Privacy and Data Protection Agreement

This Privacy and Data Protection Agreement (hereinafter referred to as the 'Privacy Agreement'), sets forth the standard obligations that all third parties (hereinafter referred to as 'Vendor', and includes their affiliates, agents, or partners) must follow when receiving or accessing personal data from or on behalf of any of the entities part of the Emeritus Group for processing in order to provide any type of Service(s) to any of such entities.

This Privacy Agreement is incorporated and forms part of the Services Agreement (also referred to as Consultancy Agreement or MSA, hereinafter referred to as the "Main Agreement") entered into between Vendor and any Emeritus Group entity (hereinafter "Client") and applies to the services to be provided by Vendor under such Main Agreement ("Services").

This Privacy Agreement is applicable and enforceable even in cases where there is no Main Agreement between the Parties, or in case only a purchase order or an SOW exists between the Parties.

Vendor and the Client are hereinafter together referred to as the 'Parties'.

1. **Privacy Terms**

   Vendor represents and warrants that the Vendor shall comply with the provisions of this Privacy Agreement, which will supersede and replace any and all existing data usage, storage, and sharing provisions and agreements signed between the parties (if any) in relation to the matters set forth in this Privacy Agreement. In the event of a conflict between this Privacy Agreement and the provisions of related agreements between the parties existing at the time when this Privacy Agreement is agreed or entered into thereafter, this Privacy Agreement shall prevail to the extent of such conflict.

2. **Instructions and Ownership**

   a. The Vendor shall process Client Personal Data only on documented instructions from the Client, unless required to do so by Data Protection Laws to which the Vendor is subject. In this case, the Vendor shall inform the Client 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 Client throughout the duration of the processing of Client Personal Data. These instructions shall always be documented.
   b. The Vendor shall immediately inform the Client if, in the Vendor's opinion, instructions given by the Client infringe the applicable Data Protection Laws.
   c. Client Personal Data processed by the Vendor directly or indirectly in the performance of this Privacy Agreement shall remain the property of the Client at all times.
   d. The Client Personal Data must be made available (electronic access or file transfer, as may be requested) to the Client within seventy-two (72) hours of such request, at no additional cost, by the Vendor.
   e. Vendor and its sub-processors (where authorized) shall return, delete, destroy, or dispose-off (as directed by the Client) all (or selected) Client Personal Data and any copies thereof as per

Client's instructions, and at any time at its sole discretion. Client Personal Data shall be deleted/destroyed/disposed-off (if so directed) in a secure manner using industry-standard data wiping practices.

3. Obligations of the Vendor

a. While processing Client Personal Data, Vendor shall comply with and be accountable for compliance with its obligations under the Applicable Laws including the Data Protection Law.
b. Vendor shall process Client Personal Data for the duration as instructed, solely for the purpose of providing the services specified in the respective agreements between the parties unless it receives further instructions from the Client, and for no other individual or entity, and for no other purpose.
c. The Vendor shall promptly notify the Client of any request, complaint, or communication it has received from the data subject(s), or any concerned/relevant regulatory authority related to processing of Client Personal Data under this Privacy Agreement. It shall not respond to the request, complaint, or communication itself, unless authorized to do so by the Client, and promptly forward the said request, complaint, or communication to the Client, within seventy-two (72) hours of receipt.
d. In no case will Client Personal Data processed by the Vendor be furnished or made accessible to any third-party/sub-processor, without the prior written approval/authorization of the Client, or as provided in this Privacy Agreement.
e. Vendor shall grant access to the Client Personal Data undergoing processing to members of its personnel (employees) only to the extent strictly necessary for implementing, managing, and monitoring of this Privacy Agreement and/or other relevant agreements entered into between the parties, and for delivery of services within scope. Vendor accepts full liability for any breach(es) of this Privacy Agreement by its employees.
f. Vendor shall take reasonable steps to ensure the reliability of any personnel who have access to Client Personal Data and shall ensure that persons authorized to process the Client Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and have received proper training and instruction as to the requirements of this Privacy Agreement.
g. Vendor shall not, directly or indirectly, sell, rent, disclose, distribute, disseminate, commercially exploit, enrich their own database or transfer any Client Personal Data to any third party for any purpose whatsoever, without the prior written approval of the Client.
h. If applicable, when the Vendor collects personal data on behalf of Client, it shall only do so with prior written approval and instructions from the Client. The Vendor shall notify the individuals (data subjects) in accordance with the Data Protection Laws of the circumstances and purposes of such collection, and obtain necessary authorization and consent required to enable Client to use, disclose, or transfer (process) such personal data.
i. To ensure security of processing, the Vendor shall establish and maintain necessary administrative, technical, organizational, and physical safeguards to protect Client Personal Data against personal data breach while such data is in the possession or under the control of the Vendor. Additionally, Vendor shall implement an appropriate network security program

(that includes, without limitation, encryption of Client Personal Data during storage and transit).

j. Vendor shall maintain complete, accurate, and up to date written records of all processing activities carried out on behalf of the Client containing information as required under the applicable Data Protection Laws and shall make such records available to the Client within seventy-two (72) hours of the Client's request for such records.

k. The Client shall have the right to audit and assess Vendors' compliance with the security and privacy requirements pursuant to this Privacy Agreement conducted by or on behalf of the Client.

l. Vendor shall not disclose Client Personal data to any law enforcement agency, government, or regulatory authority, without the prior written approval of the Client, unless otherwise prohibited by the Applicable Law. The Vendor shall inform the Client of the receipt of such a request within two (2) days of receiving such request to allow the Client to seek a protective order or exercise other appropriate remedy available to the Client, unless otherwise prohibited by the Applicable Law.

m. Vendor shall furthermore assist the Client in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available with the Vendor:

    i. The obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of Client 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/individuals (data subjects).

    ii. Vendor will, upon Client's request, provide the Client with such assistance as it may reasonably require to comply with its obligations under applicable Data Protection Laws to respond to requests from individuals to exercise their rights under the applicable Data Protection Laws (e.g., rights of access, rectification, erasure, restriction, portability, and objection) in cases where the Client cannot reasonably fulfill such requests independently without the assistance of the Vendor. In cases where requests from individuals to exercise their rights have come independently to the Vendor, it shall without undue delay, and no later than three (3) days from the date of receipt of the request, inform the Client of such request. Vendor shall not respond to data subject request(s) unless instructed and authorized by the Client in writing.

    iii. The obligation to consult the competent/relevant regulatory 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 Client to mitigate the risk.

    iv. The obligation to ensure that Client Personal Data is accurate and up to date, by informing the Client without delay if the Vendor becomes aware that the Client Personal Data it is processing is inaccurate or has become outdated.

    v. The Vendor shall not, by any act or omission, place the Client in breach of any Applicable Law including Data Protection Law.

4. Data Breach Notification

In the event of a personal data breach involving Client Personal Data processed by the Vendor, the Vendor shall cooperate with and assist the Client for the Client to comply with its obligations under the relevant provisions of the applicable Data Protection Laws. Vendor shall immediately notify the Client telephonically to the Client's point of contact (POC) for the Vendor and also via email to such POC with a copy to privacy@emeritus.org without undue delay, and in not more than after forty-eight (48) hours after it becomes aware of the personal data breach. The details of personal data breach notification to the Client shall comply with the Applicable Laws including the Data Protection Laws. The Vendor shall comply with any subsequent/additional instructions from the Client in connection with the personal data breach.

Vendor shall not notify or make any statement, announcement or press release (or provide any documentation) to any third party (including but not limited to the media, customers, regulators and supervisory authorities, and individuals affected by the personal data breach) about personal data breach events covered under this clause, and/or other matters concerning Client Personal Data, without the prior written approval of Client.

5. International Transfers

a. The Vendor shall not transfer any Personal Data outside the country where the personal data was made available (by way of access or transfer) to the Vendor by the Client unless such transfer is made on documented instructions and authorization from the Client and complies with the applicable Data Protection Law.

b. Client agrees that where the Vendor engages a sub-processor in accordance with the relevant provisions of this Privacy Agreement for carrying out specific processing activities and those processing activities involve an international/cross-border transfer of Client Personal Data within the meaning of the relevant provisions of the applicable Data Protection Laws, the Vendor and the sub-processor can ensure compliance with such provisions (subject to a prior authorization from the Client as stipulated under clause 5(a) above) by using standard contractual clauses (if available) in terms of such Data Protection Laws, provided the conditions for the use of those standard contractual clauses are met. In all other cases where no standard contractual clauses exist under the applicable Data Protection Laws, Vendor shall ensure that such international/cross-border transfer between the Vendor and its sub-processor shall be governed by the provisions of the relevant module of the Model Clauses that shall be read and apply *mutatis mutandis* in relation to the country of origin of Client Personal Data in scope.

c. This section becomes applicable in case any transfer of Client Personal Data from the Client to the Vendor is a Restricted Transfer of Client Personal Data. Parties agree to abide by the Model Clauses incorporated hereto by reference and form an integral part of this Privacy Agreement. In case any provision of this Privacy Agreement contradicts the Model Clauses, the Model Clauses shall prevail. This Privacy Agreement is not intended to amend the terms

of the Model Clauses, and no term of this Privacy Agreement should be read or interpreted as having that effect.

i. **Client Personal Data covered under GDPR** where **Client is the Controller** of whole or part of Client Personal Data and the Vendor is a Processor, Module 2 (transfer controller to processor) of the Model Clauses, completed as follows, shall apply in relation to such data. Capitalized terms in this clause (if not defined in this Privacy Agreement) shall have meaning as defined under the GDPR:
   1. Clause 7 is included, option 1 for clause 9(a), optional part of clause 11(a) is included, option 1 for clause 17.
   2. Time period reference in clause 9(a) shall be thirty (30) days.
   3. The relevant member state for the purpose of clause 17 and 18(b) shall be Spain.
   4. The competent supervisory authority for the purpose of Part C of Annexure I shall be the Spanish Data Protection Agency (AEPD).
   5. Annexures I, II and III to the Model Clauses shall be deemed completed with the information and as per the instructions set out in Annexures I, II and III, respectively, of this Privacy Agreement.

ii. **Client Personal Data covered under GDPR** where **Client is the Processor** of whole or part of Client Personal Data and the Vendor is its sub-processor, Module 3 (transfer processor to processor) of the Model Clauses, completed as follows, shall apply in relation to such data. Capitalized terms in this clause (if not defined in this Privacy Agreement) shall have meaning as defined under the GDPR:
   1. Clause 7 is included, option 1 for clause 9(a), optional part of clause 11(a) is included, option 1 for clause 17.
   2. Time period reference in clause 9(a) shall be thirty (30) days.
   3. The relevant member state for the purpose of clause 17 and 18(b) shall be Spain.
   4. The competent supervisory authority for the purpose of Part C of Annexure I shall be the Spanish Data Protection Agency (AEPD).
   5. Annexures I, II and III to the Model Clauses shall be deemed completed with the information and as per the instructions set out in Annexures I, II and III, respectively, of this Privacy Agreement.

iii. **Client Personal Data covered under UK GDPR:** In relation to Client Personal Data protected by the UK GDPR, the UK Addendum will apply in relation to such data, completed as follows:
   1. The relevant module of Model Clauses, completed as set out above in this section, shall also apply to transfers of such Client Personal Data, subject to sub-clause 2 below.
   2. Tables 1 to 3 of the UK Addendum shall be deemed completed with relevant information from the Model Clauses, completed as set out above, and the

options “importer” and “exporter” shall be deemed checked in Table 4. The start date of the UK Addendum (as set out in Table 1) shall be the date of this Privacy Agreement.

iv. Parties agree that in case of a transfer of Client Personal Data by Emeritus to the Vendor to a country outside the country of origin of such Personal Data (international/cross-border transfer or as onward transfer), other than those covered under GDPR as per clauses 5(c)(i) and (ii), and under UK GDPR per clause 5(c)(iii) above, the conditions of this section shall apply.

Parties agree to abide by the Model Clauses as per clause 5(c)(i), which are incorporated hereto by reference, that shall be read and apply *mutatis mutandis* in relation to the country of origin of such Client Personal Data. The Client shall be deemed to be the Controller (or any cognate term under the Applicable Laws including Data Protection Laws of the country of origin of the Client Personal Data).

1. Clause 7 is included, option 1 for clause 9(a), optional part of clause 11(a) is included, option 1 for clause 17.
2. Time period reference in clause 9(a) shall be thirty (30) days.
3. The term relevant member state for the purpose of clause 17 and 18(b) and (c), shall be interpreted in a manner that allows the Data Subjects to exercise their rights in their place of habitual residence, i.e. the country of origin of Client Personal Data in scope.
4. References to competent supervisory authority in accordance with Clause 13 and Part C of Annexure I shall be interpreted as the concerned regulator or the supervisory authority of the country of origin of Client Personal Data in scope.
5. Annexures I, II and III to the Model Clauses shall be deemed completed with the information and as per the instructions set out in Annexures I, II, and III respectively, of this Privacy Agreement.

6. California (U.S.A.) Specific Terms

To the extent Vendor processes Client Personal Data originating from and protected by the Data Protection Law of California (U.S.A.) then the terms specified herein shall apply in addition to the terms of this Privacy Agreement. In the event of any conflict or ambiguity between the terms under this clause and any other term(s) of this Privacy Agreement, the terms of this clause will prevail. Capitalized terms in this clause (if not defined in this Privacy Agreement) shall have meaning as defined under the California Privacy Rights Act of 2020 (CPRA).

a. Vendor is a Service Provider to the Client and the Processing of Client Personal Data by the Vendor shall be undertaken only for the Client’s purposes in accordance with this clause and

this Privacy Agreement. The Client has not received any monetary or other valuable consideration from the Vendor and that the Client is not Selling Client Personal Data to the Vendor as per CPRA.

b. The Vendor is prohibited from:
    i. Combining Client Personal Data with Personal Information it has received from, or on behalf of, another Person(s), or collected from its own interaction with the Consumers.
    ii. Selling or Sharing the Client Personal Data.
    iii. Retaining, using, or disclosing the Client Personal Data for any purpose other than for the Business Purposes specified in this Privacy Agreement and/or other relevant agreements between the parties, including retaining, using, or disclosing the Client Personal Data for a Commercial Purpose other than the Business Purposes specified in this Privacy Agreement and/or other relevant agreements between the parties, or as otherwise permitted by CPRA.
    iv. Retaining, using, or disclosing the Client Personal Data outside of the direct business relationship between the parties.
c. If the Vendor engages any other Person to assist it in Processing Client Personal Data for a Business Purpose on behalf of the Client, or if any other Person engaged by the Vendor engages another Person to assist in Processing Client Personal Data for that Business Purpose, it must notify the Client of that engagement, and the engagement must be pursuant to a written contract binding the other Person to observe all the requirements set forth in this clause.

7. Indemnification

Vendor agrees to defend, indemnify, and hold the Client harmless, to the extent permitted by law, from any liability, claims, damages, fines, penalties, costs, demands and expenses (including costs of defense, settlement, and reasonable legal fees), arising from or related to any breach of this Privacy Agreement by Vendor, or its Affiliates, personnel/employees, or sub-processors. Vendor will not settle any dispute or agree to any settlement without the prior written consent of the Client. Client reserves the right to retain its own counsel and to actively participate in settlement and all litigation proceedings as it in its sole judgment determines necessary or desirable. This clause shall survive the termination or expiration of this Privacy Agreement.

8. Termination for Breach

Without prejudice to any provisions of the applicable Data Protection Laws, in the event that Vendor is in breach of its obligations under this Privacy Agreement, Client may, without any liability towards Vendor:

a. Instruct Vendor to suspend the processing of Personal Data until the latter complies with this Privacy Agreement; or
b. Terminate the Main Agreement and this Privacy Agreement.

The Vendor shall promptly inform the Client in case it is unable to comply with the instructions of the Client or this Privacy Agreement, for whatever reason.

9. Term and Post Termination

a. This Privacy Agreement will remain in full force and effect for as long as any processing including but not limited to access and storage of Client Personal Data by Vendor (and its sub-processors) takes place.

b. Following termination of the Main Agreement, Vendor shall (and ensure that its sub-processors shall), at the choice of the Client (and within thirty days of receipt of communication from the Client), delete all Client Personal Data (whether in electronic or physical form) and certify to the Client that it has done so, or return all the Client Personal Data to the Client and delete existing copies unless the applicable Data Protection Laws requires storage of such Client Personal Data (only to the extent and for such period as required by such laws). Until the data is deleted or returned, the Vendor shall continue to ensure compliance with this Privacy Agreement. Vendor shall ensure the confidentiality of all such Client Personal Data and shall ensure that it is only processed as necessary for the purpose(s) specified in the applicable Data Protection Laws requiring its storage and for no other purpose.

c. Vendor shall confirm in writing within ten (10) days of such erasure or return, as applicable, that Vendor and its sub-processors have acted according to the direction(s) of the Client and no longer possess/hold/retain any Client Personal Data or part thereof in any form - electronic or physical, and that such data is no longer retrievable and accessible.

10. Severability

If any provision of this Privacy Agreement is rendered ineffective or void by order of any court or competent regulatory authority or by virtue of Applicable Laws including Data Protection Laws, the remaining provisions of the Privacy Agreement shall not be affected. The parties shall promptly and in good faith work to replace the ineffective or void provision with a lawful provision that meets the purpose of ineffective or void provision.

DEFINITIONS

Whether or not any term is capitalized:

'Applicable Law' means all central, state, local, foreign, or international statutes, codes, enactments, acts of legislature or parliament, laws, by-laws, ordinances, regulations, rules, notifications, treaties, regulatory guidelines and interpretations, and judicial or administrative orders, as each may be amended, re-enacted or consolidated from time to time, of any authority having jurisdiction over a party or the subject matter of this Privacy Agreement.

'Affiliate' means any entity that directly or indirectly controls, is controlled by, or is under common control with, another entity, where "control" means the beneficial ownership of more than 50% of the issued share capital of a company or the legal power to direct or cause the direction of the management of the company and "controls" and "controlled" shall be interpreted accordingly.

'Client Personal Data' means personal data (1) obtained or accessed by the Vendor from any of the entities part of Emeritus Group (irrespective of whether the Emeritus Group entity is a controller or a processor towards such personal data, such terms as defined under the GDPR); (2) obtained or accessed from any other source, including without limitation, a data subject, for processing by the Vendor on behalf of any of the entities part of the Emeritus Group; or (3) generated while delivering the services in terms of this Privacy Agreement and other relevant agreements between the parties.

'(Data) Controller' means the natural or legal person, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

'(Data) Processor' means a natural or legal person, or other body which processes Personal Data on behalf of the Controller.

'Data Protection Law' means all applicable data protection, security or privacy-related laws, statutes, directives, or regulations in any relevant jurisdiction.

'Data Subject' means any person to whom personal data relates.

'Emeritus Group' means Eruditus Learning Solutions Pte Ltd (ID # 201230726W), a company incorporated under the laws of Singapore having offices at 78 Shenton Way, # 20-02, Singapore - 079120, along with its affiliates and subsidiaries.

'General Data Protection Regulation or GDPR' means Regulation (EU) 2016/679 of the European Parliament and of the Council 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.

'Model Clauses' means the standard contractual clauses annexed to the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, or any successor standard contractual clauses that may be adopted pursuant to an EU Commission decision.

‘Personal Data’ means any data related to an identified or identifiable living natural person, provided, however, that if an applicable law has a different definition of Personal Data (or a similar term referring to information relating to an individual), such definition shall be applied to the extent applicable.

‘Personal Data Breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

‘Processing’ means (1) any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; and (2) any other action that may be taken with respect to personal data.

‘Restricted Transfer’ means: (i) where the GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission (including an onward transfer); and (ii) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018 (including an onward transfer).

‘Sub-processor’ means any person (excluding an employee of the Vendor) appointed by or on behalf of the Vendor to process Client Personal Data on behalf of the Client in connection with the Services.

‘UK Addendum’ means the "International Data Transfer Addendum to the European Commission Standard Contractual Clauses" issued by the Information Commissioner under s.119A(1) of the Data Protection Act 2018.

ANNEXURE I

The Parties shall separately complete and execute this annexure if international/cross-border transfer of personal data as per clause 5(c) of the Privacy Agreement is in scope.

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date:

Role: controller/processor

Data importer(s): *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses:

Signature and date:

Role: processor/sub-processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

……..

Categories of personal data transferred

……..

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

……..

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

……..

Nature of the processing

……..

Purpose(s) of the data transfer and further processing

……..

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

……..

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

……..

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

As stated under Clause 5.c of the Privacy Agreement.

ANNEXURE II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Technical and organisational measures as specified at the following link:

https://emeritus.org/wp-content/uploads/2025/03/Technical-and-Organisational-Measures.pdf

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

Same measures (https://emeritus.org/wp-content/uploads/2025/03/Technical-and-Organisational-Measures.pdf) apply to sub (sub-) processors.

ANNEXURE III – LIST OF SUB-PROCESSORS

The Parties shall separately complete and execute this annexure if engaging of sub-processors as per clause 3(d) of the Privacy Agreement is in scope.

The controller has authorised the use of the following sub-processors:

1. Name: …

Address: …

Contact person's name, position and contact details: …

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …

2. …