DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") forms part of the Agreement ("**Agreement**") between: (i) _____ **("Client")** acting on its own behalf and as agent for each Client Affiliate; and (ii) Absorb Software Inc. ("**Company**") acting on its own behalf and as agent for each Company Affiliate. The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Applicable Laws**" means any legislation (including primary or secondary legislation), statute, or regulation from time to time in force in either (a) any European Union Member State laws; (b) any nation of the United Kingdom; or (c) any other jurisdiction in which either any Client Group Member or any Company Group Member operates, and which is applicable to any Client Group Member or any Company Group Member in the receipt or provision of the Services (as the case may be);

1.1.2 "**Client Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Client, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.3 "**Client Group Member**" means Client or any Client Affiliate;

1.1.4 "**Client Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Client Group Member pursuant to or in connection with the Agreement;

1.1.5 "**Contracted Processor**" means Company, Company Affiliate or a Sub-processor;

1.1.6 "**Company Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;

1.1.7 "**Data Protection Law(s)**" means:

1.1.7.1 the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**");

1.1.7.2 the laws of any Member State of the European Union implementing or supplementing the EU GDPR;

1.1.7.3 the EU GDPR as it forms part of the law of the United Kingdom by virtue of the Data Protection Act 2018 and the European Union (Withdrawal) Act 2018 ("**UK GDPR**");

1.1.7.4 the UK Data Protection Act 2018;

1.1.7.5 the laws or legislation of any other jurisdiction that relate to or govern the processing of personal data or personal information,

in each case, to the extent applicable in respect of any processing of Client Personal Data in connection with the Services and each as amended, extended, re-enacted or replaced from time to time;

1.1.8 "**EEA**" means the European Economic Area;

1.1.9 "**Restricted Transfer**" means:

1.1.9.1 a transfer of Client Personal Data from any Client Group Member to a Contracted Processor; or

1.1.9.2 an onward transfer of Client Personal Data from a Contracted Processor to another Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of any of:

(a) the Standard Contractual Clauses;

(b) a determination under the relevant Data Protection Law that the country or international organisation to which the transfer of Client Personal Data will be made ensures an adequate level of protection for such Client Personal Data; and

(c) any other appropriate safeguard in respect of such data transfer as is provided for under the relevant Data Protection Law;

1.1.10 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Company for Client Group Members pursuant to the Agreement;

1.1.11 "**Standard Contractual Clauses**" means the Annex to the 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 (as may be amended, updated or superseded from time to time) for transfers of Client Personal Data as set out in Annex 2 (the "**EU Standard Contractual Clauses**"). ;

1.1.12 "**Sub-processor**" means any person (including any third party and any Company Affiliate, but excluding an employee of Company or any of its sub-contractors) appointed by or on behalf of Company or any Company Affiliate to Process Personal Data on behalf of any Client Group Member in connection with the Agreement; and

1.2 The terms, "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Authority

Company warrants and represents that, before any Company Affiliate Processes any Client Personal Data on behalf of any Client Group Member, Company's entry into this Addendum as agent for and on behalf of that Company Affiliate will have been duly and effectively authorised (or subsequently ratified) by that Company Affiliate.

3. Processing of Client Personal Data

3.1 Company and each Company Affiliate shall:

3.1.1 comply with all applicable Data Protection Laws in the Processing of Client Personal Data; and

3.1.2 not Process Client Personal Data other than on the relevant Client Group Member's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Company or the relevant Company Affiliate shall to the extent permitted by Applicable Laws inform the relevant Client Group Member of that legal requirement before the relevant Processing of that Client Personal Data unless Applicable Laws prohibit this notification on important grounds of public interest.

3.2 Each Client Group Member:

3.2.1 instructs Company and each Company Affiliate (and authorises Company and each Company Affiliate to instruct each Sub-processor) to:

3.2.1.1 Process Client Personal Data; and

3.2.1.2 in particular, transfer Client Personal Data outside the EU/EEA/UK

as reasonably necessary for the provision of the Services and consistent with the Agreement; and

3.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in Section 3.2.1 on behalf of each relevant Client Affiliate.

3.3 Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Client Personal Data as required by article 28(3) EU GDPR (and, where

applicable, equivalent requirements of other Data Protection Laws). Client may make reasonable amendments to Annex 1 by written notice to Company from time to time as Client reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this section 3.3) confers any right or imposes any obligation on any party to this Addendum.

4. Company and Company Affiliate Personnel

Company and each Company Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Client Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Client Personal Data, as strictly necessary for the purposes of the Agreement. The Company and each Company Affiliate shall ensure that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security

5.1 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 natural persons, Company and each Company Affiliate shall in relation to the Client Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in the EU GDPR and UK GDPR (to the extent applicable) and the measures set out at Annex 3 to this Addendum.

5.2 In assessing the appropriate level of security, Company and each Company Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

6. **Sub-processing**

6.1 Each Client Group Member authorises Company and each Company Affiliate to appoint (and permit each Sub-processor appointed in accordance with this section 6 to appoint) Sub-processors in accordance with this section 6 and any restrictions in the Agreement.

6.2 Company and each Company Affiliate may continue to use those Sub-processors already engaged by Company or any Company Affiliate as at the date of this Addendum, subject to Company and each Company Affiliate in each case as soon as practicable meeting the obligations set out in section 6.4.

6.3 Company shall make available to Client a list of current Sub-processors being utilized to perform Services on Support Site. Client will receive notification of changes to same and shall have ten (10) days to notify Company in writing of objection to proposed changes. If Client notifies Company in writing of any objections (on reasonable grounds) to the appointment, Company shall work with Client in good faith to make available a commercially reasonable change in the provision of the Services which avoids the use of that proposed Sub-processor, if available.

6.4 With respect to each Sub-processor, Company or the relevant Company Affiliate shall:

6.4.1 before the Sub-processor first Processes Client Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate due diligence to ensure that

the Sub-processor is capable of providing the level of protection for Client Personal Data required by the Agreement;

6.4.2 ensure that the arrangement between on the one hand (a) Company, or (b) the relevant Company Affiliate, or (c) the relevant intermediate Sub-processor; and on the other hand the Sub-processor, is governed by a written contract including terms which offer at least the same level of protection for Client Personal Data as those set out in this Addendum; and

6.4.3 provide to Client for review such copies of the Contracted Processors' agreements with Sub-processors (which may be redacted to remove sensitive or confidential commercial information or other information not relevant to the requirements of this Addendum) as Client may request from time to time.

6.5 Company shall remain fully responsible to the Client for the performance of the Sub-processor's obligations.

7. Data Subject Rights

7.1 Taking into account the nature of the Processing, Company and each Company Affiliate shall, assist each Client Group Member by implementing appropriate technical and organisational measures, insofar as is possible, for the fulfilment of the Client Group Members' obligations, as reasonably understood by Client, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

7.2 Company shall:

7.2.1 notify Client if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Client Personal Data within five (5) business days of receipt of same; and

7.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Client or the relevant Client Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Company shall to the extent permitted by Applicable Laws inform Client of that legal requirement before the Contracted Processor responds to the request.

8. **Personal Data Breach**

Company shall notify Client without undue delay upon Company or any Sub-processor becoming aware of a Personal Data Breach affecting Client Personal Data, and when making such notification shall provide Client with such information as the Company has available at that time in respect of the Personal Data Breach to aid each Client Group Member in meeting any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws. Company shall co-operate with Client and each Client Group Member and take such reasonable commercial steps as are directed by Client to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

Company and each Company Affiliate shall provide reasonable assistance to each Client Group Member, at Client expense, with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which

Client reasonably considers to be required of any Client Group Member by any provision of the EU GDPR, UK GDPR or equivalent provisions of any other Data Protection Law applicable to such Processing of Client Personal Data, in each case solely in relation to Processing of Client Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. Deletion or return of Client Personal Data

10.1 Subject to section 10.2, Client may, on termination of the Agreement, in its absolute discretion by written notice to Company require Company and each Company Affiliate to (a) return a complete copy of all Client Personal Data to Client by secure file transfer in such format as is reasonably notified by Client to Company; and/or (b) delete and procure the deletion of all other copies of Client Personal Data Processed by any Contracted Processor.

10.2 Each Contracted Processor may retain Client Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Company and each Company Affiliate shall ensure the confidentiality of all such Client Personal Data and shall ensure that such Client Personal Data is only Processed as necessary for the purpose(s) specified in this Addendum and in the Applicable Laws requiring its storage and for no other purpose.

11. Audit rights

11.1 Subject to Sections 11.2 to 11.3, Company and each Company Affiliate shall make available to each Client Group Member on request information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by any Client Group Member or an auditor mandated by any Client Group Member in relation to the Processing of the Client Personal Data by the Contracted Processors. Company shall immediately inform Client if, in its opinion, an instruction pursuant to this section 11 (Audit Rights) infringes the any applicable provision of EU GDPR or UK GDPR or other Data Protection Law.

11.2 Information and audit rights of the Client Group Members only arise under section 11.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the EU GDPR and UK GDPR).

11.3 Client or the relevant Client Affiliate undertaking an audit shall give Company or the relevant Company Affiliate reasonable notice of any audit or inspection to be conducted under section 11.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any inconvenience, damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

12. Restricted Transfers

12.1 Subject to section 12.2, in respect of any Restricted Transfer from a Client Group Member to a Contracted Processor of any Client Personal Data that is subject to the EU GDPR or UK GDPR., the relevant Client Group Member (as "data exporter") and relevant Contracted Processor, (as "data importer") each agree to comply with the provisions of the EU Standard Contractual Clauses in respect of the Restricted Transfer.

12.2 Upon receipt of written request from the other party, Company and Client each agree to reasonably co-operate with the other party with a view to entering into the EU Standard Contractual Clauses to the extent reasonably necessary under Data Protection Laws in respect of any Restricted Transfer (or as may be otherwise required by any Supervisory Authority).

13. General Terms

13.1 The parties to this Addendum:

13.1.1 hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

13.1.2 agree that this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement*,*

other than in respect of the Parties' respective obligations under the Standard Contractual Clauses, in which case the choice of jurisdiction and governing law set out in the relevant Standard Contractual Clauses shall apply.

13.2 Nothing in this Addendum reduces Company's or any Company Affiliate's, nor Client's or any Client Affiliate's obligations under the Agreement in relation to the protection of Personal Data or permits Company or any Company Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Agreement. In the event of any conflict or inconsistency between the Agreement, this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

13.3 Subject to Section 13.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

13.4 Client or Company may:

13.4.1 by at least 30 (thirty) calendar days' written notice to the other party from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under Section 12.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

13.4.2 propose any other variations to this Addendum which Client or Company reasonably considers to be necessary to address the requirements of any Data Protection Law.

13.5 If Client or Company gives notice under section 13.4.1:

13.5.1 The party that received such notice shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by the

other Party to protect the Client Group Members or Contracted Processors against additional risks associated with the variations made under section 13.4.1.

13.6 If Client or Company give notice under section 13.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in the notice as soon as is reasonably practicable.

13.7 Neither Client nor Company shall require the consent or approval of any Client Affiliate or Company Affiliate to amend this Addendum pursuant to this section 13.5 or otherwise.

13.8 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Agreement with effect from the date first set out above.

_____

Signature _____

Name _____

Title _____

Date Signed _____

Absorb Software Inc.

Signature _____

Name _____

Title _____

Date Signed _____

ANNEX 1: DETAILS OF PROCESSING OF CLIENT PERSONAL DATA

This Annex 1 includes certain details of the Processing of Client Personal Data as required by article 28(3) EU GDPR.

Data Exporter	Name: As set out in the Addendum or Agreement for Client Group Member. Address: As set out in the Addendum or Agreement for Client Group Member. Contact person's name, position and contact details: As set out in Addendum or Agreement for Client Group Member Activities relevant to the data transferred under these Clauses: As set forth in the Agreement Signature and date: Signature of the Addendum shall be deemed signature of Annex I of the Standard Contractual Clauses. Role: Controller
Data Importer	Name: Absorb Software Inc. Address: #2500 – 685 Centre St. S, Calgary Alberta Canada T2G 1S5 Contact person's name, position and contact details: Jean Hernandez Information Security Officer privacyofficer@absorblms.com Activities relevant to the data transferred under these Clauses: As set forth in the Agreement Signature and date: Signature of the Addendum shall be deemed signature of Annex I of the Standard Contractual Clauses. Role: Processor
Categories of data subjects whose personal data is transferred	Personal data transferred may include, but is not limited to: • Users including any prospective, current or former employee, agent, contractor, approved third-party, consultant, or any other User of Client Group Member.
Categories of personal data transferred	The personal data transferred may include, but is not limited to, the following categories of data: • **Name** including first and last names; • **Contact information**, including residential and work mailing addresses and telephone numbers and e-mail addresses, and emergency contact information; • **Personal details** including date of birth; • **Employment information** including hire date; place of executing the

	employment; department of employment; job title; job category; job status and supervisor; **Education and training information:** education, certifications and training.
Sensitive data transferred (if applicable) and applied restrictions or safeguards in respect of special category data	N/A.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).	• one off or multiple data transfer on commencement of Services; • Regular and irregular transfer of Client Personal Data; or • Continuous remote access to Data Exporter systems;
Nature of the processing	As described by the term "Services" as set out in the Agreement including: Provision of the Absorb Learning Management System (LMS)
Purpose(s) of the data transfer and further processing	The nature of the processing may include, but is not limited to, collection, recording, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The purpose of the processing is to provide the Services as set forth in the underlying Services Agreement.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	Data will be retained during the life of an active service agreement; and upon termination destroyed in accordance with Company's retention policies
Competent supervisory authority	The Data Protection Commission (Ireland) or the Information Commissioner's Office (UK) as applicable

ANNEX 2: STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF CLIENT PERSONAL DATA (EU SCCs)

The Parties agree that:

(a) Annex I to these Standard Contractual Clauses shall be as set out in Annex 1 of this Addendum; and

(b) Annex II to these Standard Contractual Clauses shall be as set out in Annex 3 (Technical and Organizational Measures) of this Addendum.

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) 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 (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 (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.

(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

(a) 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);

iii. Clause 9 – Module Two: Clause 9(a), (c), (d) and (e);

iv. Clause 12 –Module Two: Clause 12(a), (d) and (f);

v. Clause 13;

vi. Clause 15.1(c), (d) and (e);

vii. Clause 16(e);

viii. Clause 18: Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to the 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.

Clause 7

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.

(b) Once it has completed the Appendix and signed Annex I 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.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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.

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 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 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**

(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.

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 (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 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 noncompliance. 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.

Clause 9

Use of sub-processors

(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 fifteen (15) business 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. (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) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7. 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.

Clause 10

Data subject rights

(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.

Clause 11

Redress

(a) 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.

(b) 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.

(c) 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.

(d) 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.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) 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

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.

(a) 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.

(b) 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.

(c) 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.

(d) 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.

(e) 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.

(f) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
Supervision

(a) 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 shall act as competent supervisory authority.

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

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 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.

(a) 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;

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.

(b) 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.

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

(d) 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).

(e) 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. 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 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

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

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) 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.

(c) 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.).

(d) 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.

(e) 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.

(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

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 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

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

(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 Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the

(d) Member State in which he/she has his/her habitual residence.

(e) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX 3 TECHNICAL AND SECURITY MEASURES

Company and Company Affiliates have implemented a wide range of technical and organizational measures as follows:

1. Hosting infrastructure: Absorb LMS infrastructure architecture is designed for resilience and high availability, spread over two AWS availability zones (i.e. two physical data centres), enabling a hot/hot data centre strategy.

2. Physical security (data processing facilities excluding data centers): All data processing facilities including office areas are secured with controlled access enforced at all entry points. Access rights as well as access logs are reviewed on a regular basis.

3. Physical security (data centers): Absorb LMS is hosted in AWS and relies on AWS for physical security. AWS has implemented a wide range of controls for physical security which can meet the most stringent requirements in the industry.

4. Roles and responsibilities: Roles and responsibilities for security and privacy are defined and established.

5. Security/privacy/GDPR awareness training: All personnel are required to take the training upon hire and on an annual basis.

6. Policies and procedures. Policies and procedures are in place and reviewed on an annual basis.

7. Access management: Access control rules are enforced at hypervisor, network, system, storage, application, and data layers. Principles for segregation of duties and least privilege are implemented. Users and access permissions are reviewed on a regular basis.

8. Data encryption. Data is encrypted at rest (AES-256) and in transit (TLS 1.2) to ensure data confidentiality and integrity.

9. Data transfer. Where GDPR applies, data transfer to outside EEA is governed by GDPR data transfer rules.

10. Data minimalization. The use of data including data sharing is limited to what is necessary for the specific purposes.

11. Third parties: Process for managing and monitoring third party access including subprocessing has been established. Absorb has data processing addendum in place with all subprocessors.

12. Backup and recovery: Procedures are documented and implemented, and recovery tests are performed on a regular basis.