Archer Data Processing Addendum

This Data Processing Addendum (the "**DPA**" or "**Addendum**") is effective as of the date of the last signature below (the "**Effective Date**") between the Archer entity set forth in the Agreement (as hereinafter defined, and the Archer entity, "**Archer**"), and the other party set forth below in the signature block (the "**Client**"). Both Client and Archer are individually referred to as a "**Party**" and jointly as "**Parties**".

1. Definitions. All capitalized terms not defined in this DPA have the meanings set forth in the Agreement.

The terms "**Controller**," "**Data Subject**," "**Personal Data**," "**Process**" (including its variants) and "**Processor**" have the meanings given in the GDPR.

"**Agreement**" means (x) the master subscription agreement or other agreement between Client and Archer governing Client's access to Archer's software (the "**Archer Application**"), (y) any service agreement between Client and Archer governing the provision of professional services by Archer if such professional services contain access to Client's Personal Data by Archer, or (z) both of the foregoing agreements together if applicable. Both the Archer Application and professional services are collectively, the "**Archer Solution**".

"**Data Breach**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data Processed by Archer.

"**Data Protection Laws**" means any laws, statutes, directives, or regulations applicable to the Processing of Personal Data to which a party to this Addendum is subject and apply to the Archer Solution provided under the Agreement, including but not limited to, (1)Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 repealing Directive 96/46/EC (the "**EU GDPR**"); (2) National laws (including the Data Protection Act 2018) implementing the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (3) the Swiss Federal Act on Data Protection as updated on 25 September 2020 and its corresponding ordinances ("**Swiss FADP**"); and (3) laws and regulations of the United States applicable to the processing of Personal Data under the Agreement, including but not limited to, (a) the California Consumer Privacy Act of 2018, as amended by the California Privacy Act of 2020 and its implementing regulations (collectively, the "**California Privacy Laws**"), (b) the Virginia Consumer Data Protection Act, effective January 1, 2025, (c) the Colorado Privacy Act and its implementing regulations, effective July 1, 2023, (d) the Connecticut Data Privacy Act effective July 1, 2023, (e) the Utah Consumer Privacy Act, effective December 31, 2023, (f) the Iowa Consumer Data Privacy Act, effective January 1, 2025; and (g) the New Jersey Data Privacy Act, effective January 15, 2025.

"**Standard Contractual Clauses**" means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**"); and (ii) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("**UK IDTA**").To

"**Subprocessor**" means a third party engaged by Archer that Processes Personal Data pursuant to the Agreement.

2. Data Processing Obligations; **Governance**.

2.1. Data Processor & Controller. As between Archer and Client, Archer shall Process Personal Data under the Agreement as a Processor acting on behalf of the Client, and if applicable, Client's affiliates that Client permits to use Archer's Services, acts as Controller. For California Privacy Law, Archer is a Service Provider. The parties agree that unless otherwise agreed to in writing by both parties, Client shall not require Archer to undertake or

engage in any activity under the Agreement that would require, or result in, Archer acting in the capacity of a Controller.

2.2. Instructions. Client's initial instructions to Archer regarding processing Personal Data are laid out in the Agreement and this Addendum. Client can issue modifications to its instructions and issue new instructions. Because of the nature of Archer's services as multi-client services, Client shall take the technical and operational feasibility of following its instructions into account. Archer shall use reasonable efforts to follow any Client instructions if they are required by Data Protection Law and are technically and operationally reasonably feasible. If carrying out an instruction is not required by Data Protection Law, is not technically and/or operationally reasonably feasible, Archer considers the instruction unlawful, or any combination of the foregoing, Archer shall notify Client without undue delay. The Parties shall then discuss the matter and work together in good faith to find a solution that is feasible and addresses the underlying legal issue or other concern or interest to Client. Archer is not liable to a Data Subject when acting on Client's instructions.

2.3. Client Personal Data Restrictions. Client agrees to limit any Personal Data it transfers to Archer, or to which Archer is otherwise given access for processing to only the Personal Data needed by Archer to fulfill its obligations under the Agreement and this Addendum.

2.4. Governance. Client acts as a single point of contact. Where authorizations, consent, instructions, or permissions are provided by Client, these are provided not only on behalf of the Client but also on behalf of any Client Affiliates using Archer's Services. Archer is not responsible for determining if Client's instructions related to Processing of Personal Data are compliant with applicable law. However, if Archer's reasonable opinion is that a Client instruction infringes applicable Data Protection Laws, Archer shall notify Client as soon as reasonably practicable and shall not be required to comply with such infringing instruction.

2.5. Client Warranty. Client hereby warrants and represents, on a continuous basis throughout the Term of the Agreement, that all Personal Data provided or made available by Client to Archer for Processing in connection with the Agreement was collected by Client and transmitted to Archer in accordance with applicable Data Protection Laws and Client has obtained all necessary approvals, consents, authorizations, and licenses from each and every Data Subject required under Data Protection Laws to enable Archer to Process Personal Data pursuant to the Agreement and to exercise its rights and fulfil its obligations under the Agreement.

2.6. Assistance. Archer shall provide Client with reasonable assistance with data protection impact assessments, prior consultations with data protection authorities that Client is required to carry out under Data Protection Laws, dealing with requests from Data Subjects, and any other assistance obligations required by applicable law.

2.7. Data Subject Requests. If Archer receives a request from a Data Subject regarding their Personal Data, Archer shall promptly ask the Data Subject to redirect its request to Client. Archer shall not respond to such communication directly without Client's prior authorization, unless legally compelled to do so. If Archer is required to respond to such a request, Archer shall promptly notify Client and provide Client with a copy of the request, unless legally prohibited from doing so.

2.8. Appropriate Personnel. Archer shall only engage personnel who have committed themselves to observing data privacy obligations. Archer shall regularly train those employees to whom it grants access to Client's Personal Data on security and privacy law compliance.

2.9. Client Warranty. Client shall, in its use of the Services, comply with its obligations under Data Protection Laws when Processing Personal Data and when issuing Processing instructions to Archer. Client hereby warrants continually throughout the term of the Agreement(s) that all Personal Data provided or made available by Client to Archer for Processing in connection with the Agreement was collected by Client and transmitted to Archer in accordance with applicable Data Protection laws and Client has obtained all necessary approvals, consents, authorizations and licenses from each and every Data Subject required under Data Protection Laws to enable Archer to Process Personal Data pursuant to the Agreement and to exercise its rights and obligations under the Agreement.

2.10. California Privacy Law. If the processing of Personal Data is subject to California Privacy Law, Archer: (i) represents that it understands the restrictions in this Addendum, and its obligations under California Privacy Law, and shall comply with it; (ii) shall not retain, use, or disclose Personal Data other than for the business purposes specified the Agreement, including for a commercial purpose, except as otherwise permitted by applicable United States data protection laws, including California Privacy Law; (iii) shall not combine Personal Data it receives from or on behalf of Client with personal data that it receives from another Client, except as otherwise permitted by applicable United States data protection laws, California Privacy Law; and (iv) shall not disclose or transfer Personal Data to any third party in a manner that qualifies as "selling" or "sharing" Personal Data under the California Privacy Law. Archer shall notify Client promptly if it makes the determination that it can no longer meet its obligations under applicable United States data protection laws, including California Privacy Law.

2.11. Correction, deletion, or blocking of Personal Data. Archer may be required to correct, erase and/or block Client Personal Data if and to the extent the functionality of the Service does not allow the Client to do so. However, Archer shall not correct, erase and/or block Personal Data unless instructed by Customer.

2.12. Data Deletion. Upon termination of the Agreement, Archer shall, as soon as reasonably practicable and in accordance with applicable law, delete Client's Personal Data on Archer systems. The provisions of this Addendum shall continue to apply to Client Personal Data until all such data is deleted. A certificate of destruction shall be provided upon request.

2.13. Data Breach. No later than seventy-two (72) hours after Archer has a reasonable degree of certainty about the occurrence of accidental or unlawful destruction, loss or alteration of, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed by Archer pursuant to this Addendum (a "**Personal Data Breach**"), Archer shall notify Client of the Personal Data Breach, provide such information as Client may reasonably require to meet its obligations under Data Protection Laws regarding the Personal Data Breach, and take steps to remediate the Personal Data Breach. Archer may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by Archer. Archer shall not inform any unaffiliated third party of the Personal Data Breach without first obtaining Client's prior written consent other than, in each case as necessary, another Client affected by the same Data Breach, a Subprocessor potentially possessing relevant information, experts or consultants utilized by Archer of any Data Breach relating to the Personal Data without first obtaining Client's prior written consent, and except as otherwise required by applicable law.

3. Subprocessing.

3.1. Sub-processor Approval. In accordance with Art. 28 (2) GDPR, Client hereby provides its general authorization to Archer to appoint any Sub-processors identified by Archer https://www.archerirm.com/company/legal-center (the "**Subprocessor List**") to Process Personal Data on Archer's behalf. Archer shall ensure that Sub-processors on the Sub-processor List are contractually obligated to protect Personal Data in compliance with Data Protection Laws and consistent with the obligations imposed on Archer in this Addendum. Archer shall remain responsible for the acts and omissions of each Sub-processor on the Sub-processor List as if they were the acts and/or omissions of Archer and shall insure that, where applicable, it has entered the appropriate Standard Contractual Clauses with its Sub-processors. Client agrees that Archer may provide written notification of any change to the Sub-processor List by updating the Sub-processor List. Alternatively, if Client subscribes to receive notifications from the Sub-processor List, Archer shall send an e-mail notification to Client of the engagement at least 30 days in advance of such appointment by maintaining an up-to-date Subprocessors List

3.2. Subprocessor Objections. If Client has a legitimate and material data protection reason to object to a Subprocessor added to the Subprocessor List, Client may object to the engagement of such Subprocessor by notifying Archer at legalnotices@archerirm.com and providing the basis for such objection within ten (10) days of Archer's notification. If Client does not so object, the engagement of such Subprocessor shall be deemed accepted by Client. If the Parties cannot mutually agree to a reasonable resolution within an additional 15

days of Archer's receipt of Client's objection, Client may terminate the affected software, professional services, or both. Client's objection does not affect Archer's ability to use the new Subprocessor.

3.3. Emergency Replacement. Archer may replace a Subprocessor without advance notice where the reason for the change is outside of Archer's reasonable control and prompt replacement is required for security or other urgent reasons. In this case, Archer will inform Client of the replacement Subprocessor as soon as possible following its appointment, and Client will have the same rights to object to such replacement Sub-processor as outlined in section 3.2 of this Addendum.

4. Security Measures. Taking into account industry standards, the reasonable costs of implementation, the nature, scope, context, and purposes of the Processing, and any other relevant circumstances relating to the Processing of the Personal Data on Archer systems, Archer shall implement appropriate technical and organizational measures to establish security, confidentiality, integrity, availability, and resilience of processing systems and services involved in the Processing of the Personal Data are commensurate with the risk in respect of such Personal Data. The Parties agree that the technical and organizational security measures described in the information security provisions at https://www.archerirm.com/company/legal-center provide an appropriate level of security for the protection of Personal Data to meet the requirements of this clause. Archer shall periodically (i) test and monitor the effectiveness of its safeguards, controls, systems, and procedures, and (ii) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of the Personal Data, and address these risks. Archer shall implement and document appropriate business continuity and disaster recovery plans, to enable Archer to continue or resume providing the Archer Application (including restoring access to the Personal Data where applicable) in a timely manner after a disruptive event.

5. International Data Transfers & Standard Contractual Clauses.

5.1. When providing the Archer Solution, Archer may make international transfers of Personal Data to its Affiliates, subsidiaries, or Subprocessors. When making such transfers, Archer shall establish an appropriate protection to safeguard the Personal Data transferred under or in connection with this Addendum.

5.2. When the Archer Solution involves the transfer of Personal Data from the United Kingdom to countries outside the EEA (which are not subject to an adequacy decision under Data Protection Laws) (each, an "**ex-UK Transfer**") such transfer shall be subject to the following requirements: (a) Archer has in place intra-group agreements that incorporate UK Standard Contractual Clauses (the "**UK IDTA**") with any Affiliates or subsidiaries which may have access to the Personal Data; and (b) Archer has in place agreements with its Subprocessors that incorporate the UK IDTA, as appropriate.

5.3. When Archer transfers Personal Data from the EEA to countries outside the EEA which are not subject to an adequacy decision under Data Protection Laws (each, an "**ex-EEA Transfer**"), such transfer shall be subject to the following requirements: (a) Archer shall have intra-group agreements that incorporate EU Standard Contractual Clauses with any affiliates or subsidiaries which may have access to the Personal Data; and (b) Archer shall have agreements with its Subprocessors that incorporate a lawful Personal Data transfer mechanism.

5.4. When the transfer of Personal Data from Client to Archer in connection with the Archer Solution constitutes an ex-EEA Transfer, Archer and Client shall comply with the EU Standard Contractual Clauses in relation to such ex-EEA Transfer (which for these purposes are hereby incorporated into this Agreement and executed by the parties) with the amendments set out below applied to the EU Standard Contractual Clauses:

5.4.1. When Client (as data exporter) acts as the Controller and Archer (as data importer) acts as a Processor, then Module Two applies, and the other Modules are disregarded.

5.4.1.1. The appropriate designation is set forth in the Schedule 1 section in this DPA.

5.4.1.2. In Clause 9(a), Option 2 applies. Archer shall inform the Client of any intended changes to sub-processors at least thirty (30) days in advance.

5.4.1.3. In Clause 17, Option 2 applies. As described in Clause 17, Parties agree that the law of the relevant Member State shall be the governing law.

5.4.1.4. For Clause 18(b), disputes shall be resolved in the courts of Data Exporter Member State.

5.4.1.5. Liability arising under the EU Standard Contractual Clauses in respect of a party shall form part of the liability of such party under the Agreement.

5.4.1.6. Annex II and III shall be as set out below.

5.5. When the transfer of Personal Data from Client to Archer regarding the Archer Solution constitutes an ex-UK Transfer, Archer and Client shall comply with the UK Standard Contractual Clauses in relation to such ex-UK Transfer (which for these purposes are hereby incorporated into this Agreement and executed by the parties) with the designations and amendments set out in Section 6.4 to this DPA.

5.6. When providing the Archer Solution involves the transfers of Personal Data from Switzerland to countries which are not subject to an applicable adequacy decision pursuant to the Swiss FADP, the EU Standard Contractual Clauses, in accordance with the designations set forth in Section 5.4.1 above, shall apply to such transfers, subject to the following modifications:

5.6.1. References in the EU Standard Contractual Clauses to the EU GDPR shall be interpreted as references to the Swiss FADP.

5.6.2. References to EU, Union, Member State, and EU Member State shall be interpreted as references to Switzerland applicable Swiss laws, and such references shall not be read as preventing data subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU Standard Contractual Clauses.

5.6.3. The competent supervisory authority, in relation to Clause 13 of the EU Standard Contractual Clauses and Part C of Annex 1, will be the Federal Data Protection and Information Commissioner ("**FDPIC**") of Switzerland.

5.6.4. in Clause 17, the EU Standard Contractual Clauses shall be governed by the laws of Switzerland.

5.6.5. For purposes of Clause 18 (b), the applicable courts of Switzerland shall apply.

5.7. If any provision of this Data Protection Addendum or the Agreement contradicts, directly or indirectly, with the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

5.8. If a new or modified version of the Standard Contractual Clauses or an alternative mechanism supersedes these Standard Contractual Clauses, such new or modified version of the Standard Contractual Clauses or an alternative mechanism shall be deemed to be incorporated into this Addendum.

6. Annexes to the Standard Contractual Clauses and the UK IDTA.

6.1. Annex 1 to the Standard Contractual Clauses.

6.1.1. List Of Parties:

6.1.1.1. Data Exporter: the entity identified as Client in this Addendum.

- **Address**: the address for Customer associated with its account or as otherwise specified in the Addendum or the Agreement.
- **Contact Person's name, position, and contact details**: the contact details associated with Customer's account, or as specified in this Addendum or the Agreement.
- **Activities relevant to the data transferred under the SCCs**: the activities are specified in Section 2 of the Addendum.
- **Role**: Controller.

6.1.1.2. Data Importer: Archer as identified in this Addendum, or the applicable Archer Technologies affiliate or Subprocessor.

- **Address**: as specified in the Agreement.
- **Contact Person's name, position, and contact details**: the contact details for Archer are specified in the Addendum or the Agreement.
- **Activities relevant to the data transferred under the SCCs**: as specified in this Addendum.
- **Role**: Processor.

6.1.2. Applicable Module(s): Module Two: Controller to Processor.

6.1.3. Description of Transfer:

6.1.3.1. Categories of Data Subjects whose Personal Data is transferred: Customer's end users, employees, contractors, suppliers and other third parties relevant to the Services.

6.1.3.2. Categories of personal data transferred:

- **Contact details**: which may include name, address, email address, telephone, fax, other contact details, emergency contact details, associated local time zone information.
- **Client Details**: which may include Contact details, invoicing, and credit related data.
- **IT Systems and Operational Information**: which may user ID and password details, computer name, email address, domain name, user names, passwords, IP address, permission data (according to job roles), account and delegate information for communication services, individual mailboxes and directories, chat communication data, software and hardware inventory, tracking information regarding patterns of software and internet usage (e.g. cookies), and information recorded for operational and/or training purposes.
- **Client Support**: which may include personal identifiers, voice, video and data recordings.
- **Other**: Any other Personal Data contained within Customer Content.

6.1.3.3. Sensitive data transferred: Archer does not intend to process any special categories of Personal Data on behalf of the Customer. Customer agrees not to provide, transfer, or disclose any special categories of Personal Data at any time to any of Archer's service offerings.

6.1.3.4. Transfer Frequency: continuous basis.

6.1.3.5. Purpose(s) of the data transfer and further processing: to provide the services described in the Agreement.

6.1.4. Competent Supervisory Authority: the Data Exporter's competent supervisory authority is determined in accordance with the EU GDPR.

6.2. Annex 2 Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data: the Information Security Provisions here: https://www.archerirm.com/company/legal-center, which are incorporated by reference.

6.3. Annex 3 List of Sub-processors: as indicated here: https://trust.archerirm.com/?_gl=1*147ws9v*_gcl_au*MjEzMDg1NDg2My4xNzQ2MjEwODUz.

6.4. The UK IDTA: as set forth in Schedule 2 to this Data Processing Addendum.

7. Auditing Rights. If Client is subject to an audit or investigation from a data protection regulator, Archer shall, when required, respond to any information requests, and/or agree to submit its premises and operations to audits, including inspections by Client and/or the competent data protection regulator, in each case for the purpose of evidencing its compliance with this Addendum, provided that: (v) Client shall ensure that all information obtained or generated in connection with any information request, audit or inspection is kept strictly confidential (unless disclosure to a competent data protection regulator or as otherwise required by applicable law); (w) Client ensures that any information request, audit or inspection is undertaken within normal business hours (unless such other time is mandated by a competent data protection regulator) with minimal disruption to Archer's business, and acknowledging that such information request, audit or inspection shall be subject to any reasonable policies, procedures or instructions of Archer for the purposes of preserving security and confidentiality; (x) Client shall give Archer at least 15 days' prior written notice of an information request and/or audit or inspection (unless the competent data protection regulator provides Client with less than 15 days' notice, in which case Client shall provide Archer with as much notice as practically possible); (y) a maximum of one information request, audit and/or inspection may be requested by Client in any 12 month period unless an additional information request, audit and/or inspection is mandated by a competent data protection regulator in writing; and (z) Client shall pay Archer's reasonable costs for any assistance or facilitation of any audit or inspection or other work undertaken unless such costs are incurred due to Archer's breach of its obligations under this Addendum. If any audit request is not at the request of a data protection regulator, Client agrees (1) to request information in the first instance in written form, (2) Archer may respond to such requests by providing up-to-date attestations, reports or extracts from independent bodies (e.g., ISO 27001 reports/certificates) that

scrutinizes and confirms the processing of Client's Personal Data is in accordance with the agreed to measures herein, it being understood that Client may demand additional clarifications and perform on-site inspections where necessary to satisfy Data Protection Law requirements, or (3) on Archer's request, to conduct the audit through a certified auditor the Parties jointly agree on.

8. General.

8.1. Conflict. If there is any conflict between this Addendum and the Agreement, the terms of this Addendum prevail regarding its subject matter.

8.2. Amendment. Archer may modify the terms of this Addendum as provided in the Agreement (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary, to comply with Data Protection Laws, or (iii) to implement or adhere to applicable Standard Contractual Clauses, approved codes of conduct or certifications, binding corporate rules, or other compliance mechanisms, which may be permitted under Data Protection Laws. Supplemental terms may be added as an Annex or Appendix to this Addendum where such terms only apply to the Processing of Personal Data under the Data Protection Laws of specific countries or jurisdictions. Archer shall provide notice of such changes to Client, and the modified Addendum shall become effective, in accordance with the terms of the Agreement or as otherwise provided on Archer's website if not specified in the Agreement.

Archer	Client
Entity Name: as set forth in the Agreement.	**Entity Name**:
By:	**By**:
Name:	**Name**:
Title:	**Title**:
Date:	**Date**:

Schedule 1: Standard Contractual Clauses

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of data to a third country.

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

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

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required

under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to

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

8.8 Onward transfers

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

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

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

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

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

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

8.9 Documentation and compliance

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

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

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

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

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

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

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

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

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

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

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

Clause 15

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

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

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

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type

of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland (specify Member State).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

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

ANNEX I

A. **LIST OF PARTIES** **(As set forth in section 6.1 of this Data Processing Addendum)**

1. **Data exporter(s):** [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: .....

Address: .....

Contact person's name, position and contact details: .....

Activities relevant to the data transferred under these Clauses: .....

Signature and date: .....

Role (controller/processor): .....

2. **Data importer(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: .....

Address: .....

Contact person's name, position and contact details: .....

Activities relevant to the data transferred under these Clauses: .....

Signature and date: .....

Role (controller/processor): .....

B. **DESCRIPTION OF TRANSFER** **(As set forth in sections 6.1.2 & 6.1.3 of this Data Processing Addendum)**

Categories of data subjects whose personal data is transferred

.....

Categories of personal data transferred

.....

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.

.....

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

.....

Nature of the processing

.....

Purpose(s) of the data transfer and further processing

.....

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

.....

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

.....

C. **COMPETENT SUPERVISORY AUTHORITY** **(As set forth in section 6.1.4 of this Data Processing Addendum)**

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

ANNEX II

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

As set forth in Section 4 of the Data Processing Addendum.

ANNEX III

LIST OF SUB-PROCESSORS

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

As set forth in Section 3 of the Data Processing Addendum.

Information Commissioner's Office

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

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:	Full Name (optional): Job Title:

	Contact details including email:	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: As of the date the Data Processing Addendum is signed by the parties. Reference (if any): N/A. Other identifier (if any): N/A. 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 section 6.1 of this Data Processing Addendum.
Annex 1B: Description of Transfer: As set forth in sections 6.1.2 & 6.1.3 of this Data Processing Addendum.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: As set forth in Section 4 of the Data Processing Addendum.
Annex III: List of Sub processors (Modules 2 and 3 only): As set forth in Section 3 of the Data Processing Addendum.

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 **Error! Reference source not found.**: ☒ Importer ☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses

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 **Error! Reference source not found.** of those Mandatory Clauses.