Customer Master Data Protection Agreement

This Customer Master Data Protection Agreement (**"MDPA"**), forms part of the Agreement (as defined below), and applies where, and to the extent that, Cisco processes Personal Data as a Processor for Customer when providing Products and/or Services (as defined below) under the Agreement (each a "**Party**" and together the "**Parties**").

Unless otherwise specified in this MDPA, the terms of the Agreement shall continue in full force and effect. All capitalized terms not defined in this MDPA shall have the meanings set forth in the Agreement. Any privacy or data protection related clauses or agreement previously entered into by Cisco and Customer, shall be superseded and replaced with this MDPA.

1. Definitions

1.1. **"Affiliates"** means companies within the Cisco group that may Process Customer Personal Data in order to provide the Products and/or Services. Such Affiliates include Cisco Systems, Inc., Cisco Commerce India Private Limited, Cisco Systems G.K., Cisco Systems Australia Pty Limited, Cisco Systems Canada Co., Cisco International Limited, Cisco Systems (Italy) S.R.L., Cisco Systems International B.V., ThousandEyes LLC, Broadsoft, Inc., AppDynamics LLC, AppDynamics International Ltd. and Meraki LLC. Unless otherwise explicitly agreed by the Parties, any legal entities which become part of the Cisco group of companies through an acquisition or merger are not considered Affiliates for the purposes of this MDPA.

1.2. **"Agreement"** means the written or electronic agreement between Customer and applicable Cisco entity for the provision of the Services and/or Products to Customer or any other terms where the parties expressly agree to this document (e.g.: the Cisco End User License Agreement ("**EULA**")).

1.3. **"APEC"** means the Asia Pacific Economic Cooperation, a regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific. See www.apec.org for more information.

1.4. **"APEC Member Economy"** means the 21 members of APEC: Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong-China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States, and Vietnam.

1.5. **"Approved Jurisdiction"** means a member state of the EEA, or other jurisdiction approved as having adequate legal protections for data by the European Commission, currently found here: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

1.6. **"Cisco"** means the applicable Cisco entity that is party to the Agreement and its Affiliates.

1.7. **"Controller"** means an entity that determines the purposes and means of the processing of Personal Data.

1.8. **"Customer"** means the Party identified in the Agreement receiving Services and/or Products from Cisco under the Agreement**.**

1.9. **"Data Breach"** means a breach of Security Measures leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data.

1.10. **"Data Protection Laws"** means all mandatory applicable laws that apply to the Processing of Personal Data under the Agreement.

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

1.12. **"EEA"** means those countries that are members of European Free Trade Association (**"EFTA"**), and the then-current, post-accession member states of the European Union.

1.13. **"GDPR"** means Regulation 2016/679 of the European Parliament and of the Council 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).

1.14. **"Personal Data"** means any information about, or related to, an identifiable individual Processed on behalf of the Customer. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual, natural person.

1.15. **"Privacy Data Sheet(s)"** means the applicable document located on Cisco's Trust Portal that describes the Processing activities in relation to the Service(s) supplied to Customer under the Agreement.

1.16. **"Processing"** means any operation or set of operations that is performed upon Personal Data, whether or not by automatic means, such as collection, recording, securing, organization, storage, adaptation or alteration, access to, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction. "**Processes**" and "**Process**" shall be construed accordingly.

1.17. **"Processor"** means an entity that processes Personal Data on behalf of a Controller.

1.18. **"Product"** means Cisco branded hardware and software offering purchased by Customer.

1.19. **"Representatives"** means either Party including its Affiliates' officers, directors, employees, agents, contractors, temporary personnel, subcontractors and consultants.

1.20. **"Security Measures"** means the technical and organizational measures designed to protect the Personal Data as set forth in Attachment A.

1.21. **"Special Categories of Personal Data"** means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, certain financial information when identified as such by mandatory applicable law, precise geolocation over time and data related to offenses or criminal convictions.

1.22. **"Service"** means Cisco branded service offering purchased by Customer.

1.23. **"Standard Contractual Clauses"** means the agreement set forth in Attachment B as approved by the European Commission for the transfer of Personal Data to Processors established in third countries which do not ensure an adequate level of data protection and any subsequent changes approved by the European Commission with an official decision.

1.24. **"Subprocessor"** means another Processor engaged by Cisco to carry out Processing of Customer's Personal Data.

2. Obligations of the Parties

2.1. The Parties agree that, for this MDPA, Customer shall be the Controller and Cisco shall be the Processor.

2.2. Customer shall:

a. use the Products and/or Services in compliance with Data Protection Laws;

b. ensure all instructions given by it to Cisco in respect of the Processing of Personal Data are at all times in accordance with Data Protection Laws;

c. ensure all Personal Data provided to Cisco has been collected in accordance with Data Protection Laws and that Customer has all authorizations and/or consents necessary to provide such Personal Data to Cisco; and

d. keep the amount of Personal Data provided to Cisco to the minimum necessary for the provision of the Products and/or Services.

2.3. Cisco shall:

a. only Process the Personal Data in accordance with Customer's documented instructions, the applicable Privacy Data Sheet(s), Annex 1 to the Standard Contractual Clauses (where applicable) and this MDPA. Cisco will promptly notify Customer if Cisco reasonably believes that Customer's instructions are inconsistent with Data Protection Laws;

b. ensure its applicable Representatives who may Process Personal Data have written contractual obligations in place with Cisco to keep the Personal Data confidential;

c. appoint data protection lead(s). Upon request, Cisco will provide the contact details of the appointed person(s);

d. assist Customer as reasonably needed to respond to requests from supervisory authorities, Data Subjects, customers, or others to provide information related to Cisco's Processing of Personal Data;

e. if required by Data Protection Laws, court order, subpoena, or other legal or judicial process to Process Personal Data other than in accordance with Customer's instructions, notify Customer without undue delay of any such requirement before Processing the Personal Data (unless mandatory applicable law prohibits such notification, in particular on important grounds of public interest);

f. only Process Personal Data on its systems or facilities to the extent necessary to perform its obligations under the Agreement;

g. where applicable, act as a subprocessor of such Personal Data;

h. maintain records of the Processing of any Personal Data received from Customer under the Agreement;

i. not lease, sell, distribute, or otherwise encumber Personal Data unless mutually agreed to by the Parties in a separate agreement;

j. provide such assistance as Customer reasonably requires (either on its own behalf or on behalf of its customers), and Cisco or a Representative is able to provide, in order to meet any applicable filing, approval or similar requirements in relation to Data Protection Laws;

k. provide such information and assistance as Customer reasonably requires (taking into account the nature of Processing and the information available to Cisco) to enable compliance by Customer with its obligations under Data Protection Laws with respect to:

   i. security of Processing;

   ii. data protection impact assessments (as such term is defined by the GDPR);

   iii. prior consultation with a supervisory authority regarding high-risk Processing; and

   iv. notifications to the applicable supervisory authority and/or communications to Data Subjects by Customer in response to any Data Breach;

l. on termination of the MDPA for whatever reason, cease to Process Personal Data, and upon Customer's written request and without undue delay, (i) return, or make available for return, Personal Data in its possession or control, or (ii) securely delete or permanently render unreadable or inaccessible existing copies of the Personal Data; unless continued retention and Processing is required or is permitted by Data Protection Laws and/or mandatory applicable law. At Customer's request, Cisco shall give Customer confirmation in writing that it has fully complied with this Section 2.3 (k.iv) or provide a justification as to why such compliance is not feasible.

3. Transfers of Personal Data

3.1. Transfers of Personal Data from EEA or Switzerland to third countries**.** Where Cisco Processes Personal Data from the EEA or Switzerland on behalf of Customer, in a country which is not an Approved Jurisdiction, Cisco shall perform such Processing in accordance with the Standard Contractual Clauses set forth in Attachment B to this MDPA and/or in accordance with Articles 44 to 49 of the GDPR.

3.2. Transfers of Personal Data from the UK to third countries**.** Where Cisco Processes Personal Data from the UK in a third country, such Processing shall be performed in accordance with Attachment B, as amended by the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses included in Attachment C (the **"Addendum"**). Any further changes to this Addendum approved with an official decision by the Information Commissioner's Office will be incorporated by reference and a copy of the new Addendum will be available on the Cisco Trust Center.

3.3. Transfers of Personal Data from jurisdictions other than the EEA, Switzerland or UK to third countries**.** For jurisdictions other than the EEA or Switzerland, Cisco shall not transfer Personal Data outside of the jurisdiction where the Personal Data is obtained unless permitted under Data Protection Laws. Where Cisco Processes Personal Data from an APEC Member Economy on behalf of Customer, Cisco shall perform such Processing in a manner consistent with the APEC Cross Border Privacy Rules Systems requirements ("**CBPRs**") (see www.cbprs.org) to the extent the requirements are applicable to Cisco's Processing of the Personal Data. If Cisco is unable to provide the same level of protection as required by the CBPRs, Cisco shall promptly notify Customer and cease Processing. In such event, Customer may terminate the Agreement with respect only to those Products and/or Services for which Cisco is unable to provide the same level of protection as required by the CBPRs by written notice within 30 days.

4. Subprocessing

4.1. Cisco shall not subcontract its obligations under this MDPA to new Subprocessors, in whole or in part, without providing Customer with notice (for example, by publishing this information at Cisco's Trust Portal or by e-mail or in-application messaging) and an opportunity to object. If Customer objects to the proposed subcontracting on reasonable grounds related to the protection of the Personal Data and the Parties cannot resolve the objection, the Customer may terminate the applicable part of the Agreement with respect only to those Products and/or Services which cannot be provided by Cisco without the use of the objected Subprocessors by giving written notice to Cisco.

4.2. Where Cisco appoints a Subprocessor, Cisco will execute a written agreement with the Subprocessor(s) containing terms at least as protective as this MDPA.

4.3. Cisco shall be liable for the acts or omissions of Subprocessors to the same extent it is liable for its own actions or omissions under this MDPA.

4.4. For the purposes of Clause 9 of the Standard Contractual Clauses, Customer provides a general consent to Cisco to engage Subprocessors. Such consent is conditional on Cisco's compliance with Section 4 of this MDPA.

5. Rights of Data Subjects

Data Subject requests**.** Cisco shall, to the extent legally permitted, promptly redirect the Data Subjects to send their requests to the Customer or notify Customer if it receives a request from a Data Subject for access to, rectification, portability, objection, restriction or erasure of such Data Subject's Personal Data. Unless required by Data Protection Laws, Cisco shall not respond to any such Data Subject request without Customer's prior written consent except to redirect the Data Subject to the Customer. Cisco shall provide such information and cooperation and take such action as the Customer reasonably requests in relation to a Data Subject request.

6. Security

Controls for the Protection of Personal Data**.** Cisco shall implement and maintain appropriate technical and organizational measures designed to protect the Personal Data as set forth in the Security Measures. Cisco regularly monitors compliance with these Security Measures.

7. Audit

7.1. Cisco shall make available to the Customer such information as is reasonably necessary to demonstrate Cisco's compliance with the obligations of this MDPA in accordance with the terms of the Security Measures.

7.2. Customer acknowledges and agrees that any exercise of its audit rights under Clause 8.9 of the Standard Contractual Clauses will be conducted in accordance with this MDPA.

8. Notification and Communication

8.1. Notification**.** Cisco shall notify Customer within 48 hours of confirmation of a Data Breach relating to Customer's Personal Data. Cisco shall provide all such timely information and cooperation as Customer may reasonably require in order for Customer to fulfil its Data Breach reporting obligations under (and in accordance with the timescales required by) Data Protection Law. Cisco shall further take such measures and actions as it considers necessary or appropriate to remedy or mitigate the effects of the Data Breach and shall keep Customer informed in connection with the Data Breach.

8.2. Information Security Communication**.** Except as required by mandatory applicable law, Cisco agrees that it will not inform any third party of a Data Breach referencing or identifying the Customer, without Customer's prior written consent. Cisco shall reasonably cooperate with Customer and law enforcement authorities concerning a Data Breach. Cisco shall retain, for an appropriate period of time, all information and data within Cisco's possession or control that is directly related to any Data Breach. If disclosure of the Data Breach referencing or identifying the Customer is required by mandatory applicable law, Cisco will work with Customer regarding the timing, content, and recipients of such disclosure.

8.3. Post-incident**.** Cisco shall reasonably cooperate with Customer in any post-incident investigation, remediation, and communication efforts.

8.4. Complaints or notices related to Personal Data**.** If Cisco receives any official complaint, notice, or communication that relates to Cisco's Processing of Personal Data or either Party's compliance with Data Protection Laws in connection with Personal Data, to the extent legally permitted, Cisco shall promptly notify Customer and, to the extent applicable, Cisco shall provide Customer with commercially reasonable cooperation and assistance in relation to any such complaint, notice, or communication. Customer shall be responsible for any reasonable costs arising from Cisco's provision of assistance in relation to any official complaint, notice, or communication that relates to Customer's compliance with Data Protection Laws.

9. General

9.1. Except for any liability which cannot be limited or excluded under mandatory applicable law, the aggregate liability of Cisco for all Data Breaches and any breach of this MDPA (whether for breach of contract, misrepresentations, negligence, strict liability, other torts or otherwise) shall not exceed US$1,000,000.

9.2. Where a Data Breach and/or breach of this MDPA is also a breach of any confidentiality or non-disclosure obligations in the Agreement, the liability cap in Section 9.1 will apply.

9.3. Nothing in this MDPA is intended to limit the Parties' direct liability towards data subjects or applicable supervisory data protection authorities which cannot be limited under mandatory applicable law.

9.4. No one other than a Party to this MDPA, their successors and permitted assignees shall have any right to enforce any of its terms.

9.5. This MDPA will remain in force for the term of Agreement.

Attachment A

Security Measures

Information Security Exhibit can be found on the following direct link: https://trustportal.cisco.com/c/r/ctp/trust-portal.html#/1604543381171981.

Attachment B

Standard Contractual Clauses (controller to processor)

COMMISSION IMPLEMENTING DECISION (EU) 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

(Text with EEA relevance)

For purposes of this Attachment B: any reference to “data exporter” means Customer, acting as data exporter on behalf of its EEA or Swiss customer(s) where applicable, and any reference to “data importer” means Cisco each a “**party**”; together “**the parties**”.

The parties have agreed on the following Standard Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Annex 1.

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 personal 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 1.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 1.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 1.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 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3 (b);
   iii. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
   iv. Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
   v. Clause 13;
   vi. Clause 15.1(c), (d) and (e);
   vii. Clause 16(e);
   viii. Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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 1.B.

Clause 7
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 1.A.

b. Once it has completed the Appendix and signed Annex 1.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 1.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.

MODULE TWO: Transfer controller to processor

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 1.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 2 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 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 1.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 2. 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 1.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:

a. 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;

b. 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;

c. 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

d. 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

MODULE TWO: Transfer controller to processor

a. GENERAL WRITTEN AUTHORISATION 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 30 days 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

MODULE TWO: Transfer controller to processor

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 2 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.

MODULE TWO: Transfer controller to processor

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

MODULE TWO: Transfer controller to processor

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

MODULE TWO: Transfer controller to processor

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 1.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

MODULE TWO: Transfer controller to processor

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

MODULE TWO: Transfer controller to processor

15.1. <u>Notification</u>

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. For Modules One, Two and Three: 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

MODULE TWO: Transfer controller to processor

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 the Netherlands.

Clause 18
Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

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 the Netherlands.

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.

____

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

____

Annex 1 To Attachment B

The Standard Contractual Clauses

This Annex 1 forms part of the Clauses.

A. List of Parties

Data exporter

The data exporter is Customer, acting as data exporter on behalf of itself or a customer where applicable. Activities relevant to the transfer include the performance of services for Customer and its customer(s).

Data importer

The data importer is Cisco. Activities relevant to the transfer include the performance of services for Customer and its customer(s).

B. Description of transfer

1. Categories of data subjects whose personal data is transferred

The personal data transferred may concern the following categories of data subjects: Employees, contractors, business partners, representatives and end customers of the Customer, and other individuals whose personal data is processed by or on behalf of Customer or Customer's customers and delivered as part of the Services and Products.

2. Categories of personal data transferred

The personal data transferred may concern the following categories of data:

Personal data related directly or indirectly to the categories of data subjects listed above, including online and offline customer, prospect, and partner data, and personal data provided by or on behalf of the Customer or its users of the Services and Products. More detailed categories of personal data are reflected for certain Services and Products in Cisco's Privacy Data Sheets available at https://trustportal.cisco.com.

3. 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.

Unless data exporter or its users use data importer's products and services to transmit or store sensitive data, data importer does not process sensitive data.

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

The Transfer happens on a continuous basis.

5. Nature of Processing

Personal data will be subject to processing activities such as storing, recording, using, sharing, transmitting, analyzing, collecting, transferring, and making available personal data. More details on Cisco's processing activities of personal data are reflected for certain Services and Products in Cisco's Privacy Data Sheets available at https://trustportal.cisco.com.

6. Purpose(s) of the data transfer and further processing

The personal data transferred may be subject to the following basic processing activities, as may be further set forth in contractual agreements entered into from time to time between Cisco and Customer: (a) customer service activities, such as processing orders, providing technical support and improving offerings, (b) sales and marketing activities as permissible under mandatory applicable law, (c) consulting, professional, security, storage, hosting and other services delivered to Customer, and (d) internal business processes and management, fraud detection and prevention, and compliance with governmental, legislative, and regulatory requirements. More detailed purposes for Cisco's processing of personal data are reflected for certain Services and Products in Cisco's Privacy Data Sheets available at https://trustportal.cisco.com.

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

Personal data will be retained as needed to fulfill the purposes for which it was collected, such as delivery of the Services and Products, and as necessary for Cisco to comply with its business requirements, legal obligations, resolve disputes, protect its assets, and enforce its rights and agreements.

Specific data retention periods for Cisco's processing of personal data are reflected for certain Services and Products in Cisco's Privacy Data Sheets available at https://trustportal.cisco.com.

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

Personal data will be transferred to Cisco's sub-processors as described in the applicable Service's or Product's Privacy Data Sheets available at https://trustportal.cisco.com.

C. Competent Supervisory Authority

It is competent supervisory authority/ies in accordance with Clause 13 with responsibility for ensuring compliance by the data exporter.

Annex 2 To Attachment B

The Standard Contractual Clauses

Annex 2 to Attachment B, the Standard Contractual Clauses, is the Information Security measures located in Attachment A.

Annex 3 To Attachment B

List of Sub-processors

The controller has authorised the use of the sub-processors listed in the applicable Cisco Privacy Data Sheet published on Cisco's Trust Portal at https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=Privacy%20Data%20Sheet|Privacy%20Data%20Map.

Should Customer obtain additional Products and/or Services governed under the Agreement, whereby Cisco may process Personal Data on behalf of Customer, the applicable Privacy Data Sheets, as available on Cisco Trust Portal will apply and will be incorporated herein by reference.

Attachment C

UK 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	As of the Effective Date of the MDPA	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Customer	Cisco

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 the MDPA - Reference: Approved EU SCCs enclosed in Attachment B to the MDPA above

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 out in Annex 1 to Attachment B, section A (List of Parties)

Annex 1B: Description of Transfer: as set out in Annex 1 to Attachment B, section B (Description of transfer)

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

Annex III: List of Sub processors (Modules 2 and 3 only): as set out in Annex 3 to Attachment B (List of subprocessors)

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 28 January 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 and enclosed in Attachment B to this MDPA.
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.