DATA PROCESSING AGREEMENT

This Data Processing Agreement ("***DPA***") is dated as of _____ ("***Effective Date***") and is by and between ENTER SUDDATH/STRLX ENTITY located at ENTER SUDDATH/STRLX ADDRESS and, as applicable, those specific additional, related entities listed below (collectively, "***Enterprise***") and _____ located at _____ ("***Company***"). This DPA shall govern those certain services, which include, but are not limited to, providing, facilitating, and/or arranging transportation, relocation, and/or logistics related services ("***Services***") in accordance with an agreement or other commercial relationship between Enterprise and Company (collectively, the "***Agreement***").

1. Definitions:[1]

1.1 "***Applicable Data Protection Laws***" means any and all privacy and data protection laws anywhere in the world now in existence or as amended or enacted in the future, including, but not limited to: (***i***) Regulation 2016/679/EU ("***GDPR***"); (***ii***) Swiss Federal Act on Data Protection ("***FADP***"); (***iii***) Cybersecurity Law, Data Security Law, Personal Information Protection Law, Civil Code and Civil Procedure Law of the People's Republic of China; (***iv***) California Consumer Privacy Act of 2018 and California Privacy Rights Act of 2020; (***v***) Colorado Privacy Act; (***vi***) Utah Consumer Privacy Act; (***vii***) Virginia Data Protection Act; and (***viii***) Connecticut Data Privacy Act.

1.2 "***Authorized Person***" means an individual or entity authorized by either Company or Enterprise, as applicable to Process Personal Information.

1.3 "***Controller***" means the individual or entity that determines the purpose and means of Processing Personal Information.

1.4 "***Confidential Information***" means any and all information, including Personal Information, provided by a party for a party's provision of Services under the Agreement.

1.5 "***Data Subject***" means the individual to whom the Personal Information applies.

1.6 "***Data Breach***" means an occurrence in which Confidential Information is accidentally or unlawfully destroyed, lost, altered, accessed or disclosed without authorization.

1.7 "***EU SCCs***" means the Standard Contractual Clauses issued pursuant to Commission Implementing Decision (EU) 2021/914 of June 4, 2021, on standard contractual clauses for the transfer of Personal Information to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

1.8 "***Personal Information***" means any information relating to an identified or identifiable natural person.

1.9 "***Process***, ***Processing***, ***Processes,*** or ***Processed***" means any operation or set of operations which is performed upon Personal Information, whether or not by automatic means, including, but not limited to, collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing by transmitting, disseminating or otherwise making available, aligning, combining, restricting, erasing or destroying.

1.10 "***Processor***" means an individual or entity that Processes Personal Information on behalf of a Controller.

1.11 "***Sell***" means to rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, Personal Information to a third party for monetary or other valuable consideration.

1.12 "***Share***" means to rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, Personal Information to a third party for cross-context behavioral advertising, whether or not for monetary or other consideration.

1.13 "***Subprocessor***" means an individual or entity contractually engaged by a Processor to Process Personal Information.

1.14 "***Targeted Advertising***" means focused and promotional communications to a Data Subject based on Personal Information obtained by a Data Subject's use of websites, applications, systems or other related technology or services.

1.15 "***Unauthorized Person***" means an individual or entity who is not an Authorized Person.

2. Relationship of the Parties: Company and Enterprise acknowledge and agree that each may act in the capacity of a Controller (but not a joint Controller), Processor, or Subprocessor and shall comply with all Applicable Data Protection Laws.

3. Compliance with Applicable Data Protection Laws: Each party represents and warrants that it ***i***) shall only Process Personal Information for the provision of Services as required under the Agreement and/or as otherwise instructed in writing (email or otherwise) and only for as long as needed for the provision of Services or in compliance with the instructions, and always in accordance with Applicable Data Protection Laws including, but not limited to, non-aggregation of Personal Information; ***ii***) does not receive Personal Information as consideration for Services; ***iii***) will not Sell Personal Information; or ***iv***) will not Share Personal Information for Targeted Advertising. A party will immediately notify the other if, in its reasonable opinion, an instruction to Process Personal Information violates Applicable Data Protection Laws.

[1] Definitions are inclusive of all analogous terms that have similar meanings as set forth in Applicable Data Protection Laws.

4. Confidentiality of Processing: Authorized Persons shall be subject to a strict duty of confidentiality (whether contractual or statutory), shall not permit any Unauthorized Persons to Process Personal Information, and will at all times comply with the requirements set forth in this DPA. Authorized Persons may access Personal Information from a remote location on either a temporary or permanent basis.

5. Cooperation and Data Subjects' Rights: The parties shall provide all reasonable and timely assistance when responding to requests, correspondence, inquiries, or complaints from a Data Subject, including any requests made to exercise rights under Applicable Data Protection Laws, and shall instruct, to the extent applicable, any Controllers, Processors or Subprocessors to do the same. In the event that any such request, correspondence, inquiry or complaint is made directly to a party, or to its Controllers, Processors or Subprocessors, the parties shall, and shall require the same of any of its Controllers, Processors and/or Subprocessors, within twenty-four (24) hours, provide full written details of such request to Controller. All Controllers, Processors and Subprocessors shall wait for further instruction from Controller before taking any action with regard to such request, correspondence, inquiry, or complaint.

6. Access by Authorities or Other Third Parties: To the extent legally permissible, the parties will promptly, and no later than five (5) business days following receipt, and in all cases before producing and/or providing access to any Confidential Information, notify the other of ***i***) any request for access to Confidential Information from a regulatory body, government official, or other third party, and/or ***ii***) any warrant, subpoena, request for production, other legal process, or other request to a party regarding Confidential Information. The parties shall comply with any legal hold regarding Confidential Information and will provide reasonable support for compliance with third-party requests. Each party will reasonably cooperate, and shall contractually require the same of its Controllers, Processors and/or Subprocessors, with a regulator's legal request to access Confidential Information.

7. Data Protection Impact Assessment: If a party reasonably believes or becomes aware that Processing of Personal Information is likely to result in a violation of the data protection rights and/or freedoms given to Data Subjects under Applicable Data Protection Laws, it shall promptly inform the other in writing and provide all such reasonable and timely assistance as may be required in order to conduct a data protection impact assessment. Each party represents and warrants that it has no reason to believe that the Applicable Data Protection Laws prevent it from complying with the terms and conditions of this DPA. In the event of changes to Applicable Data Protection Laws which are likely to have a substantial, adverse effect on a party's representations, warranties and obligations hereunder, such impacted party will promptly notify the other in writing.

8. Subcontracting: The parties acknowledge and agree that each may contractually engage with Controllers, Processors and/or Subprocessors to Process Personal Information. Each party shall ***i***) impose data protection rights and contractual terms on any Controller, Processor, or Subprocessor it appoints that provide at least the same level of protection for Confidential Information and Personal Information as set forth in this DPA; ***ii***) provide details of any Controller, Processor, or Subprocessor appointed, on request; and ***iii***) remain fully liable, and shall indemnify and hold the other harmless, from and against any breach of this DPA or any Data Breach that is caused by an act, error or omission of such party's Controllers, Processors, Subprocessors, and/or Authorized Persons.

9. International Transfers: Each party authorizes the other to make international data transfers of Personal Information in accordance with this DPA so long as such transfer is for the provision of Services and in accordance with the Agreement and all Applicable Data Protection Laws.

To the extent that Personal Information is transferred from Switzerland to a third country and is subject to the FADP, each party shall comply with all applicable obligations outlined in the FADP, and this DPA shall be modified to comply with the FADP. Further, the competent supervisory authority of the Swiss Federal Data Protection and Information Commissioner ("***FDPIC***") shall apply exclusively, but only to the extent that the Personal Information transfer is subject to the EU SCCs. Where the EU SCCs are modified by this section 9, all references to the GDPR shall be understood as references to the FADP. Where both the GDPR and FADP apply, there will be parallel authority between the FDPIC and the GDPR supervisory authority designated in Clause 13 of the EU SCCs.

Data Subjects in Switzerland may file a lawsuit in Switzerland related to their data privacy rights.

Except as otherwise provided in this section 9, the FADP terms do not modify, limit, or reduce any data protection representations and warranties the parties make in this DPA.

With respect to Personal Information transferred from the European Economic Area, each party agrees to the EU SCCs. The EU SCCs form part of this DPA, and take precedence in the event of a conflict with this DPA. The EU SCCs can be found on the European Commission's website at commission.europa.eu.

In the event the EU SCCs are applicable to the Services, the parties acknowledge and agree that ***i***) Module One of the EU SCCs shall apply when one party acts as the Controller and exporter, and the other acts as a Controller and importer; ***ii***) Module Two of the EU SCCs shall apply when one party acts as the Controller and exporter, and the other acts as a Processor and importer; ***iii***) Module Three of the EU SCCs shall apply when one party acts as the Processor and exporter, and the other acts as a Subprocessor and importer; and ***iv***) Module Four of the EU SCCs shall apply when one party acts as a Processor and exporter, and the other acts as a Controller and importer. In addition, Annexes to the EU SCCs must be completed in accordance with the applicable module of the EU SCCs. The Annexes are attached hereto as **Schedule 1** and must be completed by the parties if the EU SCCs apply to the Services.

With respect to the EU SCCs, the parties agree that:

a. Clause 7 – Docking Clause, applies;
b. Clause 9 – Use of Subprocessors, option 2 (general written authorization) applies and the designated time period is thirty (30) days;
c. The optional language contained in Clause 11 – Redress, is not applicable;
d. Clause 13(a), if Enterprise is not established in an EU Member State (see Enterprise's address to confirm), then the language applicable to a data exporter without an appointed representative applies;
e. Clause 17 – Governing Law, option 1 shall apply and be completed to reflect the laws of Ireland, but only to the extent the Services are not provided in Germany, in which case the parties agree that the laws of Germany shall govern; and
f. Clause 18(b) shall be completed to reflect the courts of Ireland, but only to the extent that Services are not provided in Germany, in which case the courts of Germany shall apply.

With respect to Personal Information transferred from the United Kingdom, the parties agree to the International Data Transfer Addendum, which is attached hereto as **Schedule 2** and must be completed by the parties if the Services contemplate the transfer of Personal Information from the United Kingdom. Each party will promptly notify the other in writing if it can no longer comply with the EU SCCs or this DPA. A party shall not be required to provide specific information about why it can no longer comply if providing such information is prohibited by Applicable Data Protection Laws.

With respect to Personal Information transferred from The People's Republic of China, each party agrees to the Standard Contract for Overseas Transfer of Personal Information issued by the Cyberspace Administration of China ("***SCOTPI***"). SCOTPI forms part of this DPA, and takes precedence in the event of a conflict with this DPA. SCOTPI can be found on the Office of the Central Cyberspace Affairs Commission's website at cac.gov.cn. In addition, **Schedule 3** must be completed by the parties if SCOTPI applies.

10. Security: Each party shall implement and maintain throughout the term of this DPA, or for as long as the party remains in possession of Confidential Information, appropriate technical and organizational security measures to protect Confidential Information, including protection against Data Breaches. Such security measures shall include, at a minimum, the measures specified in Annex II of the EU SCCs. In the event the EU SCCs are not applicable, technical and organizational security measures must be in accordance with Applicable Data Protection Laws and highest industry standards.

11. Data Breach: Upon discovery of a Data Breach, a party shall immediately, but no later than 24 hours, inform the other party in writing of the Data Breach and timely provide information describing the Data Breach as it becomes known or as otherwise reasonably requested. The party who sustained the Data Breach shall undertake all measures and actions necessary to remedy or mitigate the effects of the Data Breach and shall keep the other party updated on all developments. The parties shall provide assistance in relation to any notifications required by Applicable Data Protection Laws. All costs and/or expenses incurred as a result of the Data Breach shall be borne solely by the party who sustained the Data Breach.

12. Deletion or Return of Data: Upon termination or expiration of the Agreement, each party shall, upon request of the other, destroy or return all Confidential Information in the other party's possession or control (including any Confidential Information provided to a Controller, Processor, or Subprocessor for Processing). This requirement shall not apply to the extent that a party is required by Applicable Data Protection Laws to retain some or all of the Confidential Information, in which event such Confidential Information shall be isolated and protected in accordance with this DPA.

13. Indemnity: Each party shall defend, indemnify, and hold harmless the other party, its customers, officers, directors, employees, agents, representative and affiliates from and against all losses, claims, costs, harms, expenses (including reasonable legal fees and expenses), liabilities or damages suffered or incurred as a result of a Data Breach, breach of this DPA and/or Applicable Data Protection Laws.

14. Audit: Each party shall permit the other, or its appointed third-party auditors, to audit a party's compliance with this DPA and Applicable Data Protection Laws. Each party shall make available all information, facilities, systems and staff necessary to conduct such audit. Each party acknowledges that the other party, or its third-party auditors, may enter a party's premises for the purposes of conducting this audit, provided that there is reasonable prior notice of an intention to audit, the audit is conducted during normal business hours, and all reasonable measures are taken to prevent unnecessary disruption to operations. Upon reasonable request, each party may be required to demonstrate compliance with this DPA by completing security questionnaires, or by providing security policies or summaries of assessments with industry standards (such as ISO 27001, SOC II), penetration testing, and/or vulnerability scans.

15. Miscellaneous: If there is a conflict between any provision in this DPA and any provision in the Agreement, this DPA shall take precedence. The duration of a party's Processing of Confidential Information will be limited to the term of the Agreement; provided, however, that this DPA shall survive termination or expiration of the Agreement for as long as Confidential Information remains in a party's or its Controllers', Processors', or Subprocessors' care, custody, and control.

COMPANY ACKOWLEDGES AND AGREES THAT COMPANY HAS AN OBLIGATION TO COMPLY WITH APPLICABLE LAW AND PROVIDE ENTERPRISE WITH ALL INFORMATION THAT IS NECESSARY FOR SUCH COMPLIANCE. COMPANY FURTHER ACKNOWLEDGES AND AGREES THAT COMPANY, REGARDLESS OF WHETHER COMPANY OR ENTERPRISE SIGNS THIS DPA, WILL BE BOUND BY THE TERMS AND CONDITION OF THIS DPA UPON COMPANY'S ACCEPTANCE OF SERVICES FROM ENTERPRISE.

ENTERPRISE **COMPANY**
(REENTER SUDDATH/STRLX ENTITY INFORMATION LISTED IN FIRST PARAGRAPH OF DPA)

Signature: _____ Signature: _____

Printed Name: _____ Printed Name: _____

Title: _____ Title: _____

And, as applicable:

ENTERPRISE **(IF ADDITIONAL SUDDATH/STRLX ENTITIES ARE ENTERING INTO DPA, INCLUDE INFORMATION HERE)**

ENTER SUDDATH/STRLX ENTITY NAME

Signature: _____

Printed Name: _____

Title: _____

Address:_____

SCHEDULE 1

ANNEX I

A. LIST OF PARTIES (Must be completed)

Data exporter(s):

Name: Click or tap here to enter text.

Address: Click or tap here to enter text.

Contact person's name, position and contact details: Click or tap here to enter text.

Activities relevant to the data transferred under these Clauses:

Signature: _____

Date: _____

Role (controller/processor):

Data importer(s):

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: Click or tap here to enter text.

Signature: _____

Date: _____

Role (controller/processor):

B. DESCRIPTION OF TRANSFER (Must be completed)

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 (Must be completed if Module One, Two, or Three Apply)

MODULE ONE: Transfer Controller to Controller (i.e., one party acts as the Controller and exporter, and the other acts as a Controller and importer)
MODULE TWO: Transfer Controller to Processor (i.e., one party acts as the Controller and exporter, and the other acts as a Processor and importer)
MODULE THREE: Transfer Processor to Processor (i.e., one party acts as the Processor and exporter, and the other acts as a Subprocessor and importer)

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2
D02 RD28
Ireland

The Federal Commissioner for Data Protection and Freedom of Information shall be the Competent Supervisory Authority for those services provided in Germany
Graurheindorfer Str. 153
53117 Bonn
Germany

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA (Must be completed if Module One, Two, or Three apply)

MODULE ONE: Transfer Controller to Controller (i.e., one party acts as the Controller and exporter, and the other acts as a Controller and importer)

MODULE TWO: Transfer Controller to Processor (i.e., one party acts as the Controller and exporter, and the other acts as a Processor and importer)

MODULE THREE: Transfer Processor to Processor (i.e., one party acts as the Processor and exporter, and the other acts as a Subprocessor and importer)

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorization

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimization

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure

]

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III

LIST OF SUB-PROCESSORS (Must be completed if Module Two or Three apply)

MODULE TWO: Transfer Controller to Processor (i.e., one party acts as the Controller and exporter, and the other acts as a Processor and importer)

MODULE THREE: Transfer Processor to Processor (i.e., one party acts as the Processor and exporter, and the other acts as a Subprocessor and importer)

1. Name:

   Address:

   Contact person's name, position and contact details:

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

2. Name:

   Address:

   Contact person's name, position and contact details:

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

SCHEDULE 2

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("***Addendum***"). **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

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):	Full Name (optional): Job Title: Contact details including email:
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

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

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

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 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, re-enacted 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, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
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. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";
    j. Clause 13(a) and Part C of Annex I are not used;
    k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";
    l. In Clause 16(e), subsection (i) is replaced with: *"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";*
    m. Clause 17 is replaced with: *"These Clauses are governed by the laws of England and Wales.";*
    n. Clause 18 is replaced with: *"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.";* and
    o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

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

19. 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.

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

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

SCHEDULE 3

INSTRUCTIONS FOR OVERSEAS TRANSFER OF PERSONAL INFORMATION (Must be completed if SCOTPI **applies)**
The details of Personal Information to be transferred overseas in accordance with this DPA are as follows:

Purpose of processing: [ ]

Means of processing: [ ]

Scale of overseas transfer of Personal Information: [ ]

Categories of transferred Personal Information: [ ]

Categories of Sensitive Personal Information transferred: [ ]
Please note that the definition and scope of Sensitive Personal Information under the Chinese law are different from those under the GDPR. Please refer to GB/T 35273 Information Security Technology — Personal Information Security Specification for guidance.

The Overseas Recipient only provides Personal Information to the following third parties outside the People's Republic of China (if applicable): [ ]

Method of transmission: [ ]

Period of retention after overseas transfer: [ ]

Place of storage after overseas transfer: [ ]

Miscellaneous (fill in as required): [ ]