535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

MINDTICKLE DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Exhibits, Appendices and Annexes, ("DPA") is incorporated by this reference into the agreement for the purchase of Mindtickle's online learning and enablement system software offered as a service (commonly named the SaaS Subscription Agreement or Master Subscription and Services Agreement and/or Order Form) between Customer and MindTickle, Inc. or MindTickle Interactive Media Private Limited (each, "Mindtickle") (the "Agreement"), and applies to all orders for the Subscription Services to reflect the parties' agreement with regard to the Processing of Personal Data. All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. This DPA is entered into as of the later of the dates beneath the parties' signatures below.

This DPA is supplemental to the Agreement and sets out the terms that apply when Personal Data (defined below) is Processed (defined below) by Mindtickle under the Agreement. The purpose of the DPA is to ensure such Processing is conducted in accordance with Data Protection Laws (defined below), and with due respect for the rights and freedoms of individuals whose Personal Data are processed.

HOW TO EXECUTE THIS DPA

This DPA has been pre-signed by Mindtickle as the data importer. When Mindtickle receives the DPA completed and signed by Customer as specified below, this DPA will become a legally binding addendum to the Agreement. To make this DPA a part of the Agreement, Customer must do the following:

(a) Complete the information in the signature block of this DPA and have an authorized representative sign on pages 7 and 19.
(b) If e-signatures are accepted in Customer's jurisdiction and Customer elects to execute the DPA through Adobe Sign, follow the prompts to provide the required information and e-signature as indicated above and, upon selecting "Click to Sign" at the end, the DPA will be executed and submitted. Alternatively, the DPA may be printed, completed and signed as indicated above, and returned to Mindtickle via email at: dealdesk@mindtickle.com.

DATA PROCESSING TERMS

The parties agree as follows:

1. Definitions

1.1. For the purposes of this DPA:

(a) **"Affiliate(s)"** has the same meaning ascribed to it in the Agreement and, if not defined in the Agreement, the term means any legal entity directly or indirectly controlling, controlled by or under common control with a party, where control means the ownership of a majority share of the stock, equity or voting interests of such entity.
(b) **"Customer"** means the non-Mindtickle party to both the Agreement and this DPA that has access to the Subscription Services.
(c) **"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., and its implementing regulations.
(d) **"Controller"** means the entity which determines the purposes and means of the Processing of Personal Data.
(e) **"Customer Data"** means any electronic data, content, information, or material submitted by Customer or its Users through the Platform that is not already available publicly.
(f) **"Data Protection Laws"** means all laws and binding regulations of the European Union, the EEA, Switzerland and United Kingdom applicable to the Processing of Personal Data under the Agreement,

including Regulation 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 ("GDPR"), including as implemented or adopted under the laws of the United Kingdom. For clarity, if Mindtickle's Processing activities involving Personal Data are not within the scope of an applicable Data Protection Law, such law is not applicable for purposes of this Addendum.

(g) **"Data Subject"** means the identified or identifiable person to whom Personal Data relates.
(h) **"EEA"** means the European Economic Area including EFTA states, Norway, Iceland and Liechtenstein.
(i) **"Mindtickle"** means MindTickle, Inc. or MindTickle Interactive Media Private Limited, respectively, that is a party to both the Agreement and this DPA.
(j) **"Personal Data"** means any information relating to an identified or identifiable natural person, where such data is Customer Data.
(k) **"Process"** or **"Processing"** means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
(l) **"Processor"** means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA.
(m) **"Sensitive Personal Data"** means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.
(n) **"Standard Contractual Clauses"** means the agreement executed by and between Customer and Mindtickle and attached hereto as "Exhibit A" pursuant to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
(o) **"Sub-processor"** means any Processor engaged by Mindtickle to Process Personal Data in connection with the Subscription Services.
(p) **"Subscription Services"** means the online learning and enablement system software offered as a service hosted on the Mindtickle platform (the "Platform") and provided by Mindtickle to Customer under the Agreement.
(q) **"Supervisory Authority"** means an independent public authority which is established by an EU member state pursuant to the GDPR or, for the United Kingdom, the Information Commissioner's Office ("ICO").
(r) **"UK Addendum"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the ICO as set out in Exhibit B attached hereto.

1.2. Capitalized terms used but not defined in this DPA have the same meanings as set out in the Agreement.

2. Roles and Responsibilities

2.1. Parties' Roles. Customer is (or represents that it is acting with full authority on behalf of) the "Controller," and appoints Mindtickle as a "Processor" (as such terms or equivalent thereof are defined under applicable Data Protection Law) to process the Personal Data on Customer's behalf. In some circumstances Customer may be a Processor, in which case Customer appoints Mindtickle as Customer's sub-processor, which shall not change the obligations of either Customer or Mindtickle under this DPA, as Mindtickle will remain a Processor with respect to the Customer in such event.

2.2. Customer's Processing of Personal Data. Customer shall, in its use of the Subscription Services, Process Personal Data in accordance with the requirements of Data Protection Laws, including any applicable requirement to provide notice to Data Subjects of the use of Mindtickle as Processor. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data. Further, Customer has, and will continue to have, the right to transfer, or provide access to, the Personal Data to Mindtickle for Processing by Mindtickle and its Sub-processors in accordance

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

with the terms of the Agreement and this DPA. Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data to the extent applicable under the CCPA.

2.3. Mindtickle's Processing of Personal Data. Mindtickle shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions or as required by Union or Member State law to which the processor is subject. In case the Personal Data needs to be Processed as required by Union or Member State law, Mindtickle shall inform the Customer of that legal requirement before Processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be provided by the Customer throughout the duration of the Processing of Personal Data. Mindtickle processes Customer Data for the following purposes: (i) Processing as reasonably required to provide the services as set forth in the Agreement and this DPA; (ii) Processing initiated by Users in their use of the Subscription Services; (iii) Processing to comply with other reasonable instructions provided by Customer (e.g., via email or support tickets); and (iv) as otherwise required by applicable law. The Agreement and this DPA set out Customer's complete and final instructions to Mindtickle in relation to the Processing of Personal Data and any Processing required outside of the scope of these instructions (inclusive of the rights and obligations set forth under the Agreement) will require prior written agreement of the parties. Mindtickle shall comply with its obligations as a "Service Provider" under CCPA and will not use, or disclose Customer Data except as necessary to provide the Subscription Services. Mindtickle does not sell (as the term is defined in the CCPA) the Customer Data we collect.

3. Security

3.1. Security. Mindtickle shall implement and maintain appropriate technical and organisational measures ("Security Measures" listed in Annex II) taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects. Such measures shall be designed to ensure a level of security, confidentiality, integrity, and resilience appropriate to the risk in order to protect Personal Data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, access or use.

3.2. Confidentiality of Processing. Mindtickle shall ensure that Mindtickle's access to Personal Data is limited to those personnel performing services in accordance with the Agreement. Mindtickle shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements or are under an appropriate statutory obligation of confidentiality.

3.3. Security Incidents. Mindtickle shall notify Customer after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, transmitted, stored or otherwise Processed by Mindtickle or its Sub-processors of which Mindtickle becomes aware ("Security Incident"), pursuant to the terms of the Agreement, within the time period required under applicable Data Protection Laws but in any event no more than forty-eight (48) hours following confirmation of the Security Incident by Mindtickle and shall provide such timely information as Customer may reasonably require to enable Customer to fulfil any data breach reporting obligations under Data Protection Laws.

3.4. Remediation of Security Incident. Mindtickle will take reasonable steps to identify and remediate the cause of Security Incident to the extent the remediation is within Mindtickle's reasonable control. Mindtickle's notification of or response to a Security Incident under Section 3.3 shall not be construed as an acknowledgement by Mindtickle of any fault or liability with respect to the Security Incident. The obligations under Section 3.4 shall not apply to Security Incidents that are caused by Customer or Customer's Users.

3.5. Updates to Security Measures. Customer is responsible for reviewing the information made available by Mindtickle relating to these Security Measures and making an independent determination as to whether the Subscription Services meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

that Mindtickle may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the material degradation of the overall security of the Subscription Services purchased by Customer.

3.6. Customer Responsibilities. Notwithstanding Mindtickle's commitments made herein, Customer is responsible for its secure use of the Subscription Services, including securing its account authentication credentials, protecting the security of Customer Data when in transit to and from the Platform and taking any appropriate steps to securely encrypt or backup any Customer Data uploaded to the Platform, if required.

4. Sub-processing

4.1. Sub-processors. Customer agrees that Mindtickle may engage Mindtickle affiliates and Sub-processors to Process the Personal Data in connection with the provision of the Subscription Services. Mindtickle shall remain liable for any breach of the DPA caused by a Sub-processor to the same extent Mindtickle would be liable if performing the services of such Sub-processor directly under the terms of this DPA.

4.2. Sub-Processor Obligations. Where Mindtickle authorizes any Sub-processor, Mindtickle will enter into a written agreement with the Sub-processor imposing data protection obligations that require the Sub-processor to protect the Customer Data to the standard required by Data Protection Laws and this DPA, to the extent applicable to the nature of the services provided by such Sub-processor, including the limitations set forth in Section 3.2 above. At the Customer's request, Mindtickle shall provide a copy of the sub-processor agreement and any subsequent amendments to the Customer. To the extent necessary to protect business secret or other confidential information, including personal data, Mindtickle may redact the text of the agreement prior to sharing the copy.

4.3. Current Sub-processors and Changes to Sub-processors. The Sub-processors currently engaged by Mindtickle and authorized by Customer are listed at Mindtickle's Sub-processor web page (the "Sub-processor List"): https://www.mindtickle.com/sub-processor-repository/. The Sub-processor List includes a mechanism for Customer to subscribe to notifications of any new Sub-processors or changes to the Sub-processor List. If Customer would like to receive notifications of new Sub-processors that Mindtickle plans to engage, Customer must subscribe on that web page in order to be notified. Mindtickle shall provide Customers that have subscribed with thirty (30) days' prior notice before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Subscription Services. Customer may object in writing to Mindtickle's appointment of a new Sub-processor within ten (10) days of such notice, provided that such objection is based on reasonable grounds relating to data protection and security. In such event, the parties will discuss such concerns in good faith with a view to achieving a mutually agreeable resolution. If the parties are unable to reach agreement on a resolution of the objection within a reasonable period of time, which shall not exceed thirty (30) days from the date of notice, either party may terminate the applicable Order Form(s) without penalty, by providing written notice to the other party, with respect only to those services which cannot be provided by Mindtickle without the use of the objected-to new Sub-processor.

4.4. Emergency Replacement. Mindtickle may replace a Sub-processor if the need for the change is urgent and necessary to provide the Subscription Services and the reason for the change is beyond Mindtickle's reasonable control. In such instance, Mindtickle shall notify Customer of the replacement without undue delay, and Customer shall retain the right to object to the replacement Sub-processor pursuant to Section 5.3 above.

4.5. Notice to Data Controller. Customer agrees that it shall either (i) provide a list of Data Controllers in Annex I.A. or (ii) include the Data Controller's email ID as a subscriber on Mindtickle's Sub-processor List for ensuring that changes to Sub-Processor List are communicated by Mindtickle to Data Controller to comply with Clause 9(a) of Module Three.

5. Cooperation

5.1. Responding to Individuals Exercising Their Rights Under Applicable Data Protection Laws. Taking into account the nature of the Processing, Mindtickle shall provide commercially reasonable assistance, including by

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

appropriate technical and organizational measures as reasonably practicable, to enable Customer to respond to any inquiry, communication or request from an individual seeking to exercise his or her rights under applicable Data Protection Laws, which may include right of access, right to rectification, restriction of Processing, object to the Processing, erasure or data portability, as applicable (each, a "Data Subject Request"). In the event such Data Subject Request is made directly to Mindtickle, Mindtickle shall promptly inform Customer by providing the full details of the request and shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. For the avoidance of doubt, Customer is responsible for responding to Data Subject Requests involving that individual's Personal Data.

5.2. Regulatory Authorities. To the extent legally permitted, Mindtickle shall notify Customer without undue delay if a Supervisory Authority, law enforcement authority or other regulatory authority makes any inquiry or request for disclosure regarding Personal Data, and will attempt to redirect the Supervisory Authority, law enforcement agency, or other regulatory authority to request that data directly from Customer. As part of this effort, Mindtickle may provide Customer's basic contact information to the authority. If compelled to disclose Customer Data to a Supervisory Authority, law enforcement agency, or other regulatory authority, Mindtickle will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Mindtickle is legally prohibited from doing so.

5.3. Data Protection Impact Assessments and Prior Consultation. Mindtickle shall, to the extent required by Data Protection Laws, provide Customer with reasonable assistance, at Customer's expense, with data protection impact assessments and/or prior consultations with Supervisory Authorities or other regulatory authorities that Customer is required to carry out under Data Protection Laws, but only where Customer does not otherwise have access to the relevant information, and to the extent such information is available to Mindtickle.

6. Security Reports and Audits

6.1. Security Reports. Customer acknowledges that Mindtickle is regularly audited against SOC 2 Type 2 or equivalent standards by independent third-party auditors. Upon Customer's written request, once annually, Mindtickle will provide a copy of the most recent SOC 2 Type 2 Report ("Report") to Customer, as relevant given Mindtickle's then current audit protocol, which Report(s) shall be Mindtickle's Confidential Information subject to the confidentiality provisions of the Agreement. Mindtickle shall also respond within a reasonable time to a reasonable written information security questionnaire submitted to it by Customer once annually.

6.2. Security Audits. Customer agrees to the provision of the Report by Mindtickle in fulfilment of any audit cooperation responsibilities that may apply to Mindtickle under Data Protection Laws. Notwithstanding the foregoing, if an audit is necessary to meet its obligations under any applicable Data Protection Laws, Mindtickle shall allow Customer (or Customer's independent third-party auditor) to conduct an audit of the procedures relevant to the protection of Personal Data, subject to the confidentiality provisions of the Agreement. Customer and Mindtickle will discuss and agree in advance on the reasonable start date, scope, and duration of, and security and confidentiality controls applicable to, any audit; and Mindtickle reserves the right to charge a fee (based on Mindtickle's reasonable costs) for any such audit. Mindtickle will provide further details of any applicable fee and the basis of its calculation to Customer in advance of such audit. Customer shall promptly notify Mindtickle with information regarding any material non-compliance discovered during an audit, and Mindtickle shall use commercially reasonable efforts to address any confirmed, material non-compliance.

7. Deletion or Return of Customer Data

7.1. Deletion or Return of Data. Upon termination or expiration of the Agreement, Customer shall, in accordance with the terms of the Agreement, request within 30 days of termination of the Agreement the return or deletion of all relevant Customer Data, save to the extent that Mindtickle is required by any applicable law to retain some or all of the Personal Data. In such event, Mindtickle shall extend the protections of the Agreement and this DPA to such Personal Data and limit any further Processing of such Personal Data to only those limited purposes that require the retention, for so long as Mindtickle maintains the Personal Data. Customer

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

acknowledges that, after such 30 day period post termination of Agreement, the Customer Data will not be available for return or retrieval to Customer.

7.2. Compliance Records. Documentation which is used to demonstrate orderly data processing in accordance with the Agreement and the DPA may be stored beyond the contract duration by Mindtickle in accordance with the retention periods specified by the respective Data Protection Laws.

8. Transfer Mechanisms

8.1. Transfer Mechanism. Where required in order to comply with applicable Data Protection Laws, the Standard Contractual Clauses attached hereto as Exhibit A and the following additional terms shall apply only to Personal Data that is transferred from the EEA, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws of the foregoing territories. Transfers of Personal Data from the United Kingdom shall be also subject to the UK Addendum set out in Exhibit B. The transfer mechanisms listed below shall apply to such transfers and can be directly enforced by the parties to the extent such transfers are subject to the Data Protection Laws and Regulations of EEA, either directly or via onward transfer, to any country or recipient:

(a) The Standard Contractual Clauses and the additional terms specified in this Section 9.1 apply to the legal entity that has executed the Standard Contractual Clauses as a data exporter and those of its affiliates that are subject to the Data Protection Laws if and to the extent Mindtickle Processes Personal Data for which such affiliate(s) qualify as the Controller. For the purpose of the Standard Contractual Clauses, the aforementioned entities shall be deemed "data exporters";

(b) Where Customer is a Controller and a data exporter of Personal Data and Mindtickle is a Processor and data importer in respect of that Personal Data, then the Parties shall comply with the Module Two: Transfer controller to processor ("**Module Two**") of Standard Contractual Clauses;

(c) Where Customer is a Processor acting on behalf of a Controller and a data exporter of Personal Data and Mindtickle is a Processor and data importer in respect of that Personal Data, the Parties shall comply with the terms of Module Three: Transfer processor to processor Clauses ("**Module Three**") of Standard Contractual Clauses.

9. Miscellaneous

9.1. Conflicts. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control. If there is a conflict between this DPA and the Standard Contractual Clauses, where the Standard Contractual Clauses are applicable, the Standard Contractual Clauses will control.

9.2. Claims. Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. Each party's and all of their Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, whether in contract, tort or under any other theory of liability, is subject to the "Limitation of Liability" section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and the DPA together.

9.3. Termination. Customer may terminate this DPA and the Standard Contractual Clauses at Customer's discretion upon Mindtickle's receipt of Customer's written notice of termination of the Agreement.

[Signature page to follow]

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

ACCEPTED AND AGREED TO:

CUSTOMER: _____
Legal Name of Customer

By: _____
Authorized Signature

Print Name: _____

Title: _____

Date: _____

MINDTICKLE, INC

By: DocuSigned by: Deepak Diwakar BF42F2A9BEF749A...
Authorized Signature

Print Name: Deepak Diwakar

Title: CTO & DPO

Date: 30-09-2022

MINDTICKLE INTERACTIVE MEDIA PRIVATE LIMITED

By: DocuSigned by: Deepak Diwakar BF42F2A9BEF749A...
Authorized Signature

Print Name: Deepak Diwakar

Title: CTO & DPO

Date: 30-09-2022

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

EXHIBIT A - STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements 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 (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

(c) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  (ii) Clause 8 – Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);
  (iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
  (iv) Clause 12 – Modules Two and Three : Clause 12(a), (d) and (f);
  (v) Clause 13;
  (vi) Clause 15.1(c), (d) and (e);
  (vii) Clause 16(e);
  (viii) Clause 18 – Modules Two and Three: Clause 18(a) and (b).
(d) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, 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 Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1. Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3. Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4. Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5. Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6. Security of processing

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter '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 purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all 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.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7. Sensitive data

Where the transfer 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 (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8. Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9. Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for 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 audit, the data exporter may take into account relevant certifications held by the data importer.
(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1. Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter ([3]).

8.2. Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3. Transparency

[3] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4. Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5. Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6. Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

all 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.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7. Sensitive data

Where the transfer 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 (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8. Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([4]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9. Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([5]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).
(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary

[5] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

rights for data subjects. ([6]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

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

Clause 10

Data subject rights

MODULE TWO: Transfer controller to processor

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

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

[6] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

(d) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([7]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
(b) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
    (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
    (ii) refer the dispute to the competent courts within the meaning of Clause 18.
(c) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
(d) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
(e) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

[7] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
   (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
   (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([8]);
   (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

[8] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

15.1. Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) [For Module Three: The data exporter shall forward the notification to the controller.]

(c) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(d) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.

(e) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(f) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2. Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

  (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

  (ii) the data importer is in substantial or persistent breach of these Clauses; or

  (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

  In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
(b) The Parties agree that those shall be the courts of the EU Member State in which the data exporter is established.
(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
(d) The Parties agree to submit themselves to the jurisdiction of such courts.

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: _____

Address: _____

Contact person's name, position and contact details:

_____

Activities relevant to the data transferred under these Clauses: Data exporter would be using the online learning and enablement system software offered as a Service by the data importer. The processing activities would include the storage of the training content and learners data, and any other Processing necessary to obtain the services, including customer support and technical support, provided by data importer, and as otherwise permitted in accordance with the Agreement and as compelled by law.

Signature: _____

Date: _____

Role (controller/processor): _____

Data Protection Officer's name and contact details (if applicable):

_____

European Union Representative's name and contact details (if applicable):

_____

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

Data importer(s):

1. Name: MindTickle, Inc.

Address: 535 Mission St, 14th Floor, San Francisco, California 94105, United States of America

Contact person's name, position and contact details: Deepak Diwakar, CTO and DPO, dpo@mindtickle.com

Activities relevant to the data transferred under these Clauses: Mindtickle performs cloud hosting for its online learning and enablement system software offered as a service hosted on the Platform, and such other services as described in the Agreement. The Personal Data transferred will be Processed in accordance with the Agreement and this DPA, and may be subject to the following Processing activities: storage and other Processing necessary to provide, maintain and improve the services provided to Customer, including customer support and technical support, and as otherwise permitted in accordance with the Agreement, and as compelled by law.

Signature: DocuSigned by: Deepak Diwakar BF42F2A9BEF749A...

Date: 30-09-2022

Role (controller/processor): Processor

2. Name: MindTickle Interactive Media Private Limited

Address: 4th Floor, Solitaire World, Pune Bangalore Highway, Baner, Pune, Maharashtra – 411045, India

Contact person's name, position and contact details: Deepak Diwakar, CTO & DPO, dpo@mindtickle.com

Activities relevant to the data transferred under these Clauses: Mindtickle performs cloud hosting for its online learning and enablement system software offered as a service hosted on the Platform, and such other services as described in the Agreement. The Personal Data transferred will be Processed in accordance with the Agreement and this DPA, and may be subject to the following Processing activities: storage and other Processing necessary to provide, maintain and improve the services provided to Customer, including customer support and technical support, and as otherwise permitted in accordance with the Agreement, and as compelled by law.

Signature: DocuSigned by: Deepak Diwakar BF42F2A9BEF749A...

Date: 30-09-2022

Role (controller/processor): Processor

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customer may submit Personal Data to the Platform, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to, Personal Data relating to the following categories of data subject:

- Permitted Users;
- employees of Customer;
- consultants of Customer (who are natural persons);
- contractors of Customer (who are natural persons);
- agents of Customer (who are natural persons); and/or
- any other individuals authorized by Customer to use the Subscription Services.

Categories of personal data transferred

Customer may submit Personal Data to the Platform, the extent of which is determined and controlled by Customer, and which may include, but is not limited to, Personal Data transfer relating to following categories of data:

- Professional identification and contact data (first name, last name, title, business address, business phone number, business email address, profile photograph, etc.);
- Business information (reporting manager, reporting hierarchy, business unit, geographic details, etc.)
- Training data (training presentations, training videos, training feedback or comments, etc.)
- Practice data (audio recording, call recording, video recording, voice over slide show, voice over presentation, etc.)
- Device data (IP address, device name, browser / OS version, device identifier, device configuration, settings, etc.).

Sensitive data transferred (if applicable)

Not applicable

The frequency of the transfer

Continuous basis

Nature of the processing

Mindtickle will Process the Personal Data as necessary to provide Subscription Services pursuant to the Agreement, and may be subject to the following Processing activities: storage and other Processing necessary to provide, maintain and improve the services provided to Customer, including customer support and technical support, and as otherwise permitted in accordance with the Agreement, and as compelled by law.

Purpose(s) of the data transfer and further processing

The purpose of the Processing under this DPA is the provision of the Subscription Services to the Customer and the performance of Mindtickle's obligations under the Agreement and this DPA (or as otherwise agreed by the parties).

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

Personal Data will be retained for the entire duration of term of the Agreement unless earlier terminated as set forth herein.

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

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

The Sub-processors currently engaged by Mindtickle, including details of the subject matter, nature and duration of processing, are listed at Mindtickle's Sub-processor web page (the "**Sub-processor List**"): https://www.mindtickle.com/sub-processor-repository/

C. COMPETENT SUPERVISORY AUTHORITY

[Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Mindtickle has implemented technical and organizational measures 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 freedom of natural persons. The specific technical and organizational measures implemented by Mindtickle, as documented at https://mindtickle.com/technical-and-organizational-security-measures/ and updated from time to time without reducing the overall security posture, covers the following areas:

(a) Measures of pseudonymisation and encryption of personal data
(b) Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
(c) Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
(d) Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
(e) Measures for user identification and authorisation
(f) Measures for the protection of data during transmission
(g) Measures for the protection of data during storage
(h) Measures for ensuring physical security of locations at which personal data are processed
(i) Measures for ensuring events logging
(j) Measures for ensuring system configuration, including default configuration
(k) Measures for internal IT and IT security governance and management
(l) Measures for certification/assurance of processes and products
(m) Measures for ensuring data minimisation
(n) Measures for ensuring data quality
(o) Measures for ensuring limited data retention
(p) Measures for ensuring accountability
(q) Measures for allowing data portability and ensuring erasure

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

EXHIBIT B - INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start Date	The date on which the Annex I of Exhibit A is signed by both the parties	
The Parties	**Exporter(who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	As set out in Annex I of Exhibit A	As set out in Annex I of Exhibit A
Key Contact	As set out in Annex I of Exhibit A	As set out in Annex I of Exhibit A

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs		☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: **Date:** The date on which the Annex I of Exhibit A is signed by both the parties **Reference (if any):** EXHIBIT A - STANDARD CONTRACTUAL CLAUSES				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: As set out in Exhibit A, Annex I, paragraph A
Annex 1B: Description of Transfer: As set out in Exhibit A, Annex I, paragraph B
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set out in Annex II of Exhibit A
Annex III: List of Sub processors (Modules 2 and 3 only): As set out in 4.3 of DPA and Exhibit A, Annex I, paragraph B

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
    b. In Clause 2, delete the words:

       "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

       "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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 (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

b. reflects changes to UK Data Protection Laws;

535 Mission St, 14th Floor, San Francisco, CA 94105, USA
Phone: +1 800 231 5578 | E-Mail: privacy@mindtickle.com
Web: www.mindtickle.com

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a. its direct costs of performing its obligations under the Addendum; and/or

    b. its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.