Privacy and Data Protection Agreement

This Privacy and Data Protection Agreement (hereinafter referred to as the 'Privacy Agreement'), is incorporated under a Consultancy Agreement and sets forth the obligations of the 'Consultant' as described and referred to in the Consultancy Agreement (hereinafter defined and referred to as **'Vendor'**, and shall include their affiliates, agents, or partners). All Processing of Personal Data from or on behalf of any of the entities of the 'Company' by the 'Consultant' to provide any type of services ('Services') shall be governed by the terms of this Privacy Agreement hereof.

The 'Company', as described and referred to in the Consultancy Agreement, shall include its affiliates and subsidiaries (hereinafter referred to as **'Client'**).

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

I. 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 (irrespective of whether it is in electronic or in physical form) (1) obtained or accessed by the Vendor from any of the entities part of the Company (irrespective of whether such 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 Company; or (3) generated while delivering the services in terms of this Privacy Agreement and other relevant agreements between the parties.

'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.

'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).

'Sensitive Data' means data which is more significantly related to the notion of a reasonable expectation of privacy, such as medical or financial information. However, data may be considered more or less sensitive depending on context or jurisdiction. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation are some examples of sensitive data (list not exhaustive).

'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.

II. PRIVACY TERMS

Vendor represents and warrants that the Vendor shall comply with the following provisions, 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.

1. **Instructions:**
    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 applicable Data Protection Laws.

2. **Ownership:**
    a. 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. It shall be identified, clearly marked, and recorded as such by the Vendor on all media and in all documentation.
    b. The Client Personal Data must be made available (electronic access or file transfer, as may be requested) to the Client within forty-eight (48) hours of such request or within the timeframe specified otherwise, at no additional cost, by the Vendor.
    c. Vendor and its sub-processors 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.
    d. Where the Client is a data processor/importer towards all or part of Client Personal data (and the Vendor is a sub-processor), in the event that the Client has factually disappeared, ceased to exist in law, or has become insolvent – the data controller(s)/exporter(s) of the relevant Client Personal Data shall have the right to terminate this Privacy Agreement and to instruct the Vendor to erase or return their respective Client Personal Data. The term(s) used in this (sub)clause and not defined in this Privacy Agreement shall derive its meaning from the GDPR.

3. **Obligations of the Vendor:**
    a. While processing Client Personal Data, Vendor shall comply with all the Applicable Laws including the Data Protection Laws.

b. The Vendor shall promptly notify the Client of any request, complaint, or communication it has received from the data subject(s), or any supervisory authority related to processing of Client Personal Data under this Privacy Agreement. It shall not respond to the request, complaint, or communication itself, unless authorised to do so by the Client, and promptly forward the said request, complaint, or communication to the Client, within twenty-four (24) hours of receipt.

c. 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 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 (data subjects).
    ii. 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 Client to mitigate the risk.
    iii. 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.
    iv. The obligation to ensure security of processing.
    v. The Vendor shall not, by any act or omission, place the Client in breach of any Applicable Law including Data Protection Law.

4. Personal data usage and use limits:

a. 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.

b. Vendor acknowledges that Client is entitled to maintain control over Client Personal Data and agrees to follow its instructions for processing.

c. In no case will Client Personal Data processed by the Vendor be furnished or made accessible to any third party, without the prior written approval of the Client, or as provided in this Privacy Agreement.

d. Vendor shall not, directly or indirectly, sell, rent, disclose, distribute, disseminate, commercially exploit, or transfer any Client Personal Data to any third party for any purpose whatsoever, without the prior written approval of the Client.

e. Vendor shall not enrich/update its own databases (existing or new) with the Client Personal Data.

f. Vendor will collect personal data from Client's customers, employees, or other data subjects or third parties on behalf of Client only with the prior written approval and appropriate instructions from the Client towards such collection.

g. Where the Vendor collects personal data on behalf of Client, it shall notify the individuals (data subjects) in accordance with the Data Protection Laws of the circumstances and purposes of such collection, and obtain necessary permissions and consents required to enable Client to use, disclose, or transfer (process) such personal data.

5. Security:

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. The Vendor shall:

a. Implement, at the least, the technical and organisational measures specified in Annexure II of this Privacy Agreement to ensure the security of the Client Personal Data.
b. Implement any additional reasonable security measures that Client may prescribe from time to time to safeguard Client Personal Data against personal data breach and/or any other (external or internal) threats.

6. Sensitive data:

If the processing involves Sensitive Data, the Vendor shall apply specific restrictions and/or additional safeguards as per the instructions of the Client.

7. Notification of personal data breach:

a. 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 at **privacy@emeritus.org** without undue delay, and in not more than after twenty-four (24) hours after it becomes aware of the personal data breach. Such notification shall contain, at least:
    i. A description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned).
    ii. 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. Vendor shall, in coordination with the Client, take reasonable and appropriate steps to stop and remediate any unauthorized use of Client Personal Data affected by the personal data breach.
c. Unless required by the applicable Data Protection Law, 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.

8. **Vendor employees:**
    a. 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.
    b. Vendor shall take reasonable steps to ensure the reliability of any personnel who have access to Client Personal Data and shall ensure that persons authorised 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.
    c. Vendor accepts full liability for any breach(es) of this Privacy Agreement by any of its employees.

9. **Documentation and compliance:**
    a. Vendor shall deal promptly and adequately with inquiries from the Client about the processing of Client Personal Data in accordance with this Privacy Agreement. The Vendor shall be able to demonstrate compliance with this Privacy Agreement.
    b. Vendor shall make available to the Client all information necessary to demonstrate compliance with the obligations that are set out in this Privacy Agreement and those that stem directly from the applicable Data Protection Laws that includes providing complete, accurate, and up to date written records of all processing activities carried out on behalf of the Client.

10. **Data subject requests:**
    a. 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.
    b. If the Vendor receives a request directly from a data subject in relation to their personal data, Vendor will promptly forward such request to the Client and in any event within three (3) days of receipt. Vendor shall not respond to data subject request(s) unless instructed and authorized by the Client in writing.

11. **Right to audit:**
    a. At Client's request, the Vendor shall permit and contribute to audits of the processing activities covered by this Privacy Agreement and other relevant agreements between the Parties, at reasonable intervals or if there are indications of non-compliance.

b. Client 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 Vendor and shall, where appropriate, be carried out with reasonable notice.

12. Use of sub-processors:

The Vendor shall not subcontract any of its processing operations performed on behalf of the Client to a sub-processor, including its affiliates, without the Client's prior specific written authorisation.

13. Disclosure:

a. If any law enforcement agency, government, or regulatory authority sends to the Vendor a demand for disclosure of the Client Personal Data, the Vendor will attempt to redirect such law enforcement agency, government, or regulatory authority to request that data directly from the Client and the Vendor is entitled to provide the Client's basic contact information to such law enforcement agency, government, or regulatory authority.

b. Except as prescribed by the lawful order of a court, such as a subpoena, or in response to a lawful access request by a law enforcement agency (subject to the clause 13a above), no Client Personal Data shall be released/disclosed by the Vendor without the Client's written consent.

c. Unless otherwise prohibited by the court or law enforcement agency making the request, the Vendor must inform the Client of the receipt of such a request within two (2) working days to allow the Client to seek a protective order or exercise other appropriate remedy available to the Client. The Vendor shall not enter into any communication or take action without the express agreement and authorization of the Client.

14. International transfers:

a. Any transfer of Client Personal Data to or access from a third country by the Vendor shall be done only on the basis of prior authorization and documented instructions from the Client.

b. Parties agree that to the extent any transfer of Client Personal Data to the Vendor from the Client is considered a Restricted Transfer, as set out under this Privacy Agreement, the conditions of this section shall become applicable. Parties agree to abide by the Model Clauses which are incorporated hereto by reference and form an integral part of this Privacy Agreement. In case any provision of this Privacy Agreement contradicts, directly or indirectly, 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. Annexures I, II and III to the Model Clauses shall be deemed completed with the information 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. Annexures I, II and III to the Model Clauses shall be deemed completed with the information 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.

15. Indemnification:

Vendor agrees to defend, indemnify, and hold the Client harmless as agreed between the parties under the Consultancy Agreement or any other relevant agreement(s) related to the Services in question, 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 the Vendor, or its affiliates, employees, or sub-processors. This clause shall survive, till perpetuity, the termination or expiry of this Privacy Agreement and/or other relevant agreements (including SOWs) between the parties.

16. 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 collects 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 (subject to clause 12 of this Privacy Agreement), 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.

17. Non-compliance with this Privacy Agreement and termination:

a. Without prejudice to any provisions of the applicable Data Protection Laws, in the event that the Vendor is in breach of its obligations under this Privacy Agreement, the Client may instruct the Vendor to suspend the processing of personal data until the latter complies with this Privacy Agreement or the contract is terminated. 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.

b. The Client shall be entitled to terminate the contract, without liability, insofar as it concerns processing of personal data in accordance with this Privacy Agreement if:
    i. The processing of Client Personal Data by the Vendor has been suspended by the Client pursuant to point (a) and if compliance with this Privacy Agreement is not restored within a reasonable time and in any event within one month following suspension.
    ii. The Vendor is in substantial or persistent breach of this Privacy Agreement or its obligations under the applicable Data Protection Laws.
    iii. The Vendor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to this Privacy Agreement or to the applicable Data Protection Laws.

18. Post termination:

a. Following termination of the contract, the Vendor shall (and ensure that its sub-processors shall, if authorized in terms of clause 12), at the choice of the Client (and within ten days of receipt of communication from the Client of such choice), delete all Client Personal Data (whether in electronic or physical form) processed on behalf of the Client 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. Until the data is deleted or returned, the Vendor shall continue to ensure compliance with this Privacy Agreement.

b. Vendor shall confirm in writing within five (5) days of such erasure or return, as applicable, that the Vendor and its sub-processors (if applicable) 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.

19. Term:

This Privacy Agreement will remain in full force and effect for as long as any processing of Client Personal Data remains in force and effect. Termination for any reason shall not relieve the Vendor from its obligations previously in effect with respect to the Client Personal Data.

ANNEXURE I of the Privacy Agreement

A. LIST OF PARTIES

Data exporter(s):

Name: "Company", as described in the Consultancy Agreement, and its affiliates and subsidiaries (as applicable)

Address: As given in the Consultancy Agreement

Contact person's name, position and contact details: As given in the Consultancy Agreement

Activities relevant to the data transferred: Exporter collabotares with top-tier universities across the globe and offers online and blended educational programs that include short courses, degree programs, professional certificates, and senior executive programs to the learners/students.

Role: As given in the Consultancy Agreement

Data importer(s):

Name: "Consultant" as described in the Consultancy Agreement

Address: As given in the Consultancy Agreement

Contact person's name, position and contact details: As given in the Consultancy Agreement

Activities relevant to the data transferred: Consultant is a subject matter expert and possesses skill-set, qualification, and specialized experience for delivering the Services as defined in the Consultancy Agreement.

Role: As given in the Consultancy Agreement

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Course/program participants i.e., learners/students

Categories of personal data transferred

- Identification data like full names
- Contact details like phone numbers and email addresses
- Educational and employment data like qualification, job title, designation, employer details, etc.
- Location of the data subjects

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.

Not applicable

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

Continous basis

Nature of the processing

- Collection
- Storage
- Use

Purpose(s) of the data transfer and further processing

- Delivering the course content to the learners/students via online/in-person sessions.
- Answering learners'/students' questions on Q&A boards.
- Grading, evaluating, and providing written feedback on assignments.
- Responding to learners'/students' questions and doubts.

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

As per the terms and duration of the Consultancy Agreement.

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

Engaging of sub-processors is not authorized and is out of scope.

C. COMPETENT SUPERVISORY AUTHORITY

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

The Spanish Data Protection Agency (AEPD)

ANNEXURE II of the Privacy Agreement - 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.

a. Anti-virus must be kept up to date.

b. Firewall must be enabled.

c. Licensed and updated software including operating system.

d. Two-factor authentication on all Emeritus related applications. For more information on two factor authentication, please refer to:

   https://www.techtarget.com/searchsecurity/definition/two-factor-authentication

e. Device idle timeout lock with password enabled.

f. Strong password with alphanumeric characters, at least 8 characters long. For example: @Pple3sAreT@$ty

g. Do not connect to an un-secure wireless network, always use WPA2 protected WiFi.

h. Shredding unwanted documents with Emeritus data on them.

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.

Engaging of sub-processors is not authorized and is out of scope.

ANNEXURE III of the Privacy Agreement – LIST OF SUB-PROCESSORS

Engaging of sub-processors is not authorized and is out of scope.