Data Processing Agreement and those of the Agreement, the provisions of this Data Processing Agreement shall prevail over those of the Agreement.

2 Commissioned Data Processing

2.1 The Processor shall process Client Data exclusively on behalf of and in compliance with Controller's instructions as defined in Art. 28, 29 GDPR (commissioned data processing). From a data protection legislation perspective, the Controller shall remain the responsible Party ("master of the data") and shall be responsible for the lawful processing of Client Data.

2.2 Client Data shall be exclusively and entirely processed for the purpose ultimately set forth in Annex 1 to this Data Processing Agreement. The processing of Client Data shall comprise the type of Client Data ultimately set forth in Annex 1 to this Data Processing Agreement as well as the categories of persons affected by the processing (data subjects) defined therein.

2.3 Processor shall not acquire any rights inherent in Client Data and shall undertake to surrender to Controller the Client Data at any time upon Controller's request. Withholding rights related to Client Data shall be excluded. Processor shall with Controller's instructions be obliged to correct or restrict the processing of Client Data.

2.4 Processor shall undertake to comply with the instructions inherent in the Agreement and the individually given instructions of the controller's executive management, the data protection officer or Controller's general counsel (hereinafter uniformly referred to as "data protection instructions") without any limitations. Individual data protection instructions shall be given in writing or via e-mail. In justified exceptional cases, it shall also be possible to give verbal data protection instructions; however, such instructions shall be promptly confirmed in writing or via e-mail. In the event that Processor should be of the opinion that a data protection instruction violates statutory provisions and/or the Agreement, Processor shall undertake to promptly notify the Controller and shall also have the right to refrain from executing the data protection instruction until it has been confirmed by the Controller.

2.5 Processor shall undertake to commission in writing a company data protection officer if, as a rule, at least twenty (20) individuals are constantly engaged in the automatic processing of personal data (§ 38 Sect. 1 S. 1 BDSG – Federal Data Protection Act). The Processor shall communicate the name of Processor's data protection officer to the Controller in writing. Any change in the identity of the data protection officer shall be promptly communicated to the Controller in writing by Processor.

3 Data Security / Technical and Organisational Measures

3.1 Processor shall require any individuals engaged in the processing of Client Data to commit to confidentiality pursuant to Art. 28 Sect. 3 S. 2 lit. b, 29 and 32 Sect. 4 GDPR.

3.2 Processor shall organise the processes and activities in such a manner that they meet the data security requirements and that ensures that Client Data are processed exclusively in compliance with the data protection related instructions of the Controller (in particular through separation of Client Data from data of other Processor's Controllers) and in particular in a manner that ensures that unauthorised third parties shall not be in a position to access such data.

3.3 Processor is obliged within the scope of responsibilities assigned to Processor in the Agreement, to comply with the security of the data processing activities pursuant to Art. 28 Sect. 3 lit. c, 32 GDPR, in particular in combination with Art. 5 Sect. 1, Sect. 2 GDPR. Processor shall guarantee when processing to deploy suitable technical and organisational precautions to warrant a level of protection that is adequate for the inherent risks including confidentiality, integrity, availability and resilience of processing systems and services. Taking into account the state of the art, the costs of implementation and type, scope, circumstances and purposes of processing as well as the different levels of likelihood and severity of risks for the rights and freedom of natural persons. Subject to additional data protection related instructions of the Controller, the technical and organisational measures set forth in Annex 2 to this Data Processing Agreement shall be considered the technical and organisational measures as defined in Section 3.3 of this Data Processing Agreement upon execution of the Agreement and/or this Data Processing Agreement.

3.4 Processor shall not process any Client Data over the necessary extent of fulfilling the contractual obligation (in particular not to duplicate or pass on to third parties without authorisation).

3.5 Processor shall completely and irrevocably delete or destroy (hereinafter uniformly referred to as "delete") any and all provided and additionally processed Client Data in all of Processor's systems (including any reproductions, as well as archiving and backup files) pursuant to the provisions set forth in Annex 3 to this Data Processing Agreement as soon as the processing of Client Data is no longer necessary to fulfilment of the contract processing activities and at the latest upon termination of the rendering of contracted services (in particular in the event of cancellation or any other form of contract termination).

3.6 The deletion of Client Data shall be documented by the Processor and shall be confirmed in writing to the Controller upon request. This deletion obligation covers not Client Data, which has to be archived based on any statutory retention and/or archiving obligation. The processing of Client Data shall be restricted according to legal requirements and shall be deleted after the expiration of the retention and/or archiving obligation.

4 Notification Obligation

In the event of extraordinary incidents according to Art. 33 and 34 GDPR as well as in case of violations of provisions for the protection of personal data or against provisions set forth in this Data Processing Agreement and its Annexes by the Processor or people employed by the Processor , Processor is obliged to immediately take all necessary measures in order to exclude any risks for the integrity and confidentiality of Client Data. Additionally, in these cases the Processor is obliged to immediately report the specific circumstances by stating the causes and the exact time as well as the extent of the extraordinary incident; furthermore match the further processing of Client Data with the Controller.

5 Subprocessors

5.1 The Processor is allowed to commission Subprocessors with handling Processor's duties after the Processor has committed the Subprocessors in writing in such a way as the Processor is obliged to the Controller on the basis of this Data Processing Agreement. In particular, the Processor has to obligate the Subprocessor in such a way that the Controller can execute his Controller Rights according to Section 7 of this Data Processing Agreement directly against the Subprocessor. Persons contractually affiliated with the Processor through employment contracts or leased workforce members employed to process Client Data, who have been verifiably committed to confidentiality in compliance with Section 3.1 of this Data Processing Agreement, are not considered Subprocessors as defined in this Section 5.

5.2 For the purpose of concluding the Agreement, the Processor has commissioned the subprocessors listed in Annex 3 to this Data Processing Agreement with the fulfilment of its obligations.

5.3 The Processor shall inform the Controller on the planned changes with regard to including and replacing Subprocessors in order for the Controller to execute the right to object to these changes.

6 Third Party Inquiries, Audits by Supervisory Authorities

6.1 If Controller should receive third party requests (especially from data subjects and journalists) for information about the processing of Client Data or extraordinary incidents, that triggers the notifications obligation according to Section 4 of the Data Processing Agreement, Processor shall undertake to promptly notify the Controller and Controller's data protection officer about the inquiry. Processor shall refrain from giving third parties information pursuant to Sentence 1 of this Section 6.1 unless Processor is mandated to provide such information by applicable laws. Section 6.1 of this Data Processing Agreement shall apply accordingly if supervisory authorities announce audits to be conducted at Processor's end or conduct such audits without prior announcement.

6.2 If Controller should be subjected to a direct audit by a supervisory authority, the Processor shall provide the fullest amount of support possible to the Controller.

7 Controlling and Information Rights

Controller's data protection officer and/or any third parties commissioned by the former shall have the right at any time, subject to giving prior written notice, to enter the business premises of the Processor, to gain unrestricted timely and spatial evidence of compliance with the applicable statutory and contractual data protection provisions. Processor shall grant Controller's data protection officer and/or any third parties commissioned by the former access, information and review rights within this scope. The same shall apply to the supervisory authority (authorities) competent for the Controller.

8 Support of the Controller

8.1 The Processor shall undertake to assist the Controller with the latter's obligation to respond to requests to exercise the rights set forth in Art. 16 - 21 GDPR by data subjects and to provide any and all relevant information in this context promptly upon request.

8.2 Processor shall furthermore undertake to assist the Controller with the implementation of data protection impact assessments pursuant to Art. 35 GDPR as well as those in conjunction with prior consultations with the supervisory authority pursuant to Art. 36 GDPR upon Controller's written request.

8.3 Processor shall undertake to provide the Controller with all documentation necessary to comply with the reporting obligation pursuant to Art. 28 GDPR.

9 Final Provisions

Unless otherwise expressly agreed upon between the Parties, the term of the Data Processing Agreement shall be governed by the provisions on the duration set forth in the Agreement.

Annex 1: Subject-matter, nature, purpose and duration of the processing as well as type of Client Data and categories of data subjects

Annex 2: Technical and organisational measures

Annex 3: Commissioned subprocessors

Place, date:

_____

On behalf of the Controller:

_____

Place, date:

_____

On behalf of the Processor:

_____

Annex 1 to the Data Processing Agreement: subject-matter, nature, purpose and duration of the processing as well as type of Client Data and categories of data subjects

1 Subject-matter, nature and purpose of data processing

The online learning platform “eStudy.fm” developed by the Processor offers all the functions necessary for the implementation of web-based distance learning equivalent to face-to-face teaching. Teachers can use the online learning platform “eStudy.fm” both for pure distance learning and as a complementing tool to face-to-face teaching (e.g. in the context of direct communication with individual students or their parents).

Teachers can set their students tasks in form of tickets via the online learning platform “eStudy.fm” and assess them once they have been completed by the students in the online learning platform "eStudy.fm". In addition, teachers can conduct lessons via integrated video conferencing and whiteboard functions and communicate with their students via chat and push messages.

The object, nature and purpose of the commissioned processing is the provision of the online learning platform "eStudy.fm" as well as the supplementary care and maintenance of the online learning platform "eStudy.fm" by the contractor.

2 Duration of data processing

The present processing agreement for the provision of the learning platform "eStudy.fm" is concluded for an indefinite period of time and shall automatically end with the termination of the last Agreement concluded between the Parties.

3 Type of Data processed by the Processor

Contact data, communication data, evaluations and grades as well as all other personal data, which users upload to the learning platform "eStudy.fm" may be processed by the Processor. These are usually the following personal data:

- name, first name, email address if applicable, photo if applicable,
- image and audio,
- communication data, especially messages between users, chat discussions and comments,
- ratings, evaluation results as well as grades,
- calendar entries,
- presentations, homework, other assignments, etc.

4 Categories of data subjects

- employees of the Controller, in particular teachers, administrators, lecturer and mentors, as well as
- other authorised users by the Controller, in particular students and parents.

Annex 2 to the Data Processing Agreement: technical and organisational measures

I. Confidentiality

1. Physical Access Control

a. The premises of the Processor in which Client Data are being processed shall be secured against access by unauthorised persons. For this purpose, the entrances to the premises must be secured with security or magnetic card locks. Doors, gates and windows must be locked tightly outside of operating hours.

b. Granting of access rights and of keys, magnetic cards, ID cards and other identity mark carriers enabling access shall be documented for the duration of the main contract in the form of an up-to-date list of any locking devices and access authorisations that have been issued.

c. If servers are being used to process Client Data, they must be kept in a separate server room or data centre, which is to be secured against unauthorised access. These rooms must be protected against burglary. Access to these premises shall be restricted to the extent that is necessary for maintenance and repair as well as to the persons who are specifically required.

2. Logical Access Control

a. The Processor's information-processing systems being used to process Client Data shall be protected by means of authentication systems. The Processor shall be obliged to use access authorisations which at least provide for user IDs and complex passwords.

b. Authentication data must be kept secret and are not to be disclosed to unauthorised third parties. In particular, the Processor is obliged not to store this authentication data in plain text. Each allocation of authentication data shall be documented for the duration of the main contract.

c. Authentication data is only to be used personally. The authentication data cannot be passed on to someone else. If unauthorised persons gain knowledge of the access data, the Processor shall notify the Controller of this without undue delay.

d. Passwords are to be chosen with enough complexity and quality. Enough complexity and quality mean a length of at least eight characters using three of the following four categories: Upper- and lower-case letters, digits and special characters.

e. Insofar as the information-processing systems or the software being used offer the possibility to save form inputs and/or passwords, the Processor is obliged to deactivate this functionality.

f. The Processor is only permitted to grant any remote maintenance access which enables access to Client Data after the approval from the Controller.

3. Data Access Control

a. If Client Data are being stored on information-processing systems of the Processor, a graded and suitable granular rights system shall be set up and technically implemented for any access to Client Data. This shall ensure that the access rights are designed in such a way that they only allow access to Client Data to the extent that is necessary for the persons employed to perform the specific tasks in question. The assignment of administrator rights shall be limited to the absolutely necessary number of employed persons of the Processor. The allocation of rights must be documented for duration of the main contract.

b. Insofar as the Processor electronically processes images (scans) of original documents that contain Client Data in accordance with the main contract, the resulting images shall be protected against access by unauthorised persons.

c. Screens or other output devices that are part of the information-processing systems and that are being used to process Client Data must be arranged in such a way that uninvolved unauthorised persons and other third parties cannot see any Client Data.

d. If the processing of Client Data takes place in the form of a non-automated file (e.g. in a structured filing system), the access control requirements of this provision shall be applied correspondingly.

4. Separation Control

The Processor is obliged to process Client Data in such a way that guarantees a separation of Client Data from any data of other Controllers or any own data of the Processor. In particular, it must be ensured that Client Data can be identified and completely deleted at any time.

5. Pseudonymisation

a. The Processor is obliged to process personal data primarily pseudonymized, provided that the provision of services remains possible and is not impaired. This effort must be proportionate to the level of protection that is to be achieved.

b. Pseudonyms must be created in such a way that personal data is replaced by unique artificial indexes, scrambles or random character strings.

c. The information to dissolve the pseudonyms shall be encrypted and access shall only be granted to authorised persons of the Processor.

II. Integrity

1. **Data Transfer Control**

a. The Processor shall ensure that Client Data cannot be copied (in particular stored on external data carriers), passed on and/or deleted.

b. If the Processor uses information-processing systems with non-volatile memory (e.g. network printers or scanners), the Processor must ensure that Client Data cannot be stored by these systems beyond the scope required directly for the performance of the contract. The Processor shall take technical measures to ensure that third parties (in particular external service providers who may be contracted to maintain the systems) cannot access any Client Data.

2. Data Entry Control

If the Processor processes Client Data, the Processor must ensure through record keeping or organizational measures that, at the request of the Controller and also until the Client Data has been deleted, it can be reliably determined at any time, even subsequently, when and by whom what Client Data has been processed (at least by keeping records of the user ID of the persons processing Client Data, of the changed date and the time of the changes).

3. Erasure

a. The Processor shall wipe all electronic data carriers that can be wiped (in particular hard disks, USB sticks, floppy-disks, tapes) containing Client Data so they cannot be restored.

b. The Processor shall destroy all paper documents and all non-erasable data carriers (including all misprints or misstorages as well as CDs and DVDs) containing Client Data with a commercially available paper shredder according to security level 3 in accordance with DIN 32757 or at least an equivalent method. Defective magnetic data carriers that cannot be mechanically destroyed as specified above (e.g. defective hard disks) must be wiped using an approved method in accordance with DIN 33858.

III. Availability

1. Availability Control

a. The Processor shall prevent data loss of any of the Client Data through accidental, negligent or intentional deletion or alteration by means of technical and organizational measures.

b. Backup copies of Client Data stored by the Processor on information-processing systems shall be treated in the same way as original data, in particular, they shall be secured against unauthorised access.

2. Resistance

a. Protective software/anti-virus programs with regular updates that are protected against any manipulation as well as a firewall must be set up, if technically possible, and run on the clients being used by the Processor.

b. All software used by the Processor shall be kept up-to-date and security-relevant updates (in particular updates, patches, fixes) shall be installed after these have been made available to the public by the manufacturer of the software.

c. Files originating from third parties, in particular executable content, may only be transferred to the Processor's information-processing systems after they have been checked manually or automatically for any harmful content.

3. Encryption

If an agreement has been made stipulating the obligation to encrypt Client Data, the Processor shall, subject to any prior arrangement to the contrary with the Controller, apply a procedure which is described in the "Technical Guideline: Cryptographic Mechanisms: Recommendations and Key Lengths, BSI TR-02102" by the German Federal Office for Information Security (BSI) in the current version, and comply with at least the following standards:

- Symmetric block ciphers AES with a key length of at least 128 bits
- Asymmetric ciphers the RSA process with a key length of at least 2048 bit
- For hash procedure SHA-256 or higher

IV. Process for Regular Testing, Assessing and Evaluating

1. Job Control

a. The persons employed by the Processor to carry out the work shall be trained in the general principles of the processing of Client Data and the specific requirements of data protection and data security for the processing of Client Data resulting from the main contract prior to carrying out the work.

b. The persons employed by the Processor are to be committed to confidentiality and the protection of personal data in writing.

c. Training courses and the compliance with all obligations shall be documented and kept available by the Processor throughout the duration of the main contract.

d. The Processor shall ensure that the rules for processing Client Data contractually stipulated are being adhered to as well as being implemented.

2. Data Protection Management

The Processor shall implement corresponding regulations and measures in all information-processing systems and any other processes in compliance with the law. This includes in particular the following, which shall be implemented within the Processor’s privacy management framework:

- Annual data protection training of the employed persons including the commitment to data secrecy;
- Monitoring of all information-processing systems, processes and service providers being used;
- Establishing an appropriate data protection management;
- Data protection by design and by default;

3. Incident Response Management

a. The Processor shall maintain corresponding reporting procedures for all information-processing systems and processes for reporting any security incidents that take place when processing Client Data and the Processor shall inform all persons to perform the contract about these procedures.

b. The Processor shall inform the Controller about any identified security incidents without undue delay.

c. The Processor shall document all identified security incidents and subsequent measures for the duration of the service provision.

Annex 3 to the Data Processing Agreement: commissioned subprocessors

Firm	Address	Nature of the collaboration
Amazon Web Services EMEA SARL	38 avenue John F. Kennedy, L-1855, Luxemburg	Hosting of the online learning platform „eStudy.fm“