Data Processing Addendum

Last Modified: October 30, 2025

Pursuant to the Agreement, SFC will provide certain services to Customer that may involve SFC (or a Subcontractor) Processing Customer Personal Data on behalf of Customer. This Data Processing Agreement ("**DPA**") applies to such Processing of Customer Personal Data by or on behalf of SFC. This DPA is incorporated into and made a part of the Batch Inference Terms and Conditions available on SFC's website.

1. Definitions

1.1 In this DPA, capitalized terms will have the meanings set forth below. Capitalized terms not otherwise defined in this DPA will have the meanings given to them in the Agreement.

1.2 "**Consumer**" means a natural person. Where applicable, Consumer will be interpreted consistent with the same or similar term under Data Protection Laws.

1.3 "**Controller**" means a person or entity that collects Customer Personal Data and alone, or jointly with others, determines the purposes and means of the Processing of Customer Personal Data. Where applicable, Controller will be interpreted consistent with the same or similar term under Data Protection Laws.

1.4 "**Data Protection Laws**" means the applicable laws, rules, and regulations of any relevant jurisdiction governing privacy, data protection, security, or the Processing by SFC of Customer Personal Data.

1.5 "**Data Subject**" means the individual to whom Customer Personal Data relates.

1.6 **"Customer"** means the Customer party stated on the Order Form.

1.7 "**Customer Personal Data**" means any Personal Data Processed by or on behalf of SFC in connection with SFC's provision of the Services to Customer.

1.8 "**Personal Data**" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with an identified or identifiable natural person. Where applicable, Personal Data will be interpreted consistent with the same or similar term under Data Protection Laws.

1.9 "**Process"** means any operation or set of operations performed on Customer Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, access, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. Where applicable, "Process" will be interpreted consistent with the same or similar term under Data Protection Laws.

1.10 "**Sale**" and "**Sell**" have the meanings given to them by applicable Data Protection Laws.

1.11 "**Security Incident**" means: the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise Processed under this DPA.

1.12 "**Services**" means any products or services provided by or for SFC to Customer pursuant to the Agreement.

1.13 **"SFC"** means San Francisco Compute Company.

1.14 "**Share**" has the meaning given to it by the California Consumer Privacy Act, as amended by the California Privacy Rights Act.

1.15 "**Subcontractor**" means any including any third party engaged by SFC to Process Customer Personal Data.

2. Scope, Roles, and Termination.

2.1 This DPA applies only to SFC's Processing of Customer Personal Data for the nature, purposes, and duration set forth in Appendix A.

2.2 For the purposes of the Agreement and DPA, Customer is the Party responsible for determining the purposes and means of Processing Customer Personal Data as the Controller and appoints SFC as a Processor to Process Customer Personal Data on behalf of Customer for the limited and specific purposes set forth in Appendix A.

2.3 Upon termination of the Agreement, except as set forth therein or herein, SFC will discontinue Processing and destroy Customer Personal Data in its or its subcontractors' and sub-processors' possession without undue delay. SFC may retain Customer Personal Data to the extent required by law but only to the extent and for such period as required by such law and always provided that SFC ensures the confidentiality of all such Customer Personal Data.

3. Processing of Customer Personal Data

3.1 SFC agrees to each of the following:

(1) SFC will (and will ensure that its employees, agents, and Subcontractors, will) Process Customer Personal Data solely on behalf of and subject to the written instructions of Customer, unless such instructions conflict with applicable law to which SFC is subject, in which case SFC will provide prior notice of that legal requirement to Customer to the extent permitted by applicable laws. The Agreement and any amendments thereto will constitute Customer's written instructions pursuant to this Section 3.1. SFC also will comply with its obligations under Data Protection Laws.

(2) SFC will not: (i) sell, rent, share, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, any Customer Personal Data to any third party for monetary or other valuable consideration; (ii) retain, use, or disclose any Customer Personal Data for any purpose other than for the specific purpose of performing the Services for Customer; (iii) retain, use, or disclose Customer Personal Data outside of the business relationship between the Parties; and (iv) combine Customer Personal Data with data obtained from, or on behalf of, sources other than Customer, except as expressly permitted under applicable Data Protection Laws and the Agreement.

(3) SFC will implement industry standard security measures designed to ensure the confidentiality, integrity, and availability of Customer Personal Data and any systems used by or on behalf of SFC to Process Customer Personal Data. Such measures will include, but not be limited to, those listed in Appendix 2 to this DPA. SFC also will maintain a comprehensive written information security program that complies with applicable Data Protection Laws.

(4) At the request of Customer, SFC will provide documentation regarding the security measures it has implemented and maintains pursuant to this Section 3 and Appendix 2 and will allow Customer to review and assess such measures. Customer will give SFC reasonable notice of any such review or assessment and will take reasonable steps to avoid causing (or, if it cannot avoid, to minimize) any damage, injury or disruption to SFC's premises, equipment, personnel, and business while its personnel are on those premises in the course of such an audit or inspection. Except as otherwise required by applicable law or a regulator or other relevant governmental entity, any audit or inspection will be conducted within normal business hours no more than once in any calendar year and as requested by Customer in response to a Security Incident.

3.2 The Parties acknowledge and agree that any disclosure or making available of any Personal Data between the Parties does not form part of any monetary or other valuable consideration exchanged between the Parties with respect to the Agreement or this DPA.

3.3 Customer Obligations.

(1) Customer will comply with applicable Data Protection Laws, including with respect to any applicable Customer obligations to provide notices to and/or obtain consents from any Data Subjects to enable SFC to Process Customer Personal Data in compliance with applicable Data Protection Laws; and

(2) Customer will notify SFC if it makes a determination that the Processing of Customer Personal Data pursuant to this DPA does not comply with applicable Data Protection Laws, in which case SFC will not be required to continue Processing such Customer Personal Data.

4. Compliance Monitoring and Assurance

4.1 Customer has the right to take reasonable and appropriate steps to ensure that SFC uses Customer Personal Data consistent with Customer's obligations under applicable Data Protection Laws.

4.2 Customer has the right to monitor SFC's compliance with this DPA through measures, including, but not limited to, requests for information and documentation regarding SFC's security program and its Processing of Customer Personal Data.

4.3 SFC will promptly notify Customer if it determines that it can no longer meet its obligations under applicable Data Protection Laws. Upon receiving notice from SFC in accordance with this subsection, Customer may direct SFC to take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data.

5. Reasonable Assistance

5.1 Where applicable, SFC will provide commercially reasonable assistance to Customer for the fulfillment of Customer's obligations to respond to Data Protection Law-related Consumer rights requests regarding Customer Personal Data.

5.2 Where applicable, SFC will not be required to delete any Customer Personal Data to comply with a Consumer's request if retaining such information is specifically permitted by applicable Data Protection Laws; provided, however, that in such case, SFC will promptly inform Customer of the exceptions relied upon under applicable Data Protection Laws and SFC will not use Customer Personal Data retained for any purpose other than provided for by that exception.

6. Reliability and Confidentiality

6.1 SFC will limit access to Customer Personal Data only to those individuals who need to know or otherwise Process such Customer Personal Data to perform the Services for Customer.

6.2 Without prejudice to any existing contractual arrangements between the Parties, SFC will ensure that its employees, personnel, and Subcontractors are subject to obligations of confidentiality applicable to Customer Personal Data no less protective of Customer Personal Data than those to which SFC itself is subject.

7. Subcontractors

7.1 SFC's current Subcontractors are set forth in Appendix 3Subcontractors. SFC will notify Customer of any intended changes concerning the addition or replacement of Subcontractors. Further, SFC will ensure that SFC's Subcontractors agree in writing to the same or equivalent restrictions and requirements that apply to SFC in this DPA and the Agreement with respect to Customer Personal Data, as well as to comply with applicable Data Protection Laws.

7.2 Customer may object in writing to SFC's appointment of a new Subcontractor on reasonable grounds by notifying SFC in writing within 30 calendar days of receipt of notice in accordance with Section 7.2. If Customer objects, the Parties will discuss Customer's concerns in good faith with a view to achieving a commercially reasonable resolution.

8. Security Incidents

8.1 SFC will notify Customer in writing promptly upon becoming aware of a Security Incident and will provide Customer with sufficient information to allow Customer to meet any obligations to report a Security Incident under Data Protection Laws. Such notification by SFC will, at a minimum, describe:

(a) the nature of the Security Incident, (where applicable) the categories and numbers of Data Subjects concerned, the date(s) on which SFC believes the Security Incident occurred, the date on which SFC became aware of the Security Incident, and separate descriptions of the categories and numbers of Customer Data records concerned;

(b) the consequences of the Security Incident; and

(c) the measures taken or proposed to be taken to address the Security Incident.

8.2 SFC will cooperate with Customer and take reasonable steps as directed by Customer to assist in the investigation, mitigation, and remediation of each Security Incident, sufficient to enable Customer to (i) perform an investigation into the Security Incident; (ii) formulate an appropriate response; and (iii) take suitable further steps in respect of the Security Incident to meet any requirement under applicable Data Protection Laws.

8.3 SFC will not inform any third party of a Security Incident without first obtaining Customer's prior written consent, unless notification is required by applicable law, rule, or regulation with the force of law to which SFC is subject, in which case SFC will, to the extent practicable and legally permitted, inform Customer of that requirement, provide a copy of

the proposed notification and consider any comments made by Customer before notifying any third party of the Security Incident.

8.4 Any notifications to Customer made pursuant to this Section 8 will be addressed to the Customer contact on the Order Form.

9. Deletion and Return of Customer Personal Data

9.1 Upon direction by Customer, and in any event no later than thirty (30) days after receipt of a request from Customer, SFC will promptly delete Customer Personal Data as directed by Customer, unless SFC is required by law to retain such data, in which case SFC will, on ongoing basis, isolate and protect the security and confidentiality of such Customer Personal Data and prevent any further processing except to the extent required by such law and will destroy or return to Customer all other Customer Personal Data not required to be retained by SFC by law.

10. Transfers of Personal Data outside the EEA under SCC Module Two. Where SFC is located outside the European Economic Area (**EEA**) in a country that is not deemed to have an adequate level of protection by the European Commission or is in the United States but not self-certified under the DPF, the parties agree to incorporate by reference the SCCs for the transfer of Personal Data that are subject to the GDPR from a data controller in the EEA to a data processor established outside the EEA, in the form set out in Module Two to the Annex to European Commission Implementing Decision (EU) 2021/914, and the SCCs are deemed to be executed by the parties. A copy of the SCCs can be accessed here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en. For the purpose of the SCCs: (i) Customer is the data exporter, SFC is the data importer, and the contact details of each party are deemed to be included in the Order Form; (ii) optional Clause 7 (Docking clause) is excluded; (iii) for Clause 9(a), Option 2 is selected and thirty (**30**) days' prior, written notice before a change of sub-processor is required; (iv) for Clause 11(a), the optional paragraph is deleted relating to an independent, dispute-resolution body; (v) for Clause 13(a), the first option is selected and the competent supervisory authority will be the Irish Data Protection Commission; (vi) for Clause 17, Option 1 is selected and the SCCs will be governed by the law of the country indicated in the governing law provision of the Agreement, unless such country is not an EU Member State, in which case the laws of Ireland; (vii) for Clause 18(b), the parties agree to the courts of the country indicated in the jurisdiction provision of the Agreement, unless such country is not an EU Member State, in which case the courts of Ireland will have jurisdiction for any disputes relating to the SCCs; (viii) the information set out in Appendices 1, 2, and 3 to this Addendum will be deemed populated into Annexes I, II, and III of the SCCs, respectively, again noting that, for Annex I.C, the competent supervisory authority is the Irish Data Protection Commission. The parties acknowledge and agree that SFC can meet its obligations under the SCCs, having considered the sundry factors specified in Clause 14, including but not limited to the laws of the receiving country or countries, the volume and categories of Personal Data, and (to SFC's knowledge) SFC's history and similar organizations' likelihood of receiving government-information requests or surreptitious surveillance. On this basis, no supplemental measures for the transfers envisaged under the SCCs are required beyond the contractual safeguards contained herein and the security measures employed by SFC reflected in Appendix 2 to this Addendum. If there is any conflict between the SCCs and this Addendum, the SCCs will prevail.

11. UK Personal Data Transfers. For transfers of or remote access to Personal Data subject to the UK GDPR, the ICO Addendum will apply where the Customer is established in the UK and SFC is located outside the UK in a country that is not the subject of an adequacy decision from the UK. The ICO Addendum is Appendix 4 to this DPA.

12. Swiss Personal Data Transfers. For transfers of or remote access to Personal Data subject to the Swiss FDPA, the SCCs cited and related language included in Section 10 of this Addendum will apply where the Customer is established in Switzerland and SFC is located outside Switzerland in a country that is not the subject of an adequacy decision by the Swiss Federal Data Protection and Information Commissioner (**Swiss FDPIC**). In addition, when applying such SCCs to such Personal Data, (i) for Clause 13(a), the Swiss FDPIC is the competent supervisory authority; (ii) for Clause 17, the laws of Switzerland govern; (iii) for Clause 18(c), Swiss Data

Subjects may bring legal proceedings in their place of habitual residence (Switzerland); and (iv) generally, references to the GDPR include reference to equivalent provisions of the Swiss FADP.

13. Miscellaneous

13.1 Any changes to this DPA will be made in writing regardless of any provisions to the contrary in the Agreement.

13.2 Conflicts or inconsistencies with respect to data privacy and data security will be resolved as follows: in any conflict between the terms of the Agreement and this DPA, this DPA will control to the extent of such conflict.

13.3 This DPA represents the entire understanding between the Parties in relation to its subject matter and supersedes all agreements and representations made by the Parties, whether oral or written. Should any provision of this DPA be deemed invalid or unenforceable, then the remainder of this DPA will remain valid and in force. The invalid or unenforceable provision will be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, (if this is not possible), (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

13.4 If any variation is required to this DPA as a result of a change in applicable Data Protection Laws, then either Party may provide written notice to the other Party of such change. The Parties will discuss and negotiate in good faith any necessary variations to this DPA to address such change.

13.5

APPENDIX 1
Processing Details

Nature of the Processing	To provide the Services to Customer.
Purpose(s) of the Processing	To provide the Services to Customer and as otherwise set forth in the Agreement.
Types of Customer Data Subject to Processing	As set out in the Order Form
Duration of Processing	As set out in the Order Form

APPENDIX 2

INFORMATION SECURITY MEASURES

As applicable to its Processing of Customer Data, SFC will implement and maintain the information security measures described below.

1. Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Customer Data is Processed, which may include, as applicable:

☐ Establishing security areas, restriction of access paths;

☐ Establishing access authorizations for employees and third parties;

☐ Access control system (ID reader, magnetic card, chip card);

☐ Key management, card-keys procedures;

☐ Door locking (electric door openers etc.);

☐ Security staff, janitors;

☐ Surveillance facilities, video/CCTV monitor, alarm system; and

☐ Securing decentralized data processing equipment and personal computers.

2. Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons, which may include, as applicable:

☐ User identification and authentication procedures;

☐ ID/password security procedures (special characters, minimum length, change of password);

☐ Automatic blocking (e.g., password or timeout);

☐ Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous password attempts;

☐ Creation of *one* master record per user, user-master data procedures per data processing environment; and

☐ Encryption of archived data media.

3. Data access control

Technical and organizational measures to ensure confidentiality and that persons entitled to use a data processing system gain access only to such Customer Data in accordance with their access rights, and that Customer Data cannot be read, copied, modified or deleted without authorization, which may include, as applicable:

☐ Internal policies and procedures;

☐ Control authorization schemes;

☐ Default configuration;

☐ Differentiated access rights (profiles, roles, transactions, and objects);

☐ Monitoring and logging of access;

☐ Disciplinary action against employees who access Customer Data without authorization;

☐ Reports of access;

☐ Access procedure;

☐ Change procedure;

☐ Deletion procedure; and

☐ Encryption.

4. Disclosure control

Technical and organizational measures to ensure that Customer Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Customer Data are disclosed, which may include, as applicable:

☐ Encryption/pseudonymization/tunneling;

☐ Logging; and

☐ Transport security.

5. Entry control

Technical and organizational measures to monitor whether Customer Data have been entered, changed or removed (deleted), and by whom, from data processing systems, which may include, as applicable:

☐ Logging and reporting systems; and

☐ Audit trails and documentation.

6. Control of instructions

Technical and organizational measures to ensure that Customer Data are Processed solely in accordance with the instructions of the Controller which may include, as applicable:

☐ Unambiguous wording of the contract;

☐ Formal commissioning (request form); and

☐ Criteria for selecting the Processor.

7. Availability control

Technical and organizational measures to ensure the integrity, availability and resilience of the processing systems, and that Customer Data are protected against accidental destruction or loss (physical/logical) which may include, as applicable:

☐ Backup procedures;

☐ Mirroring of hard disks (e.g., RAID technology);

☐ Uninterruptible power supply (UPS);

☐ Remote storage;

☐ Antivirus/firewall systems; and

☐ Disaster recovery plan, in the event of a physical or technical incident.

8. Separation control

Technical and organizational measures to ensure that Customer Data collected for different purposes can be Processed separately, which may include, as applicable:

☐ Separation of databases;

☐ “Internal client” concept / limitation of use;

☐ Segregation of functions (production/testing); and

☐ Procedures for storage, amendment, deletion, transmission of data for different purposes.

9. Testing controls

Technical and organizational measures to test, assess and evaluate the effectiveness of the technical and organizational measures implemented in order to ensure the security of the processing, which may include, as applicable:

☐ Periodic review and testing of disaster recovery plan;

☐ Testing and evaluation of software updates before they are installed;

☐ Authenticated (with elevated rights) vulnerability scanning; and

☐ Test bed for specific penetration tests and red team attacks.

10. IT governance

Technical and organizational measures to improve the overall management of IT and ensure that the activities associated with information and technology are aligned with the compliance efforts, which may include, as applicable:

☐ Certification/assurance of processes and products;

☐ Processes for data minimization;

☐ Processes for data quality;

☐ Processes for limited data retention;

☐ Processes for ensuring accountability; and

☐ Data subject rights policies.

APPENDIX 3

Subcontractors

1. Modular, Inc.

APPENDIX 4: ICO ADDENDUM

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	Effective Date of Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Customer name, as per the Order Form Trading name (if different): N/A Main address (if a company registered address): As the Order Form Official registration number (if any) (company number or similar identifier): As per Order Form	Full legal name: San Francisco Compute Compay Trading name (if different): N/A Main address (if a company registered address): As per Order Form Official registration number (if any) (company number or similar identifier): N/A
Key Contact	Full Name (optional): As Order Form Job Title: As per Order Form Contact details including email: As per Order Form	Full Name (optional): As per Order Form Job Title: As Per Order Form Contact details including email: As per Order Form

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: Effective Date of Agreement

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: Section 1 of the Data Processing Addendum to the Agreement
Annex 1B: Description of Transfer: Appendix 1 to the Data Processing Addendum to the Agreement

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Appendix 2 to the Data Processing Addendum to the Agreement
Annex III: List of Sub processors (Modules 2 and 3 only): Appendix 3 to the Data Processing Addendum to the Agreement

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☐ Importer ☐ Exporter ☒ neither Party

PART 2: MANDATORY CLAUSES

Entering into this Addendum

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

Interpretation of this Addendum

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

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.

Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, reenacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
    b. In Clause 2, delete the words: "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";
    c. Clause 6 (Description of the transfer(s)) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";
    d. Clause 8.7(i) of Module 1 is replaced with: "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";
    e. Clause 8.8(i) of Modules 2 and 3 is replaced with: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"
    f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;
    g. References to Regulation (EU) 2018/1725 are removed;
    h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";
    i. Clause 13(a) and Part C of Annex I are not used;
    j. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";
    k. In Clause 16(e), subsection (i) is replaced with: "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";
    l. Clause 17 is replaced with: "These Clauses are governed by the laws of England and Wales.";
    m. Clause 18 is replaced with: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any

country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

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

Amendments to this Addendum

16. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
17. From time to time, the ICO may issue a revised Approved Addendum which:
    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.
18. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
    a. its direct costs of performing its obligations under the Addendum; and/or
    b. its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.
19. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.