Fuse Data Processing Addendum

Last updated: 9 August 2024

1. Data Processing Agreement preamble

1.1. This Data Processing Agreement ("**DPA**") is entered into between Fuse Universal Ltd ("**Data Processor**") and the Customer ("**Data Controller**") (together the "**Parties**") and sets out the rights and obligations that apply to the Data Processor's handling of Personal Data on behalf of the Data Controller. **"Personal Data**" shall mean personal data as defined by the Applicable Data Protection Laws.

1.2. This DPA is incorporated by reference into the Master Customer Agreement dated between the Parties ("**Agreement**") for the supply of Services by the Data Processor to the Data Controller.

1.3. This DPA has been designed to ensure the Parties' compliance with Applicable Data Protection Laws. "**Applicable Data Protection Laws**" shall mean all applicable federal, state and foreign data protection, privacy and data security laws, regulations, and directives, including, without limitation, the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**"), the UK Data Protection Act 2018 ("**UK GDPR**"); the Australian Privacy Act 1988 (Cth) ("**Australian Privacy Laws**") and the California Consumer Privacy Act of 2018 ("**CCPA**").

1.4. The terms used in this DPA shall have the meanings set forth in this DPA. Capitalised 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.

1.5. This DPA shall not exempt the Parties from their respective obligations under Applicable Data Protection Laws.

Now therefore, in consideration of the mutual promises herein and other good and valuable consideration, the Parties to this DPA agree as follows:

2. Australian Privacy Laws

2.1. The Customer has been provided with this DPA because its instance of the Fuse Platform will be hosted in Australia. To the extent that the Australian Privacy Laws will apply, the following definitions shall be interchangeable:

2.1.1 "Personal Data" includes "Personal Information"; and
2.1.2 "Sensitive Data" includes "Sensitive Information";

both as defined under Applicable Data Protection Laws.

2.2. Article 28 of the UK GDPR (which the Data Processor must already comply with due to its cross-border effect) contains the most onerous written, technical and security standards for Data Processors globally and therefore the rights and obligations set out from Clause 3 onwards shall remain applicable for both parties for the duration of the Agreement.

2.3. The Data Processor certifies that it understands it will comply with the responsibilities and restrictions imposed by this DPA as a processor of personal information under Australian Privacy Laws.

3. The rights and obligations of the Data Controller and processing of Personal Data

3.1. The Data Controller appoints the Data Processor to process the Personal Data described in Appendix A.

3.2. The details on the subject matter, duration, nature and purpose of processing and the Personal Data categories and data subject types in respect of which will be subjected to processing by the Data Processor in the performance of the Services pursuant to the Agreement are specified in Appendix A.
3.3. The Data Controller shall have both the right and obligation to make decisions about the purposes and means of the processing of Personal Data and shall be responsible for ensuring that the processing that the Data Processor is instructed to perform is authorised by law.

4. Obligations of the Data Processor

4.1. The Data Processor shall solely be permitted to process Personal Data on documented instructions from the Data Controller to the extent necessary to perform its obligations under the Agreement, unless processing is required under UK, EU or Member State law to which the Data Processor is subject. In this case, and where possible to do so, the Data Processor shall inform the Data Controller of this legal requirement prior to processing unless that law prohibits disclosure of such information on important grounds of public interest.
4.2. The Data Processor shall inform the Data Controller as soon as reasonably possible if the instructions, in the opinion of the Data Processor, contravene the Applicable Data Protection Laws.

5. Confidentiality

5.1. The Data Processor shall reasonably ensure that:

a) only those persons who are currently authorised to do so are able to access the Personal Data being processed on behalf of the Data Controller;
b) only persons who require access to the Personal Data in order to fulfil the obligations of the Data Processor to the Data Controller shall be provided with authorisation; and
c) that persons authorised to process Personal Data on behalf of the Data Controller have undertaken to observe confidentiality or are subject to a duty of confidentiality which offers a degree of protection which is at least equivalent to that offered under the Agreement.

6. Security of processing

6.1. The Data Processor shall implement appropriate technical and organisational measures to protect the Personal Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Personal Data ("**Safeguards**").
6.2. Safeguards shall, taking into account the state of the art and the costs of the implementation and execution of the measures, ensure an adequate level of protection taking into account the risks involved in the processing and the nature of the Personal Data to be secured.
6.3. The Data Processor shall, in ensuring the above – in all cases –implement the level of security and the measures specified in Appendix C to this DPA.
6.4. Where the Parties agree on the requirement of establishing additional security measures, the terms and cost of implementing such measures shall be dealt with in the Agreement.

7. Use of Sub-Processors

7.1. The Data Processor shall not engage a third-party processor ("**Sub-Processor**") for the fulfilment of this DPA without the prior consent of the Data Controller.
7.2. A list of approved Sub-Processors as at the date of this DPA is listed in Appendix B to this DPA and the Data Processor shall maintain and provide updated copies of this list to the Data Controller when it adds or removes Sub-Processors in accordance with this Agreement.
7.3. Notwithstanding the above, the Data Controller consents to the Data Processor engaging Sub-Processors to process the Personal Data, provided that:

a) the Data Processor shall inform the Data Controller of any planned changes with regard to additions to or replacement of Sub-processors (including details of the processing it performs or will perform) as listed in Appendix B to this DPA; and
b) the Data Processor shall ensure that the Sub-Processor is subject to the same data protection obligations as those specified in this DPA on the basis of a contract or other legal document under the Applicable Data Protection Laws .

7.4. If the Sub-Processor does not fulfil its data protection obligations, the Data Processor shall remain liable to the Data Controller as regards the fulfilment of the obligations of the Sub-Processor.

8. Transfer of data to third countries or international organisations

8.1. Without the approval of the Data Controller, the Data Processor cannot – within the framework of this Data Processing Agreement:

a) disclose Personal Data to a data controller in a third country or in an international organisation;
b) assign the processing of Personal Data to a sub-processor in a third country; or
c) have the data processed in another of the Data Processor's divisions which is located in a third country,

unless otherwise specified within this DPA.

8.2. The Data Controller's instructions or approval of the transfer of Personal Data to a third country, if applicable, shall be set out in Appendix A to this Data Processing Agreement.

8.3. The Data Processor may only process, or permit the processing, of Personal Data outside the UK or European Economic Area ("**EEA**") under the following conditions:

(a) Data Processor 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. Data Processor must identify in Appendix A the territory that is subject to such adequacy regulations; or
(b) Supplier participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that 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 the Data Protection Legislation. Supplier must identify in Appendix A the transfer mechanism that enables the parties to comply with these cross-border data transfer provisions and Supplier must 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 Appendix A.

8.4 If any Personal Data transfer between the Data Controller and Data Processor requires execution of Addendum in order to comply with the Data Protection Legislation (where the Customer is the entity exporting Personal Data to Supplier outside the UK and EEA), the parties will complete all relevant details in, and execute, the Addendum contained in Appendix D, and take all other actions required to legitimise the transfer.

8.5 If the Customer consents to appointment by Data Processor of a subcontractor located outside the UK or EEA in compliance with the provisions of clause 8, then the Data Controller authorises Data Processor to enter into the Addendum contained in Appendix B with the subcontractor in the Data Controller's name and on its behalf.

9. Assistance to the Data Controller and Data Subject Rights

9.1. The Data Processor shall, as far as reasonably possible, assist the Data Controller in the fulfilment of the Data Controller's obligations to respond to requests for the exercise of the data subjects' rights including with: the right of access by the data subject, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and the right to object to the result of automated individual decision-making, including profiling ("**Data Subject Request**").
9.2. Taking into account the nature of the processing, the Data Processor shall provide reasonable assistance at the Data Controller's expense, to the Data Controller by providing appropriate technical and organizational measures, insofar as this is reasonably possible, for the fulfilment of Data Controller's obligation to address any Data Subject Request.

10. Notification of Personal Data breach

10.1. On discovery of a Personal Data breach at the Data Processor's facilities or a Sub-Processor's facilities ("**Security Incident**"), the Data Processor shall as soon as reasonably practicable notify the Data Controller.
10.2. The Data Processor's notification to the Data Controller shall, if possible, take place within forty-eight (48) hours after the Data Processor has discovered the breach to enable the Data Controller to comply with its data breach reporting obligations under (and in accordance with the timescales required by) the Applicable Data Protection Laws.
10.3. The Data Processor shall provide reasonable assistance to the Data Controller in the reporting of the breach to the relevant supervisory authority.

11. Erasure of data

11.1. On termination of the Agreement, the Data Processor shall, at the Data Controller's discretion, return all the Personal Data to the Data Controller and erase existing copies, except to the extent that the Applicable Data Protection Laws require storage of the Personal Data.

12. Inspection and audit

12.1. The Data Processor shall make available to the Data Controller all information reasonably necessary to allow for and contribute to audits, including inspections performed by the Data Controller or another third party auditor mandated by the Data Controller, at the Data Controller's expense, provided that the Data Controller: (i) gives the Data Processor reasonable prior notice of its intention to audit; (ii) conducts its audit during normal business hours; and (iii) takes all reasonable measures to prevent unnecessary disruption to the Data Processor's operations.
12.2. The Data Controller will not exercise its audit rights under this clause 11 more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent data protection authority, or (ii) where the Data Controller believes a further audit is necessary due to a Security Incident by the Data Processor.
12.3. The Data Controller's inspection of sub-processors, if applicable, shall be performed through the Data Processor.

13. Applicability of the CCPA

13.1. To the extent that the Data Processor will process any Personal Data that is subject to the CCPA, the Data Processor shall act as a "service provider," as such term is defined in the CCPA, and shall assist the Data Controller by appropriate technical and organizational measures for the fulfilment of the Data Controller's obligations under the CCPA, including without limitation responding to verified requests by a "consumer," as such term is defined in the CCPA.
13.2. Furthermore, the Data Processor will not engage a Sub-Processor with access to Personal Data except with the Data Controller's prior written consent in accordance with Clause 6 of this DPA and the Data Processor will only do so for a "business purpose," as such term is defined in the CCPA, pursuant to a written contract by and between the Data Processor and such Sub-Processor. Any such approved Sub-Processor shall agree to terms that are at least as protective of Personal Data as the terms of this DPA.
13.3. The Data Processor certifies that it understands it will comply with the responsibilities and restrictions imposed by this DPA as a service provider under the CCPA.

14. The Parties' agreement on other terms

14.1. The consequences of the Parties' breach of this DPA shall be addressed in accordance with the terms of the Agreement.
14.2. In the event of a conflict between this DPA and the data protection provisions within the Agreement (except where explicitly agreed otherwise in writing between the Parties), the terms and conditions set forth in this DPA shall prevail and govern the relationship between the Parties.

15. Commencement and termination

15.1. This DPA shall become effective on the date of both Parties' signature of the Agreement.

15.2. This DPA may be terminated on the basis of the terms specified in the Agreement.
15.3. This DPA shall apply for as long as the processing is performed. Irrespective of the termination of the Agreement and/or this DPA, the DPA shall remain in force until the termination of the processing and the erasure of the data by the Data Processor and any Sub-Processors.
15.4. The DPA and the Agreement shall be interdependent and cannot be terminated separately. The DPA may however – without termination of the Agreement – be replaced by an alternative valid data processing agreement.

16. Governing Law and Jurisdiction

16.1. The Parties to this DPA shall submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity.
16.2. The DPA and all non-contractual or other obligations arising of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

17. Severance

17.1. Should any of the provisions of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, 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 has never been contained therein.

18. Data Processor and Data Controller contacts

18.1. In the event your designated account manager at Fuse cannot assist with a data privacy enquiry, you may contact Fuse's data protection officer at dpo@fuseuniversal.com.

18.2. The Parties shall be under obligation continuously to inform each other of changes to contacts/contact

Please sign and return the enclosed copy of this Addendum as instructed to acknowledge the supplementation of these terms to the Agreement.

[Signatures follow on the next page]

CUSTOMER

Customer name (Required): _____

Signature (Required): _____

Name (Required) : _____

Title (Optional) : _____

Date (Required): _____

EU Representative (Required only where applicable): _____

Contact details: _____

Data Protection Officer (Required only where applicable): _____

Contact details: _____

FUSE

Notwithstanding the signatures below of any other Fuse Entity, a Fuse Entity is not a party to this Addendum unless they are a party to the Agreement for the provision of the Software and/or Services to you.

Data Protection Point of Contact: John Taylor
Contact Details: john.taylor@fuseuniversal.com

Fuse Universal Limited:

Signature: _____

Name: _____

Title: _____

Date: _____

Fuse Universal Pty Limited:

Signature:_____

Name: _____

Title: _____

Date: _____

Appendix A Information about the processing

The purpose of the Data Processor's processing of Personal Data on behalf of the Data Controller is:

- The purpose of data processing is to provide learning and training functionality for the Data Controller's users.

The Data Processor's processing of Personal Data on behalf of the Data Controller shall mainly pertain to (the nature of the processing):

- The Data Processor maintains and runs the Fuse service that stores and processes user and learning data.

Processing includes the following categories of data subject:

- Data Controller's employees, contractors.

The Processing concerns the following categories of data:

- Data Controller's employees' data.

The processing includes the following types of Personal Data about data subjects:

The only mandatory user data requirement for Fuse is a unique username for each user on the customer's instance. All other data is optional and defined by the Data Controller. This is typically generic business personal data. For example:

- Personal Data such as:
    - first name/last name
    - username (unique)
    - email address (unique)
    - custom fields such as: location, department, role, hire date, line manager, etc.

In addition, the Data Controller collects the following Personal Data:
Technical data such as:

- IP address
- browser language
- browser type and version
- geolocation
- operating system
- third-party cookie information (where we use third-party services to provide Fuse functionality)

- Fuse activity:
    - login history and transactional activity information (views, likes, shares etc.)
    - training history and learning completions
    - error logs
    - metadata for user-generated content such document uploads and video recordings

The Data Processor's processing of Personal Data on behalf of the Data Controller may be performed when this DPA commences. Processing has the following duration:

- Processing and storage of user data for the term of the Agreement and for the period of sixty (60) days thereafter at which point the Personal Data is destroyed in line with Data Processor's service termination process.

Identify Supplier's legal basis for processing Personal Data outside the UK or EEA in order to comply with cross-border transfer restrictions (select one):

- Located in a country with a current determination of adequacy (list country):

  _____.

- Binding Corporate Rules.
- Standard Contractual Clauses between Customer as "data exporter" and Supplier as "data importer".
- Standard Contractual Clauses between Supplier as "data exporter" on behalf of Customer and Supplier affiliate or subcontractor as "data importer".
- Other (describe in detail)

_____.

Appendix B Terms of the Data Processor's use of Sub-Processors and list of approved Sub-Processors

B.1 Approved sub-processors

1. Supplier may engage other processors ("**Sub-Processors**") for the Processing of Personal Data under this Data Processing Agreement, provided Supplier ensures such Sub-Processors' compliance with the terms of this Agreement. As of the effective date of the Agreement, the Supplier relies on the Sub-Processors listed in the Order as well as below to provide the Services.

2. Prior to the engagement of another Sub-Processor, the Supplier shall inform your administrator and your contact of the intended Sub-Processing at least thirty (30) days prior thereto, thereby giving you the opportunity to object to such change on reasonable grounds, as set forth in Article 28 of the EU GDPR.

3. You authorize the Supplier to transfer Personal Data to the Supplier's Affiliates and/or other Sub-Processors located in locations outside the UK or European Economic Area, as is reasonably required to provide support, perform technical projects or perform other types of services under the Fuse Master Customer Agreement, provided that, to the extent applicable, either: (i) such locations are recognized by the European Commission as providing adequate data protection; (ii) the Supplier has executed on your behalf the EU Standard Contractual Clauses with such Affiliates and/or other Sub-Processors (you hereby grant such proxy to the Supplier); or (iii) upon your request, you execute the EU Standard Contractual Clauses directly with such Affiliates and/or other Sub-Processors.

4. The Supplier shall remain fully liable to you for the performance of its Sub-Processors' obligations hereunder.

Name	Address	Description of Processing	Legal Basis for Processing
Airbrake USA	228 Hamilton Ave, 3rd Floor Palo Alto, CA 94301	Application exception logging and tracking - Processes in EU & US	Transfers will be based on the adoption of the Standard Contractual Clauses (SCCs), as approved under the Commission Implementing Decision (EU) 2021/914, together with the UK Addendum to the SCCs (as applicable) as approved by the Information Commissioner's Office in the UK and following a

			step-by-step implementation of the 01/2020 Recommendations of the EDPB on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
Amazon Web Services APAC	Level 37, 2-26 Park Street, Sydney, NSW, 2000, Australia	Hosting and Processing Services - processed in AWS Asia Pacific (Sydney)	Processed in APAC
Amazon Web Services EU	One Burlington Plaza, Burlington Rd, Dublin 4	Processing services- processed in EU West (Dublin, Ireland)	Processed in EU
Atlassisian	Level 6 341 George Street Sydney, NSW 2000 Australia	Hosted Support and Delivery platform- processed in EU West (Dublin, Ireland)	Transfers will be based on the adoption of the Standard Contractual Clauses (SCCs), as approved under the Commission Implementing Decision (EU) 2021/914, together with the UK Addendum to the SCCs (as applicable) as approved by the Information Commissioner's Office in the UK and following a step-by-step implementation of the 01/2020 Recommendations of the EDPB on measures that supplement transfer tools to ensure compliance with the EU level of

			protection of personal data.
DataDog	New York Times Bldg, 620 8th Ave 45th Floor New York USA	Logging and Application Performance Monitoring - anonymised data processed in EU & US	Transfers will be based on the adoption of the Standard Contractual Clauses (SCCs), as approved under the Commission Implementing Decision (EU) 2021/914, together with the UK Addendum to the SCCs (as applicable) as approved by the Information Commissioner's Office in the UK and following a step-by-step implementation of the 01/2020 Recommendations of the EDPB on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
Fastly	475 Brannan St. #300 San Francisco, CA 94107	Content Delivery Network – Processes worldwide (Closest POP to connecting users)	Transfers will be based on the adoption of the Standard Contractual Clauses (SCCs), as approved under the Commission Implementing Decision (EU) 2021/914, together with the UK Addendum to the SCCs (as applicable) as approved by the Information

			Commissioner's Office in the UK and following a step-by-step implementation of the 01/2020 Recommendations of the EDPB on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
Fuse Universal SA (Pty) Ltd	12 Pinewood Rd, Newlands, Cape Town, 7700	Fuse Subsidiary providing customer support services – processes in South Africa	Transfers will be based on the adoption of the Standard Contractual Clauses (SCCs), as approved under the Commission Implementing Decision (EU) 2021/914, together with the UK Addendum to the SCCs (as applicable) as approved by the Information Commissioner's Office in the UK and following a step-by-step implementation of the 01/2020 Recommendations of the EDPB on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
Good Data	San Francisco 1 Post Street, Suite 400. San Francisco, CA	System Analytics – processed in Rackspace, London	Transfers will be based on the adoption of the Standard

	94104 USA		Contractual Clauses (SCCs), as approved under the Commission Implementing Decision (EU) 2021/914, together with the UK Addendum to the SCCs (as applicable) as approved by the Information Commissioner's Office in the UK and following a step-by-step implementation of the 01/2020 Recommendations of the EDPB on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
Google	1600 Amphitheatre Parkway in Mountain View, California, United States	GStatic Fonts - Processes in EU and US	Transfers will be based on the adoption of the Standard Contractual Clauses (SCCs), as approved under the Commission Implementing Decision (EU) 2021/914, together with the UK Addendum to the SCCs (as applicable) as approved by the Information Commissioner's Office in the UK and following a step-by-step implementation of the 01/2020 Recommendations of the EDPB on

			measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
Twilio (Sendgrid)	375 Beale St suite 300 San, Francisco CA 94105 USA	SMTP Relay email notifications - processed EU & US SMS notification relay - processed EU & US	Transfers will be based on the adoption of the Standard Contractual Clauses (SCCs), as approved under the Commission Implementing Decision (EU) 2021/914, together with the UK Addendum to the SCCs (as applicable) as approved by the Information Commissioner's Office in the UK and following a step-by-step implementation of the 01/2020 Recommendations of the EDPB on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
UserPilot	1401 Lavaca Street Unit #7019 Austin, TX 78701	In-app analytics for product improvement and innovation	N/A (Hosted on AWS within E/U)
StackOne **(Optional)**	Camburgh House, 27 New Dover Road, Canterbury, Kent, CT1 3DN, United Kingdom	IPAAS platform for Fuse connectors (3rd party integrations) - if used	N/A (Hosted and processed within EU on AWS EU)

Appendix C Instruction pertaining to the use of Personal Data

C.1 The subject of/instruction for the processing

The Data Processor's processing of Personal Data on behalf of the Data Controller shall be carried out by the Data Processor performing the following:
The purpose of data processing is to provide learning and training functionality for the Data Controller's users as described in the Agreement.

C.2 Security of processing

The level of security shall reflect the following:
The Data Processor shall implement the following measures that have been agreed with the Data Controller (on the basis of the risk assessment that the Data Controller has performed):

- Provide mechanisms for the Data Controller to manage and pseudonymise its user data.
- Control unauthorised access to Personal Data and content in line with Data Processor's access control and privacy policies.
- Ensure availability of the platform in line with Data Processor's SLA.
- Provide the level of service, security, auditing and disaster recovery as outlined in Data Processor's ISO27001 policies.

C.3 Storage period/erasure procedures

In line with the Data Processor's service termination process, the Data Processor will destroy all data and content belonging to the Data Controller within the agreed mutually grace period.

C.4 Processing location

Processing of the Personal Data under this DPA cannot be performed at other locations than the following without the Data Controller's prior written consent:

- The Data Controller user data is held, stored and processed in ***the locations stated in Appendix B.***

C.5 Instruction for or approval of the transfer of Personal Data to third countries

- The Data Controller provides instructions and consent pertaining to the transfer of Personal Data to a third country, the Data Processor shall be entitled within the framework of this DPA to perform such transfer.

Appendix D - Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

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

Part 1: Tables

Table 1: Parties

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or ☐ 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?
1						
2	x	N/A	N/A	General	14 days	
3						
4						

Table 3: Appendix Information

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

Annex 1A: List of Parties:

Annex 1B: Description of Transfer:

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

Annex III: List of Sub processors (Modules 2 and 3 only):

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 0: ☐ Importer ☐ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

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

Interpretation of this Addendum

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

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.

Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 0.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or

specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 0 will prevail.

Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections 0 to 0 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

Unless the Parties have agreed alternative amendments which meet the requirements of Section 0, the provisions of Section 0 will apply.

No amendments to the Approved EU SCCs other than to meet the requirements of Section 0 may be made.

The following amendments to the Addendum EU SCCs (for the purpose of Section 0) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

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

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

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

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

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

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

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

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

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

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

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

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

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

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

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

m. Clause 17 is replaced with:

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

n. Clause 18 is replaced with:

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

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

Amendments to this Addendum

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

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

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

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
b. reflects changes to UK Data Protection Laws;

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

If the ICO issues a revised Approved Addendum under Section 0, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

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

b its risk under the Addendum,

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

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

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act

	2018 on 2 February 2022, as it is revised under Section 0 of those Mandatory Clauses.