DATA PROCESSING ADDENDUM

This DATA PROCESSING ADDENDUM is deemed entered into by Learn Amp ("the Supplier") and the Customer upon entry into the Agreement (as defined below).

BACKGROUND

A. This Data Processing Addendum (as defined below) sets out the additional terms, requirements and conditions on which the Supplier will process Personal Data when providing services under the Agreement (as defined below).

B. This Data Processing Addendum contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) for contracts between controllers and processors as well as the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to the General Data Protection Regulation ((EU) 2016/679) and the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (if applicable).

AGREED TERMS

1. DEFINITIONS AND INTERPRETATION

1.1 The following definitions and rules of interpretation apply in this Data Processing Schedule:

Addendum:	the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses;
Agreement:	the software as a service (SaaS) agreement (including the Terms and the Appendices (all as defined in the Agreement) entered into by the Customer and the Supplier;
Business Purposes:	the services to be provided by the Supplier to the Customer as described in the Agreement, this Data Processing Addendum and any other purpose specifically identified in Schedule 1;
Commissioner:	the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018);
Controller:	as defined in the Data Protection Legislation;
Data Processing Schedule:	means this data processing schedule, deemed entered into by the Supplier and the Customer upon entry into the Agreement;

Data Protection Impact Assessment:	means an assessment of the impact of the envisaged Processing operations on the protection of Personal Data, as required by Article 35 of the UK GDPR and EU GDPR;
Data Protection Legislation:	all applicable data protection and privacy legislation in force from time to time including without limitation the EU GDPR; the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (the "**DPA 2018**"); the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the Commissioner or other relevant regulatory authority and which are applicable to a party;
Data Subject:	as defined in the Data Protection Legislation;
EU GDPR:	the General Data Protection Regulation ((EU) 2016/679);
EEA:	the European Economic Area;
ICO:	the Information Commissioner's Office;
Personal Data:	as defined in the Data Protection Legislation;
Personal Data Breach:	as defined in the Data Protection Legislation;
Processing:	as defined in the Data Protection Legislation (and "**Processes**", "**processed**" and "**process**" shall be construed accordingly);
Processor:	as defined in the Data Protection Legislation;
Records:	has the meaning given to it in Clause 12.1;
Restricted Transfer:	a transfer of Personal Data which is covered by Chapter V of the UK GDPR;
Standard Contractual Clauses (SCCs):	the ICO's International Data Transfer Agreement for the transfer of Personal Data from the UK and/or the

	ICO's International Data Transfer Addendum to the EU Commission Standard Contractual Clauses and/or the European Commission's Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 as set out in the Annex to Commission Implementing Decision (EU) 2021/914, as referenced in Schedule 2;
Term:	this Data Processing Schedule's term as defined in Clause 10.1(b); and
UK GDPR:	has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

1.2 This Data Processing Addendum is subject to the terms of the Agreement and is incorporated into the Agreement.

1.3 The Annexes form part of this Data Processing Addendum and will have effect as if set out in full in the body of this Data Processing Schedule. Any reference to this Data Processing Addendum includes the Annexes.

1.4 A reference to writing or written includes email.

1.5 In the case of conflict or ambiguity between:

a) any of the provisions of this Data Processing Addendum and the remaining provisions of the Agreement, the provisions of this Data Processing Addendum will prevail; and

b) any of the provisions of this Data Processing Addendum and any executed SCC, the provisions of the executed SCC will prevail.

2. PERSONAL DATA TYPES AND PROCESSING PURPOSES

2.1 The Customer and the Supplier agree to comply with all applicable requirements of the Data Protection Legislation.

2.2 The Customer and the Supplier agree and acknowledge that for the purpose of the Data Protection Legislation:

d) in relation to Personal Data processed by the Supplier on behalf of the Customer to provide the Services, the Customer is the Controller and the Supplier is the Processor;

d) in relation to certain processing activities where the Supplier determines the purpose and means of processing (as described in the Supplier's Privacy Policy), the Supplier is an independent Controller and shall comply with its own obligations under Data Protection Legislation accordingly;

d) the Customer and where applicable the individual OC shall retain control of the Personal Data (and if an OC for its Personal Data) and remains responsible for its compliance

obligations under the applicable Data Protection Legislation, including but not limited to providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the Supplier; and

d) to the extent not stated elsewhere in this Data Processing Schedule, Schedule 1 *(Data Processing Particulars)* describes the subject matter, duration, nature and purpose of the processing and the Personal Data types and Data Subject types in respect of which the Supplier may process the Personal Data to fulfil the Business Purposes.

3. SUPPLIER'S OBLIGATIONS

3.1 The Supplier will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions or as required by applicable law. The Supplier will not process the Personal Data for any other purpose or in a way that does not comply with this Data Processing Addendum or the Data Protection Legislation, and will notify the Customer immediately if, in the Supplier's opinion, the Customer's instructions are unlawful.

3.2 The Supplier shall comply, as soon as reasonably possible, with any Customer written instructions requiring the Supplier to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.3 The Supplier will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third parties unless the Customer or this Data Processing Addendum specifically authorises the disclosure, or as required by domestic or EU law, court or regulator (including the Commissioner). If a domestic or EU law, court or regulator (including the Commissioner) requires the Supplier to process or disclose the Personal Data to a third party, the Supplier must first inform the Customer of such legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the domestic or EU law prohibits the giving of such notice.

3.4 The Supplier will reasonably assist the Customer with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of the Supplier's processing and the information available to the Supplier, including in relation to Data Subject rights, security of processing, the Data Protection Impact Assessment and reporting to and consulting with the Commissioner, or other relevant regulator under the Data Protection Legislation.

3.5 The Supplier shall, as soon as reasonably possible, notify the Customer of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting the Supplier's performance of the Agreement or this Data Processing Schedule.

4. SUPPLIER'S EMPLOYEES

4.1 The Supplier will ensure that all of its employees :

a) are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;

b) have undertaken training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties;

c) are aware both of the Supplier's duties and their personal duties and obligations under the Data Protection Legislation and this Data Processing Schedule; and

d) will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments.

4.2 The Supplier will take reasonable steps to ensure the reliability, integrity and trustworthiness of all of the Supplier's employees with access to the Personal Data.

5. SECURITY

5.1 The Supplier shall at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in the Supplier's security policy *(https://learnamp.com/security-policy)*.

5.2 The Supplier must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

a) the pseudonymisation and encryption of Personal Data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

d) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6. PERSONAL DATA BREACH

6.1 The Supplier will without undue delay, and in any event within forty-eight (48) hours, notify the Customer if it becomes aware of:

a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data. Where practicable, the Supplier will restore such Personal Data at its own expense as soon as possible;

b) any accidental, unauthorised or unlawful processing of the Personal Data; or

c) any Personal Data Breach.

6.2 Where the Supplier becomes aware of (a), (b) and/or (c) above, it shall, without undue delay, also provide the Customer with the following information:

a) a description of the nature of (a), (b) and/or (c), including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

b) the likely consequences; and

c) a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.

6.3 Immediately following the parties becoming aware of any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, the Supplier and Customer will co-ordinate with each other to investigate the matter, including but not limited to:

a) assisting with any investigation;

b) facilitating interviews with the Supplier's employees, former employees and others involved in the matter including, but not limited to, its officers and directors;

c) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required for an investigation; and

d) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data processing.

6.4 The Supplier will not inform any third party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first notifying the Customer, except when required to do so by domestic or EU law.

6.5 The Supplier agrees that the Customer shall determine:

a) whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and

b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

6.6 The Supplier shall cover all reasonable expenses associated with the performance of the obligations under Clause 6.1 to Clause 6.3 unless the matter arose from the Customer's specific written instructions, negligence, wilful default or breach of this Data Processing Schedule, in which case the Customer shall cover all reasonable expenses.

7. CROSS-BORDER TRANSFERS OF PERSONAL DATA

7.1 The Supplier (and any subcontractor, if applicable) must not transfer or otherwise process the Personal Data outside the UK and/or EEA without obtaining the Customer's prior written consent, consent of which shall be deemed to be given by the Customer in relation to existing subcontractors at the date of this Data Processing Addendum on the execution of the Agreement, as set out in Schedule 1.

7.2 Where such consent is granted, the Supplier may only process, or permit the processing, of the Personal Data outside the UK and/or EEA under the following conditions:

a) the Supplier is processing the Personal Data in a territory which is subject to adequacy regulations under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals; or

b) the Supplier participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that the Supplier (and, where appropriate, the Customer) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the UK GDPR

and EU GDPR, and the Supplier shall immediately inform the Customer of any change to that status; or

c) the transfer otherwise complies with the Data Protection Legislation for the reasons set out in Schedule 1.

7.3 The Customer and the Supplier agree that when the transfer of Personal Data is a Restricted Transfer and applicable Data Protection Legislation requires that appropriate safeguards are put in place, it shall be subject to the appropriate SCCs, as set out in Schedule 2, which shall be deemed incorporated into and form part of this Data Processing Schedule.

7.4 If any Personal Data transfer between the Customer and the Supplier requires execution of SCCs in order to comply with the Data Protection Legislation, the parties will be deemed to have executed the SCCs contained in Schedule 2, and will take all other actions required to legitimise the transfer.

8. SUBCONTRACTORS

8.1 The Supplier may only authorise a third party (subcontractor) to process the Personal Data if:

a) the Customer is provided with an opportunity to object to the appointment of each subcontractor within seven (7) days of the Supplier engaging such subcontractor. In the absence of such objection, the Customer shall be deemed to authorise the engagement of such subcontractor;

b) the Supplier enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this Data Processing Schedule, in particular, in relation to requiring appropriate technical and organisational data security measures, confidentiality, and obligations which provide sufficient guarantees from subcontractors that the Processing meets the requirements of the Data Protection Legislation, and, upon the Customer's written request, provides the Customer with copies of the relevant excerpts from such contracts; and

c) the subcontractor's contract terminates automatically on termination of this Data Processing Addendum for any reason.

8.2 The parties confirm the appointment of the subcontractors referenced in Schedule 1.

9. COMPLAINTS, DATA SUBJECT REQUESTS AND THIRD-PARTY RIGHTS

9.1 The Supplier shall, and the Customer shall cover all reasonable expenses associated with the performance of the Supplier's obligations under this Clause 9.1, take such technical and organisational measures as may be appropriate, and as soon as reasonably possible provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

a) the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify, port and erase Personal Data, object to the processing and automated processing of Personal Data, and restrict the processing of Personal Data; and

b) information or assessment notices served on the Customer by the Commissioner or other relevant regulator under the Data Protection Legislation.

9.2 The Supplier shall notify the Customer without undue delay in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.3 The Supplier shall notify the Customer within two (2) days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

9.4 The Supplier will give the Customer its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 The Supplier must not disclose the Personal Data to any Data Subject or to a third party other than in accordance with the Customer's written instructions, or as required by domestic or EU law.

10. TERM AND TERMINATION

10.1 This Data Processing Addendum will remain in full force and effect so long as:

a) the Agreement remains in effect; or

b) the Supplier retains any of the Personal Data related to the Agreement in its possession or control (the "**Term**").

10.2 Any provision of this Data Processing Addendum that expressly or by implication should come into or continue in force on or after termination of the Agreement in order to protect the Personal Data will remain in full force and effect.

10.3 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Agreement obligations, the parties may agree to suspend the processing of the Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data processing into compliance with the Data Protection Legislation within thirty (30) days, either party may terminate the Agreement on not less than seven (7) days on written notice to the other party.

11. DATA RETURN AND DESTRUCTION

11.1 At the Customer's request, the Supplier will give the Customer, or a third party nominated in writing by the Customer, a copy of or access to all or part of the Personal Data in its possession or control in a format and medium agreed with the Customer.

11.2 On termination of the Agreement for any reason or expiry of its term, the Supplier will securely delete or destroy or, if directed in writing by the Customer at the reasonable expense of the Customer, return and not retain, all or any of the Personal Data related to this Data Processing Addendum in its possession or control, no later than ninety (90) days after the termination or expiry.

11.3 If any law, regulation, or government or regulatory body requires the Supplier to retain any documents or materials or Personal Data that the Supplier would otherwise be required to return or destroy, it will notify the Customer in writing of that retention requirement, giving details of the

documents, materials or Personal Data that it must retain, the legal basis for retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

11.4 The Supplier will certify in writing to the Customer that it has destroyed the Personal Data within fourteen (14) days after it completes the deletion or destruction.

12. RECORDS

12.1 The Supplier will keep detailed, accurate and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, subcontractors (if applicable), the processing purposes, categories of processing, any transfers of Personal Data to a third country and related safeguards, and a general description of the technical and organisational security measures referred to in Clause 5.1 (the "**Records**").

12.2 The Supplier will ensure that the Records are sufficient to enable the Customer to verify the Supplier's compliance with its obligations under this Data Processing Addendum and the Supplier will provide the Customer with copies of the Records as soon as reasonably possible upon written request.

12.3 The Customer and the Supplier must review the information listed in the Annexes to this Data Processing Addendum at least once a year to confirm its current accuracy and update it when required to reflect current practices.

13. AUDIT

13.1 The Supplier will permit the Customer and its third-party representatives to audit the Supplier's compliance with its Agreement obligations, no more than one (1) time per year, on at least thirty (30) days' notice, during the Term. The Supplier will give the Customer and its third-party representatives all reasonable assistance to conduct such audits. The assistance may include, but is not limited to:

a) physical access to, remote electronic access to, and copies of the Records and any other relevant information held at the Supplier's premises or on systems storing the Personal Data; and

b) access to and meetings with any of the Supplier's personnel reasonably necessary to provide all explanations and perform the audit effectively.

13.2 The notice requirements in Clause 13.1 will not apply if the Customer reasonably believes that a Personal Data Breach occurred or is occurring, or the Supplier is in breach of any of its obligations under this Data Processing Addendum or any Data Protection Legislation.

13.3 If a Personal Data Breach occurs or is occurring, or the Supplier becomes aware of a breach of any of its obligations under this Data Processing Addendum or any Data Protection Legislation, the Supplier will:

a) promptly conduct its own audit to determine the cause;

b) produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;

c) provide the Customer with a copy of the written audit report; and

d) remedy any deficiencies identified by the audit within thirty (30) days.

13.4 At least once a year, the Supplier will conduct site audits of its Personal Data processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this Data Processing Schedule, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognised third-party audit firm based on recognised industry best practices.

13.5 On the Customer's written request, as soon as reasonably possible the Supplier will make all of the relevant audit reports available to the Customer for review. The Customer will treat such audit reports as the Supplier's confidential information under the Agreement.

13.6 The Supplier will promptly address any exceptions noted in the audit reports with the development and implementation of a corrective action plan by the Supplier's management.

14. WARRANTIES

14.1 The Supplier warrants and represents that:

a) its employees, subcontractors (if applicable), agents and any other person or persons accessing the Personal Data on its behalf are, to the best of its knowledge, reliable and trustworthy and have received the required training on the Data Protection Legislation;

b) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

c) it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Agreement's contracted services; and

d) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:

i. the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage;

ii. the nature of the Personal Data protected; and

iii. comply with all applicable Data Protection Legislation and its information and security policies, including the security measures in Clause 5.1.

14.2 The Customer will ensure that the Supplier's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.

15. NOTICE

15.1 Any notice given to a party under or in connection with this Data Processing Addendum must be in writing and delivered to:

For the Customer:

the postal address and primary email address supplied in the Order (or any later address the Customer notifies to Learn Amp in writing).

For the Supplier:

Name: Duncan Cheatle

Email address: *compliance@learnamp.com*

Postal address: The Old Rectory, Church Street, Weybridge, Surrey, KT13 8DE

15.2 For the avoidance of doubt, Clause 15.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

SCHEDULE 1 DATA PROCESSING PARTICULARS

Subject matter of the Processing	The Business Purposes.
Duration of Processing	The Subscription Term.
Nature and purpose of the Processing	The Business Purposes.
Location of the Processing	UK and EEA (with main servers in Dublin).
Business Purposes	The services to be provided by the Supplier to the Customer as described in the Agreement, and any other purpose specifically identified in this Schedule 1.
Personal Data types	Full names and HR related data, including details in respect of employment, training, test results and performance management data.
Data Subject types	Employees and contractors of the Customer.
Approved subcontractors	A full and current list of subcontractors is maintained here: https://learnamp.com/gdpr-subprocessors
The Supplier's legal basis for Processing Personal Data outside the EEA, in order to comply with cross-border transfer restrictions	Standard Contractual Clauses and Addendum.

SCHEDULE 2 STANDARD CONTRACTUAL CLAUSES AND ADDENDUM

Standard Contractual Clauses

1.1 The SCCs are incorporated into this Schedule 2 as follows:

1.1.1 For Supplier to Customer transfers, Module 4 (processor to controller transfers) applies;

1.1.2 Clause 7 (docking clause) does not apply;

1.1.3 The optional wording in Clause 11 (redress) does not apply;

1.1.4 The laws of England are the governing laws; and

1.1.5 The courts of England have jurisdiction over any disputes.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): shall be the Supplier as set out in the Agreement

Role (controller/processor): Processor

Activities relevant to the data transferred under these Clauses: sharing personal data to the Customer in the Supplier's performance of Services under this Agreement

Data importer(s): shall be the Customer as set out in the Agreement

Role (controller/processor): Controller

Activities relevant to the data transferred under these Clauses: sharing personal data to the Customer in the Supplier's performance of Services under this Agreement

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- *See Schedule 1 of the Agreement (Data Processing Particulars)*

Categories of personal data transferred

- *See Schedule 1 of the Agreement (Data Processing Particulars)*

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

- *None*

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

- *Continuous*

Nature of the processing

- *See Schedule 1 of the Agreement (Data Processing Particulars)*

Purpose(s) of the data transfer and further processing

- *See Schedule 1 of the Agreement (Data Processing Particulars)*

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

- *The period of time necessary to provide the services under the Agreement and/or in accordance with applicable legal requirements*

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

- *Same as the Processor to the extent such information is provided to subprocessors for purposes of providing the services under the Agreement*

ADDENDUM

INTERNATIONAL DATA TRANSFER ADDENDUM TO THE EU COMMISSION STANDARD CONTRACTUAL CLAUSES

PART 1: TABLES

Table 1: Parties

Start date	Contract Effective Date	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	The Supplier as set out in the Agreement	The Customer as set out in the Agreement
Key Contact	Please see clause 15.1 of the Agreement	The postal address and primary email address supplied in the Order (or any later address the Customer notifies to Learn Amp in writing).
Signature (if required for the purposes of Section 2)	_____	_____

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:					
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?
4	Yes	Yes	No			Yes

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: Has the meaning given in Table 1.
Annex 1B: Description of Transfer: The transfer of personal data relating to customers, please see the Exporter's privacy policy at *https://learnamp.com/privacy-policy*
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Please see the Exporter's GDPR compliance at *https://learnamp.com/gdpr* and security policy at *https://learnamp.com/security-policy*
Annex III: List of Sub processors (Modules 2 and 3 only): N/A

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

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.