RingCentral Customer Data Transfer Agreement Instructions

To complete the RingCentral Customer Data Transfer Agreement ("DTA"), please fill in your organization's information in the open fields:

1) The signature box at the end of the DTA (page 6)
2) Annex I "Description of the Data Exporter" (page 7)
3) Annex I in the table in Section C "Competent Supervisory Authority of the Data Exporter" (page 9) and
4) Exhibit 1 "International Data Transfer Addendum to the EU Commission Standard Contractual Clauses" Table 1 – Parties (page 11)

Once fully signed, please send the executed DTA by email to contractsaudit@ringcentral.com.

This DTA is valid only where there is an existing agreement for RingCentral Services between a RingCentral entity and the customer entity.

RingCentral Customer Data Transfer Agreement

This Data Transfer Agreement (**"DTA"**) is made by and between RingCentral and/or its Affiliates and Customer and/or its Affiliates (each a "**Party"**, together the **"Parties"**), pursuant to the agreement(s) for the provision of the RingCentral services ("**Services**") to Customer, including any data processing agreement or similar document (together, the "**Agreement**").

1. Scope and Applicability

This DTA is supplemental to the Agreement and sets out the terms that apply to the extent that RingCentral processes (or causes to be processed) any Customer Personal Data originating from the European Economic Area (**"EEA"**), United Kingdom or Switzerland in a country that has not been recognized by the relevant authorities as providing an adequate level of protection for Customer Personal Data.

Capitalized terms used but not defined in this DTA have the same meanings as set out in the Agreement or the Standard Contractual Clauses (defined below), as applicable.

2. Data Privacy Framework

RingCentral complies with and has certified to the U.S. Department of Commerce its adherence to the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) (the "Data privacy Framework"). RingCentral's Notice of Certification applies to the Services.

3. Standard Contractual Clauses

a. To the extent that the Data Privacy Framework does not apply, the Parties are deemed to have accepted and executed the standard contractual clauses as follows (together, "**Standard Contractual Clauses**"):

i. In respect of EU Personal Data, the standard contractual clauses pursuant to the European Commission's decision (EU) 2021/914 of 4 June 2021 (Commission Implementing Decision (EU) 2021/914 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 (published at https://eurlex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN), including the text from Module Two of such clauses but not including any clauses marked as optional ("**EU Standard Contractual Clauses**") which the parties expressly agree to incorporate by this reference to the DTA. For the purposes of this DTA, "**EU Personal Data**" means the personal data to which data protection laws of the European Union are applicable; and

ii. In respect of UK Personal Data, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (Version B1.0, in force 21 March 2022 or any other then-current version), attached hereto as Exhibit 1, including in "Table 2: Selected SCCs, Modules and Selected Clauses" the reference to the EU Standard Contractual Clauses described in (i) above, (together, the EU Standard Contractual Clauses and the International Data Transfer Addendum shall be referred to as the "**UK IDTA**"). For the purposes of this DTA, "**UK Personal Data**" means the personal data to which data protection laws of the United Kingdom are applicable; and

iii. In respect of Swiss Personal Data, the EU Standard Contractual Clauses as deemed amended by this DTA (the "**Swiss Standard Contractual Clauses**"), provided that any

references in the clauses to the GDPR shall refer to the Federal Act on Data Protection ("**FADP**"), the term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with clause 18(c) of the clauses, and the clauses shall also protect the data of legal persons until the entry into force of the revised FADP. For the purposes of this DTA, "**Swiss Personal Data**" means the personal data to which data protection laws of Switzerland are applicable.

The Standard Contractual Clauses are deemed to be completed with the information provided in this DTA and, in particular, the Annexes I and II to this DTA.

b. In the event of any contradiction between the Standard Contractual Clauses and this DTA, the provisions of the Standard Contractual Clauses shall prevail.

c. The parties agree that the Standard Contractual Clauses form an integral part of this DTA and that by entering into this DTA the parties are bound by the Standard Contractual Clauses as set out in this DTA.

4. Audit

a. Both parties acknowledge that it is the parties' intention ordinarily to rely on the provision of the security reports at Section 3.7 of the Data Processing Agreement between the Parties to verify RingCentral's compliance with this DTA.

b. Additionally, upon request from Customer, but not more than once during each 12-month period, RingCentral shall complete a Customer provided information security program questionnaire, limited in scope to the actual services/environments related to the Services provided to Customer ("**Security Review**").

c. After Customer's review of RingCentral's audit report or similar attestation, and of the completed information security questionnaire (including any changes introduced by RingCentral to address any gaps), if, to the extent required by the GDPR, additional information is reasonably necessary to demonstrate compliance with RingCentral's obligations pursuant to Applicable Data Protection Laws and this DTA, Customer may request in writing to perform an audit (including inspections) of RingCentral pursuant to the audit request procedure below, no more than once every twelve (12) month period, unless a supervisory authority specifically requires that an audit is carried out of RingCentral or in response to a Security Incident.

d. In order to exercise its right to audit pursuant to this section, Customer must provide RingCentral with a written, detailed request, including the explanation of gaps in RingCentral's provided audit reports and in the Security Review that render the audit necessary to demonstrate RingCentral's compliance with this DPA or with applicable law.

e. The audit may be performed by Customer or a third-party auditor (any such third party under strict confidentiality obligations, including requirements that individual auditors appointed have not performed audits of any of RingCentral's competitors in the previous twelve (12) months and that they will be prohibited from performing such audits in the twelve (12) months following RingCentral's audit) solely at Customer's expense. RingCentral may object in writing to any third-party auditor if the auditor is, in RingCentral's reasonable opinion, not suitably qualified or independent, a competitor of RingCentral, or otherwise manifestly unsuitable. Any such objection by RingCentral will require the Customer to appoint another auditor or conduct the audit itself.

f. RingCentral and Customer will agree in advance upon the scope and timing of the audit, to protect the confidential and proprietary Information of RingCentral and other parties, to minimize disruption to RingCentral's business, to limit the scope to the actual services/environments related to the Services provided to Customer, and to agree on a reasonable duration of the audit.

g. The audit performance will occur during regular business hours for the RingCentral personnel involved and the parties agree that RingCentral will make available material for Customer's review, but not for Customer to retain. RingCentral may charge a reasonable fee for costs incurred in connection with any such audit based on RingCentral's professional services rates, unless the audit shows a material breach on the part of RingCentral. RingCentral will provide Customer with details of any applicable fee, and the basis of its calculation, in advance of any such audit.

h. All information provided or made available to Customer pursuant to this section shall be deemed Confidential Information of RingCentral.

5. Subprocessors

For the purposes of Clause 9 "Use of Subprocessors" of the EU Standard Contractual Clauses , including as incorporated into the UK IDTA and as amended for the Swiss Standard Contractual Clauses, it is agreed that "OPTION 2: GENERAL WRITTEN AUTHORISATION" applies. Accordingly:

a. RingCentral acting as data importer has the Customer's (acting as data exporter) general authorisation for the engagement of sub-processor(s) from an agreed list and the data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of subprocessors at least thirty (30) calendar days in advance. If the Customer objects to the appointment of an additional Subprocessor within thirty (30) calendar days of such notice on reasonable grounds relating to the protection of the Customer Personal Data, then the parties will discuss such concerns with a view to achieving resolution.

b. If such resolution cannot be reached, then RingCentral will either not appoint the Subprocessor or, if this is not possible, Customer will be entitled to suspend or terminate the affected RingCentral Service without penalty with a thirty (30) day written notice to RingCentral.

c. Notwithstanding the foregoing, in the event of an unforeseeable force majeure (such as a RingCentral Subprocessor failure) that can provoke a degradation or interruption of the Service, RingCentral reserves the right to immediately change the failing Subprocessor to maintain or restore the standard conditions of the Service. In this situation, the notification of Subprocessor change may be exceptionally sent after the change.

d. The Subprocessors engaged by RingCentral in respect of each of the Services at the time of the Agreement are noted on the RingCentral Subprocessor list available at: https://www.ringcentral.com/legal/dpa-subprocessor-list.html.

6. Supplementary Measures

a. RingCentral warrants and represents that it shall use its best efforts to make Customer aware of any changes to the information that it has provided to the Customer under clause 14c of the EU Standard Contractual Clauses and shall advise Customer without undue delay of any changes to such information.

b. RingCentral warrants and represents that:

i. It has not purposefully created back doors or similar programming that could be used to access the personal data processed in connection with this DTA.

ii. It has not purposefully created or changed its business processes in a manner that facilitates access to such personal data.

c. RingCentral agrees to:

i. Provide the notification under clause 15.1 of the EU Standard Contractual Clauses before access is granted to personal data.

ii. Monitor any legal or policy developments that might lead to its inability to comply with its obligations under this DTA and promptly inform the Customer of any such changes and developments, if possible, ahead of their implementation.

d. If RingCentral receives a request for the disclosure of personal data processed in connection with this DTA from a public authority in a third country, the RingCentral shall:

i. Inform the requesting public authority of any incompatibility of the order with the safeguards contained in the Standard Contractual Clauses and the resulting conflict of obligations for RingCentral.

ii. Notify as soon as possible the Customer insofar as possible under the third country legal order.

7. Governing Law and Jurisdiction

The law and forum that apply to the Standard Contractual Clauses are as follow:

	EU Standard Contractual Clauses	**Swiss Standard Contractual Clauses**	**UK IDTA**
Applicable law	France	France	England and Wales
Forum	France	France	England and Wales

This DTA (as distinct from the Standard Contractual Clauses) shall be subject to the law and forum agreed in the Agreement referenced herein, if the law designated in the Agreement is (a) either a law of an EU or EEA member state, the laws of England and Wales or the law of Switzerland, and (b) excluding the respective conflict of law provisions and (c) the choice of forum is within one of the countries listed in (a). In any other case the governing law for this DTA shall be French law and the forum shall be the French Court.

8. Liability

Any limitations of liability that apply to the Agreement also apply, as between Customer and RingCentral, for purposes of the Standard Contractual Clauses and this DTA.

ANNEX I – Information required for Annex I of the EU Standard Contractual Clauses and Swiss Standard Contractual Clauses / Table 3: Appendix Information of the UK IDTA

Description of the Data exporter

Name:
Address:
Contact Details:

The relevant activities of the data exporter are as set out in the Agreement.

Role (controller/processor): Controller

Description of the Data importer

RingCentral, Inc.
20 Davis Drive, Belmont CA 94002 - USA
Privacy@RingCentral.com

The relevant activities of the data importer are as set out in the Agreement.

Role (controller/processor): Processor

Categories of data subjects whose personal data is transferred

- Customer's employees and authorized users who use the Services in connection with the business of the Customer.
- Any other individuals who are involved in or referred to in the content of communications or collaborations taking place through the Customer's use of the Services.
- Any other users of the Services.

Categories of personal data transferred

As applicable to the Services, the categories of Customer Personal Data processed may include, but are not limited to:

- Service account data which may comprise any of the following: name; telephone number; email address; physical address; title; role; profile information; application settings, login credentials (e.g., user ID, log in, account, passwords);
- Usage data which may comprise any of the following: device information (e.g., IP address, ISP, device and operating system type, operations system and client version, client version, type of microphone or speakers, connection type and related information, etc.); connection type and related information (e.g., connected over WiFi); system logs, including usage logs, backend logs, client logs; cookie identifiers; communications metadata, including Call Detail Records (CDRs) and traffic data;
- User generated content which may comprise any of the following: participants' names or phone numbers; chat messages; text of inbound and outbound faxes; voicemails; text of inbound and

outbound SMS; meetings notes; audio/video streams in transit; meeting or call recordings; content of contact center interactions (e.g., emails, social media posts, call recordings, chat, etc.); transcriptions of recorded calls or meetings; summaries of recorded calls or meetings; meeting history; shared files, pictures, and links; message attachments, such as notes, tasks, events, code snippets, and .gifs; folder creations; search history; online presence and status messages; user feedback;

- Any other type of Personal Data as needed for the performance of the Services.

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 Services are not designed to recognize and/or classify data as special categories of data or sensitive data (as defined in the GDPR or in other Applicable Data Protection Laws),

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

The personal data is transferred on a continuous basis where required for the provision of the Service.

Nature of the processing

RingCentral processes Customer Personal Data for the purposes of providing and maintaining the Services to which the Customer has subscribed, including any ancillary or related Services under the scope of the Agreement, which may include collection, storage, transmission, recording, transcription, publishing, displaying; retrieval; consultation; combination; structuring; adaptation.

Purpose(s) of the data transfer and further processing

The purpose of the processing activities carried out by RingCentral is the provision of any of the following:

- Cloud-based communications and collaboration services for high-definition voice, video, SMS, chat messaging and collaboration, conferencing, online meetings, and fax
- Customer contact center services and an omni-channel customer communication management platform that unifies all customer-facing communication channels, including voice, email, SMS, website, mobile app, chat and social media communications, onto a single platform, enabling community responses to customer service inquiries
- Virtual events and presentation services
- Professional services
- Any other Services as specified in the Agreement unless otherwise governed by specific data protection terms

Where all of the above are as described in the Agreement.

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

The criteria used to determine the period of retention for Customer Personal Data is: the term of the Agreement plus 30 days unless otherwise required by law or authorized by the parties.

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

For sub-processors that provide support:

- The nature of the processing is access and use.
- The subject matter of the processing is support and trouble-shooting.
- The duration of the processing is only for as long as necessary to resolve a support request by a Customer.

For sub-processors that provide product features:

- The nature of the processing may include but is not limited to: collection, recording, organization, storage, use, disclosure, erasure, augmentation, enrichment, transmission.
- The subject matter of the processing is engineering, product development, operations, and support and trouble-shooting.
- The duration of the processing for engineering, product development and operations is only for as long as the Customer uses the Services, and for support and trouble-shooting the duration of the processing is only for as long as necessary to resolve a support request by a Customer.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority for each Data Exporter is:

	EU Standard Contractual Clauses	**Swiss Standard Contractual Clauses**	**UK IDTA**
Competent supervisory authority	Competent authority for the data exporter:	For the purposes of Annex I.C under Clause 13: 1. If the data transmission is exclusively subject to the FADP: Federal Data Protection and Information Commissioner (**FDPIC**). 2. If the data transfer is subject to both the FADP and the GDPR: a) FDPIC, insofar as the data transfer is governed by the FADP. b) CNIL insofar as the data transfer is governed by the GDPR.	The Information Commissioner for the United Kingdom

ANNEX II – Information required for Annex II of the EU Standard Contractual Clauses and Swiss Standard Contractual Clauses / Table 3: Appendix Information of the UK IDTA

RingCentral's technical and organizational measures are described in the RingCentral Security Addendum.

Technical and organisational measures implemented pursuant to Clause 10 "Data Subject Rights" of the EU Standard Contractual Clauses (Module Two):

It is the Customer's responsibility to respond to any data subject request. Some of the RingCentral Services may provide direct technical means to enable Customer to fulfil its duties to respond to requests from data subjects under Applicable Data Protection Laws. If Customer is unable to address the data subject's request through such technical means, or where such functionality is not available, RingCentral shall, taking into account the nature of the processing, provide reasonable assistance to Customer, to enable Customer to respond to such data subject requests.

EXHIBIT 1

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date		
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: **RingCentral, Inc.** Trading name (if different): Main address (if a company registered address): 20 Davis Drive, Belmont CA 94002, USA Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Chief Privacy Officer Contact details including email: privacy@ringcentral.com
Signature (if required for the purposes of Section 2)	**EXAMPLE ONLY**	**EXAMPLE ONLY**

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 RingCentral Customer Data Transfer Agreement Reference (if any): RingCentral Customer Data Transfer Agreement Other identifier (if any): DTA 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: see Annex I of the RingCentral Customer Data Transfer Agreement.

Annex 1B: Description of Transfer: See Annex I of the RingCentral Customer Data Transfer Agreement.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II of the RingCentral Customer Data Transfer Agreement.
Annex III: List of Sub processors (Modules 2 and 3 only): N/A

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.