Data Processing Addendum

This Data Processing Addendum ("Addendum") supplements the VelocityEHS Master Subscription & Services Agreement (the "Agreement") entered into by and between VelocityEHS Holdings, Inc. ("**Company**") and the entity indicated on the applicable Customer Order Form (defined below as "**Customer**"). Any terms not defined in this Addendum shall have the meaning set forth in the Agreement.

1. Definitions

1.1 "Affiliate" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

1.2 "Applicable Laws" means any applicable laws, rules, and regulations in any relevant jurisdiction applicable to the Addendum, the Agreement, or the use or Processing of Personal Data, including those concerning privacy, data protection, confidentiality, information security, availability and integrity, or the handling of Personal Data. Applicable Laws expressly include, as applicable: (i) the General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR" or "GDPR"), (ii) the Swiss Federal Act on Data Protection, (iii) the EU GDPR as it forms part of the law of England and Wales by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (the "UK GDPR"); (iv) the UK Data Protection Act 2018; (v) the Privacy and Electronic Communications (EC Directive) Regulations 2003; and (vi) the California Consumer Privacy Act ("CCPA"), in each case, as updated, amended or replaced from time to time.

1.3 "Authorized Employee" means an employee of either Party or an employee of a Party's Affiliate who has a need to know or otherwise access Personal Data in order to enable a Party to perform its obligations under this Addendum or the Agreement and who has been apprised of the confidential nature of Personal Data before they may access such data and who has undergone appropriate background screening and training.

1.4 "Data Controller" means the Customer which alone determines the purposes and means of the Processing of Personal Data.

1.5 "Data Processor" means the Company which Processes Personal Data on behalf of and pursuant to the instructions of Customer.

1.6 "Data Subject Rights" means the rights recognized and granted to Data Subjects with respect to their Personal Data under Applicable Laws, including, when effective, the GDPR.

1.7 "EU SCCs" means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of Personal Data to countries not otherwise recognized as offering an adequate level of protection for Personal Data by the European Commission; available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (as amended and updated from time to time).

1.8 "ex-EEA Transfer" means the transfer of Personal Data, which is Processed in accordance with the GDPR, outside the European Economic Area (the "EEA"), and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

1.9 "ex-UK Transfer" means the transfer of Personal Data, which is Processed in accordance with the UK GDPR and the Data Protection Act 2018, outside the United Kingdom (the "UK"), and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018.

1.10 "Personal Data" means any information relating to an identified or identifiable living individual that is processed by either Party as a result of, or in connection with, the provision of the Services under the Agreement. An identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

1.11 "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

1.12 "Services" shall have the meaning set forth in the Agreement.

1.13 "Standard Contractual Clauses" means the EU SCCs and the UK Data Transfer Addendum.

1.14 "Suspected Security Incident" means an interruption in either Party's or any Authorized Subcontractor's systems, backups, networks, servers, databases, computers, or other hardware or technical infrastructure, whether or not connected to the Internet, whereby a Security Incident is reasonably suspected.

1.15 "UK Data Transfer Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses Version B1.0, in force 21 March 2022 issued by the UK Information Commissioner under S119A(1) Data Protection Act 2018, available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

2. Processing of Data

2.1 The Parties shall comply with this Addendum at all times during the term of the Agreement. Any failure by either party to comply with the obligations set forth in this Addendum, or any Personal Data Breach, will be considered a material breach of the Agreement, and the other party will have the right, without limiting any of the rights or remedies under this Addendum or the Agreement, or at law or in equity, to immediately terminate the Agreement for cause.

2.2 The rights and obligations of Company with respect to Processing are described herein and in the Agreement. The subject matter, nature, purpose, and duration of this Processing, as well as the types of Personal Data collected and categories of Data Subjects involved, are described in Exhibit 1 to this Addendum.

2.3 Company shall only Process Personal Data for the limited and specified purposes described in Exhibit 1, the terms and conditions set forth in this Addendum and in any Instructions, which shall include Company's rights and obligations regarding onward transfer.

2.4 Company represents and warrant that its Processing of Personal Data does and will comply with Applicable Laws, including with respect to any transmission, transfer, sharing, or otherwise disclosure of Personal Data.

2.5 Company acknowledges and confirms that it does not receive any personal information from Customer as consideration for any services or other items provided to Customer. Except as expressly set forth in the Agreement, Company shall not have, derive or exercise any rights or benefits regarding data provided by Customer ("Consumer Data") and Company shall not sell any Consumer Data. Company shall not retain, use or disclose any Consumer Data except as necessary for the specific purpose of performing the services for Customer pursuant to the Agreement. Company certifies, represents, and warrants that it understands the rules, restrictions, requirements and definitions of the CCPA and agrees to refrain from taking any action that would cause any transfers of Consumer Data to or from Company to qualify as a sale of personal information under the CCPA. The terms "personal information," "sale," and "sell" for the purposes of this Section 2.5 are as defined in Section 1798.140 of the CCPA.

3. Security of Personal Data.

3.1 At a minimum, and without limiting the foregoing, Company represents and warrants that it shall maintain all Personal Data in strict confidence and provide a level of security appropriate to the particular risks of accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure or access of Personal Data presented by the processing and the Personal Data (collectively, "**Risks**"), including (i) limiting access to Personal Data to Authorized Persons only; (ii) ensuring that all Authorized Persons are made aware of the confidential nature of Personal Data before they may access such data; (iii) securing its physical, technical, and administrative infrastructure, including all relevant business facilities, data centers, paper files, servers, networks, platforms, databases, cloud computing resources, back-up systems, passwords and credentials, hardware, and mobile devices; (iv) implementing authentication and access controls within all relevant media, applications, networks, operating systems and equipment; (v) encrypting Personal Data when transmitted over public or wireless networks or where otherwise appropriate in light of the Risks; (vi) strictly segregating Personal Data from information of Company or its employees or other customers; (vii) maintaining appropriate personnel security and integrity procedures and practices, as set forth in Section 3; (viii) maintaining written plans and policies for responding to Suspected Incidents and Personal Data Breaches; (ix) maintaining and regularly testing processes for restoring the availability and access to Personal Data in a timely manner in the event of a Personal Data Breach or Suspected Incident; (x) regularly testing, assessing, and evaluating the effectiveness of its technical and organizational security measures; and (xi) any other measures necessary to ensure the ongoing confidentiality, integrity, and availability of Personal Data and the ongoing security and resilience of systems and services used for processing.

3.2 Upon Customer's written request, or, upon the termination or expiration of the Agreement for any reason, Company shall, and shall ensure that all Authorized Persons, promptly and securely dispose of or return to Customer in an encrypted format, at Customer's choice, all copies of Personal Data.

3.3 Where and to the extent disposal of Personal Data in accordance with Section 3.2 is explicitly prevented by Applicable Law(s) or technically infeasible, Company and/or Authorized Persons, as applicable, shall (i) take measures to block such Personal Data from any further Processing (except to the extent necessary for continued Processing explicitly required by Applicable Law(s)), and (ii) continue to exercise appropriate Technical and Organizational Security Measures to protect such Personal Data until it may be disposed of in accordance with Section 3.2.

4. Authorized Persons

4.1 Customer acknowledges and agrees that Company may engage the Authorized Subcontractors listed in Exhibit 2(D) to this Addendum to access and process Personal Data in connection with the Services. Company represents, warrants, and covenants that it has not and will not permit any other third party other than Company and its Authorized Employees to Process Personal Data on behalf of Company in its provision of Services to Customer without the prior written consent of Customer. Only upon such prior written consent shall any such third party be considered an Authorized Subcontractor. Company shall submit the request for Customer's prior written authorization at least ten (10) days prior to the engagement of any such third party, together with any information necessary to enable Customer to decide on such authorization. Company shall promptly send Customer a copy of any Authorized Subcontractor agreement relevant to this Addendum.

4.2 Company represents, warrants, and covenants that it has executed written agreements with each Authorized Subcontractor that bind them to all obligations set forth in this Addendum with respect to the Processing of the Personal Data.

4.3 Company shall be responsible for the acts and omissions of Authorized Subcontractors and any other of its subcontractors, independent contractors, and other service providers to the same extent that Company would itself be liable under this Addendum had it conducted such acts or omissions.

5. Suspected Security Incident, Security Incident, and Personal Data Breach Notification

5.1 Company shall notify Customer of a Suspected Security Incident as soon as reasonably practicable, but in any event, not more than forty-eight (48) hours after becoming aware of such Suspected Security Incident. If such Suspected Security Incident becomes a Security Incident or a Personal Data Breach, Company shall notify Customer pursuant to Section 5.2.

5.2 Company shall notify Customer as soon as reasonably practicable, but in any event, not more than forty-eight (48) hours after becoming aware of a Security Incident or a Personal Data Breach and shall, in a written report, provide sufficient information to enable Customer to comply with its obligations under Applicable Laws with respect to such Security Incident or Personal Data Breach, including any obligation to report or notify such Security Incident or Personal Data Breach to Supervisory Authorities and/or Data Subjects, as applicable.

5.3 As soon as reasonably practicable after providing the report described in Section 5.2, Company shall provide Customer with a report on its initial findings regarding the Security Incident or Personal Data Breach, and thereafter shall provide regular updates describing subsequent findings with respect to such Security Incident or Personal Data Breach. As soon as reasonably practicable after Company has concluded its examination of the Security Incident or Personal Data Breach, it shall provide Customer with a comprehensive final report regarding the Security Incident or Personal Data Breach.

5.4 Company and/or any relevant Authorized Subcontractor shall use its best efforts to immediately mitigate and remedy any Security Incident or Personal Data Breach and prevent any further Personal Data Breach or recurrence thereof, at Company's own expense and in accordance with Applicable Laws.

5.5 Company nor any Authorized Subcontractor shall publicly disclose any information regarding any Suspected Security Incident, Security Incident or Personal Data Breach without Customer's prior written consent, except that Company and any relevant Authorized Subcontractor may disclose any Suspected Security Incident, Security Incident or Personal Data Breach to (i) its own employees, customers, advisors, agents, or contractors, or (ii) where and to the extent explicitly compelled to do so by Applicable Laws, to applicable Supervisory Authorities and/or Data Subjects without Customer's prior written consent. Such consent will not be unreasonably withheld.

5.6 Company and any relevant Authorized Subcontractor shall, at Customer's expense, fully cooperate with Customer and provide any assistance necessary for Customer to comply with any obligations under Applicable Laws with respect to a Security Incident or Personal Data Breach, including obligations to report or notify a Security Incident or Personal Data Breach to Supervisory Authorities and/or Data Subjects. Such assistance may include drafting disclosures, press releases and/or other communications for Customer with respect to such Security Incident or Personal Data Breach.

6. Transfers of Personal Data

6.1 If Company transfers Personal Data protected under this Addendum to a jurisdiction for which the European Commission has not issued an adequacy decision (each, a "Restricted Transfer"), Company represents, warrants, and covenants that (i) Restricted Transfer by Company may only be made to Authorized Persons as approved by Customer in accordance with Section 4 of this Addendum; (ii) any Restricted Transfer conducted by Company or any Authorized Person shall be undertaken in accordance with the appropriate Standard Contractual Clauses entered into in accordance with Applicable Law; and (iii) that each Restricted Transfer will be made after appropriate safeguards have been implemented for the Restricted Transfer of Personal Data in accordance with Applicable Laws.

6.2 Ex-EEA Transfers. Ex-EEA Transfers are made pursuant to the EU SCCs, which are deemed entered into and incorporated into this Addendum by reference. For the purposes of the EU SCCs, the appropriate module shall be Module Two (Controller to Processor), with the following options:

A. The optional docking clause in Clause 7 does not apply;
B. In Clause 11, the optional language does not apply;
C. All square brackets in Clause 13 are hereby removed;

D. In Clause 17 (Option 1), the EU SCCs will be governed by [MEMBER STATE] law;
E. In Clause 18(b), disputes will be resolved before the courts of [MEMBER STATE];
F. Exhibit 2 to this Addendum contains the information required in Annex I of the EU SCCs;
G. Exhibit 3 to this Addendum contains the information required in Annex II of the EU SCCs; and
H. By entering into this Addendum, the parties are deemed to have signed the EU SCCs incorporated herein, including its Annexes.

6.3 Ex-UK Transfers. Ex-UK Transfers are made pursuant to the UK Data Transfer Addendum, which is deemed entered into and incorporated into this Addendum by reference. For the UK Data Transfer Addendum, where applicable the following applies:

A. Exhibit 4 to this Addendum contains the information required in Part 1 – Tables, of the UK Data Transfer Addendum; and
B. By entering into this Addendum, the parties are deemed to have signed the UK Data Transfer Addendum incorporated herein.

6.4 Transfers from Switzerland. Transfers from Switzerland are made pursuant to the EU SCCs with the following modifications:

A. The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the EU SCCs shall be interpreted to include the Federal Act on Data Protection of 19 June 1992 (the "FADP," and as revised as of 25 September 2020, the "Revised FADP") with respect to data transfers subject to the FADP.

B. The terms of the EU SCCs shall be interpreted to protect the data of legal entities until the effective date of the Revised FADP.

C. Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner ("FDPIC") of Switzerland shall have authority over data transfers governed by the FADP and the appropriate EU supervisory authority shall have authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Section 13 shall be observed.

D. The term "EU Member State" as utilized in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

6.5 Supplementary Measures. In respect of any ex-EEA Transfer or ex-UK Transfer, the following supplementary measures shall apply:

A. As of the date of this Addendum, Company has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Personal Data is being exported, for access to (or for copies of) either Party's Personal Data ("Government Agency Requests").

B. Where allowed by Applicable Law, if after the date of this Addendum, Company receives any Government Agency Requests, Company shall attempt to redirect the law enforcement or government agency to request that data directly from Customer. As part of this effort, Company may provide Customer's basic contact information to the government agency. If compelled to disclose Customer's Personal Data to a law enforcement or government agency, Company shall give Customer reasonable notice of the demand, where allowed by Applicable Law, and cooperate to allow Customer to seek a protective order or other appropriate remedy unless Company is legally prohibited from doing so. Company shall not voluntarily disclose Personal Data to any law enforcement or government agency. Company shall (as soon as reasonably practicable) discuss

and determine whether all or any transfers of Personal Data pursuant to this Addendum should be suspended in the light of such Government Agency Requests.

C. If Applicable Laws require the Parties to execute the Standard Contractual Clauses applicable to a particular transfer of Personal Data as a separate agreement, the Parties shall, promptly execute such Standard Contractual Clauses incorporating such amendments as may reasonably be required to reflect the applicable appendices and annexes, the details of the transfer and the requirements of the relevant Applicable Laws.

D. If either (i) any of the means of legitimizing transfers of Personal Data outside of the EEA or UK set forth in this Addendum cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, each Party agrees to amend the means of legitimizing transfers or alternative arrangements with Customer, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Applicable Laws.

7. Rights of Data Subjects

Company will provide such assistance as is reasonably required to enable Customer to comply with Data Subject Rights requests within the time limits imposed by Applicable Laws.

8. Miscellaneous

8.1 This Addendum may be amended or modified only by a writing signed by both Parties. Both parties may disclose this Addendum to third parties (including other controllers, Data Subjects and regulators) for purposes of demonstrating compliance with Applicable Laws.

8.2 In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms in the EU SCCs or UK Data Transfer Addendum (where applicable); and (2) the terms of this Addendum; (3) the Agreement.

IN WITNESS WHEREOF, the parties hereto have executed and agree to the terms of this Addendum, including the Exhibits attached hereto, as of the date of the last signature below.

Customer: [INSERT]		**Company:** VelocityEHS Holdings, Inc.	
By:	_____	By:	_____
Print Name:	_____	Print Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____
Email:	_____	Email:	_____

Exhibit 1

Details of Processing

Nature and Purpose of Processing: Each Party will Process Customer's Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this Addendum, and in accordance with Customer's instructions as set forth in this Addendum. The nature of Processing shall include:

The Parties will process Personal Data as necessary to fulfil the Party's obligations under the Agreement and as otherwise set forth in this Addendum.

Duration of Processing: The term of the Agreement.

Continuous for the term of the services agreement between the data exporter and data importer.

Categories of Data Subjects: Categories of data subjects whose personal data is transferred include:

[Please identify the categories of data subjects whose data will be processed in connection with the services. Examples include: employees, students, contractors, consultants, clients, and customers.]

Categories of Personal Data: Categories of Personal Data include:

[Select those categories of personal information on the list below that will be processed in connection with the Services.]

- identity information (*e.g.,* name, age/date of birth, gender, photograph)
- contact information (*e.g.*, phone number, address, email address)
- citizenship information
- education information (*e.g.,* transcript, education history or file)
- employment information (*e.g.,* employer, job title, salary)
- criminal offense information (*e.g.,* arrest, detention, indictment, acquittal, sentencing, correctional supervision, release date)
- investigative report information (*e.g.,* polygraphs or psychological evaluation)
- data about an individual's tax filings
- disability Information
- information from or about children:
    - under age 13
    - age 13 - 16
- social security number or other government issued ID number (*full or partial*)

- credit card or payment card number
- personal credit information (*e.g.,* a report from a credit reporting agency or similar report for use in determining eligibility for a job, loan or other benefit)
- insurance Information (non-health)
- data that reasonably can be tied to a specific individual or computer, mobile telephone or tablet, such as IP address, MAC address or advertising ID.
- location data (*e.g.,* GPS, Bluetooth, GSM)
- other (please specify): _____

Special categories of data / sensitive Personal Data

The Personal Data transferred concern the following special categories of data (please specify):

[Select those special categories of personal information on the list below that will be processed in connection with the Services.]

- racial or ethnic origin
- political affiliation
- religious affiliation or beliefs
- trade union membership
- genetic information (*e.g.,* DNA profile)
- biometric data (*e.g.,* facial images, fingerprints)
- health information (*e.g.,* health insurance coverage, medical records, medical history, treatment or diagnosis)
- sexual orientation or gender identity
- other (please specify): _____

Exhibit 2

The following includes the information required by Annex I and Annex III of the EU SCCs.

A. LIST OF PARTIES

For transfers of EU Personal Data:

Data exporter(s):

Name: [INSERT]
Address: [INSERT]
Contact person's name, position and contact details:
[INSERT]

Activities relevant to the data transferred under these Clauses:
The data importer provides services to the data exporter in accordance with the Agreement.

_____ _____
(Signature) *(Date)*
Role: *controller*

Data importer(s):

Name: VelocityEHS Holdings, Inc.
Address: 222 Merchandise Mart Plaza, Suite 1750, Chicago, IL 60654

Contact person's name, position and contact details:
Brian Stroud, Senior Compliance Manager bstroud@ehs.com

Activities relevant to the data transferred under these Clauses:
The data importer provides services to the data exporter in accordance with the Agreement.

.

(Signature) *(Date)*

Role: *processor*

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose Personal Data is transferred
As described in Exhibit 1.

Categories of Personal Data transferred

As described in Exhibit 1.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
As described in Exhibit 1.

Nature of the processing

As described in Exhibit 1.

Purpose(s) of the data transfer and further processing
As described in Exhibit 1.

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period
As described in Exhibit 1.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
As described in Section D below.

C. COMPETENT SUPERVISORY AUTHORITY

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

For transfers of EU Personal Data:

Name: Data Protection Commission, Ireland
Address: 21 Fitzwilliam Square South Dublin 2 D02 RD28 Ireland

For transfers of UK Personal Data:

Name: UK Information Commissioner's Office
Address: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

D. LIST OF SUB-PROCESSORS

The controller has authorised the use of the following sub-processors:

Name:
Address:
Contact person's name, position and contact details:

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):

Exhibit 3

Description of the Technical and Organisational Security Measures implemented by the Company

As described in Section 3 of the Addendum.

Exhibit 4

Table 1: Parties

Start date	[DATE]	
The Parties	**Importer/Exporter (who sends/receives the Restricted Transfer)**	**Importer/Exporter (who sends/receives the Restricted Transfer)**
Parties' details	Full legal name: VelocityEHS Holdings, Inc. Trading name (if different): Main address (if a company registered address): 222 Merchandise Mart Plaza, Suite 1750, Chicago, IL 60654	Full legal name: Trading name (if different): Main address (if a company registered address):

	Official registration number (if any) (company number or similar identifier): 07061995	Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Brian Stroud Job Title: Senior Compliance Manager Contact details including email: bstroud@ehs.com	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	[X] The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: [DATE] Reference (if any): VelocityEHS Master Subscription & Services Agreement entered into by and between VelocityEHS Holdings, Inc. and [INSERT]. 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						
3						

4						

Table 3: Appendix Information

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

Annex 1A: List of Parties: As set forth in Annex 1A of the EU SCCs.
Annex 1B: Description of Transfer: As set forth in Annex 1B of the EU SCCs.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set forth in Annex II of the EU SCCs.
Annex III: List of Sub processors (Modules 2 and 3 only): As set forth in Annex 3 to the EU SCCs.

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 of the ICO's Standard Data Protection Clauses: [X] Importer [X] Exporter ☐ neither Party