<p style="text-align:center">**DATA PROCESSOR AGREEMENT**</p>

These data processor terms (the "**Data Processor Agreement**") form part of the Agreement between You and Dext covering Your use of the Dext Products.

1.   **DEFINITIONS**

1.1.   Defined terms used in this Data Processor Agreement shall have the meanings given to them in Dext's General Terms and Conditions (found here) and in addition, the following words shall have the following meanings:

Approved Jurisdiction	as defined at clause 2.7 of this Data Processor Agreement and as supplemented by any territory or territories where Sub Processors are based.
Data Processing Details	means the information set out at Appendix 1 of this Data Processor Agreement which applies to all Dext Products being procured by You in any Order Confirmation.
Data Protection Legislation	shall mean the Data Protection Act 2018, the Retained Regulation (EU) 2016/679 (UK GDPR) as incorporated under the European Union (Withdrawal Act) 2018 and as amended by The Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit) Regulations 2019, and any other laws or regulations applicable in the United Kingdom, and where applicable to Us in the performance of the Agreement to You, the General Data Protection Regulation (Regulation (EU) 2016/679 (EU GDPR)), in each case as amended or repealed from time to time.
	"personal data", "data subject", "controller", "processor", "process" and "supervisory authority" shall be interpreted in accordance with the GDPR applicable to the laws of England and Wales.
	"Your personal data" shall mean the personal data in Your Customer Data that is processed by Us pursuant to the Agreement.
End Date	as defined at clause 2.15 of this Data Processor Agreement.
GDPR	means, as appropriate, the UK GDPR or EU GDPR.
Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
Revised Instruction	means a request for information sent by Us to You pertaining to whether Your instruction post the End Date remains to delete Your personal data.
Sub Processor	shall mean a processor appointed by Us, as described at clause 2.11 of this Data Processor Agreement.
UK Addendum	means Addendum B.1.0 issued by the UK Information Commissioner's Office in accordance with s119A of the Data Protection Act 2018 set out in Appendix 3 of this Data Processor Agreement as amended from time to time.

1.2.   The notice provisions at clause 9.10 of Schedule 1 of Dext's General Terms and Conditions shall not apply to this Data Processor Agreement. Instead, where there is an obligation to notify in this Data Processor Agreement, an email to the primary contact each party has on file for the other will suffice.

2.   **PROCESSOR CLAUSES**

2.1.   The parties acknowledge that the factual arrangements between them dictate the role of each party in respect of the Data Protection Legislation. Notwithstanding the foregoing, each party acknowledges that the intention is that You will be sharing Your and, to the extent applicable, Your Permitted Users' personal data with Dext in order for Dext to fulfil its obligations under the Agreement and analyse the Customer Data, including Your personal data.

2.2.   In the event that We process Your, and, to the extent applicable, Your Permitted Users' personal data under or in connection with the Agreement, the parties record their intention that We are the processor, and You are the controller of such personal data. The Data Processing Details sets out the subject-matter and duration of the processing of Your personal data, the nature and purpose of the processing, the type of personal data and the categories of data subjects. Subject to clause 2.12 of this Data Processor Agreement, We may amend the Data Processing Details from time to time.

2.3.   Each party shall comply with its obligations under applicable Data Protection Legislation, and You warrant and undertake that You shall not instruct Us to process Your personal data where such processing would be unlawful.

2.4.   You acknowledge that We do not want, nor expect any special category of personal data to be uploaded by You or Permitted Users or Authorised Users and You agree not to (and to ensure that Your Permitted Users or Authorised Users as applicable do not) upload the same. Breach of this clause shall constitute a material breach of Your Agreement with US which may allow Us to terminate the Agreement in accordance with its terms including, without limitation, clause 6.1 of Schedule 1 of Dext's General Terms and Conditions.

2.5.   You also agree that (i) Dext is not acting on Your or any of Your Permitted User or Authorised User's behalf as a Business Associate or subcontractor; (ii) the Dext Products may not be used to store, maintain, process or transmit protected health information ("PHI") and (iii) the Dext Products will not be used in any manner that would require Dext or any of the Dext Products to be compliant with the Health Insurance Portability and Accountability Act of 1996, as amended and supplemented ("HIPAA"). In the preceding sentence, the terms "Business Associate," "subcontractor," "protected health information" or "PHI" shall have the meanings described in HIPAA.

2.6.   Subject to clause 2.2 above, We will also act as controller in respect of Our use of personal data relating to Your Permitted Users and/or Authorised Users solely in relation to Us performing the Agreement.

2.7.   Subject to clause 2.9 and 2.10 below, We shall process Your personal data only in accordance with Your documented instructions and shall not transfer Your personal data outside of the European Union or the UK (the "**Approved Jurisdiction**") without the documented instruction. For the avoidance of any doubt, any configuration of the Dext Products by You (or Us, acting on Your instruction) or Your use of the Dext Products shall

constitute 'written instructions' for the purposes of this Data Processor Agreement and in relation to any transfer as a result of such configuration, We shall have put in place appropriate safeguards to protect Your personal data and ensure that the relevant data subjects have enforceable subject access rights and effective legal remedies as required by the Data Protection Legislation including entering into appropriate clauses with You or Our contractors (as appropriate) including Standard Contractual Clauses as such term is defined in the Data Protection Legislation.

2.8. Where we process personal data in non – Approved Jurisdictions, We shall comply with the EU Commission's Standard Contractual Clauses (annexed to EU Commission Decision 2021/914/EU of 4 June 2021) (the "**EU SCCs**") which shall be entered into and incorporated into the Agreement by this reference, as amended by the UK Addendum. Nothing in the interpretations in this clause 2.8 is intended to conflict with either Yours or Our rights or responsibilities under the EU SCCs and, in the event of any such conflict, the EU SCCs (as amended by the UK Addendum) shall prevail.

2.9. We may process Your personal data other than in accordance with Your documented instructions where required to do so by applicable law provided that (unless prohibited by applicable law on important grounds of public interest) We shall notify You of such legal requirement before such processing.

2.10. We shall ensure that individuals engaged in the processing of Your personal data under the Agreement are subject to written obligations of confidentiality.

2.11. We shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk involved in processing Your personal data pursuant to the Agreement. We shall assist You by appropriate technical and organisational measures in fulfilling Your obligations as controller in relation to the security of processing Your personal data. Our general security measures are set out in clause 4 to this Data Processor Agreement.

2.12. We may engage such other processors ("**Sub Processors**") as We consider reasonably appropriate for the processing of Your personal data in accordance with the terms of the Agreement (including but not limited to in connection with support, maintenance and development, staff augmentation and the use of third-party data centres). Any Sub Processors We currently use are accepted by You, and are as described in Appendix 1 of this Data Processor Agreement. By You entering into the Agreement, You are providing Us with general written authorisation to add a Sub Processor and/or replace or remove a Sub Processor where We deem necessary. You may request a list of Our Sub Processors at any time. We shall ensure that all Sub Processors are bound by contract with Us which include appropriate data processing terms and We shall remain liable for Sub Processors' acts and omissions in connection with the Agreement.

2.13. In the event that any data subject exercises its rights under applicable Data Protection Legislation against You, We shall use reasonable commercial efforts to assist You in fulfilling Your obligations as controller and provide You with a suitable response without undue delay (and in any event within 5 days) following written request from You provided that We may: (a) extend such time period (provided always that We shall use all reasonable endeavours to provide such assistance within a time period to enable You to comply with Your obligations under applicable Data Protection Legislation); and/or (b) charge You on a time and materials basis in the event that We consider, in Our reasonable discretion, that such assistance is onerous, complex, frequent or time consuming. We shall promptly notify You in writing in the event that We receive any request, complaint, notice or other communication direct from a third party or data subject which relates directly or indirectly to the processing of Your personal data.

2.14. Upon discovering We have experienced a Personal Data Breach in respect of Your personal data We shall notify You without undue delay and shall assist You to the extent reasonably necessary in connection with mitigation of the impact of the Personal Data Breach and any notification to the applicable supervisory authority and data subjects, considering the nature of processing and the information available to Us.

2.15. In the event that You consider that the processing of personal data performed pursuant to the Agreement requires a privacy impact assessment or prior consultation with a supervisory authority to be undertaken, following written request from You, We shall use reasonable commercial endeavours to provide relevant information and assistance to You to facilitate such privacy impact assessment or prior consultation. We may charge You for such assistance on a time and materials basis. We shall provide You with a data protection impact assessment upon request, and prior consultations with supervisory authorities, which are required by Article 35 or 36 of the GDPR, in each case solely in relation to the processing of Your personal data by Us.

2.16. Following the earlier of termination or expiry of the Agreement (the "**End Date**"), Your instruction is for Us to delete Your personal data held by Us. Unless We receive a Revised Instruction from You within 10 days of the End Date confirming Your instruction, We may delete Your personal data held by Us. You may, at no additional cost and within that 10-day period following the End Date, choose to have Your personal data returned to You or as otherwise agreed with Us. Where applicable law requires Us to retain all or some of Your personal data, We shall notify You of this lawful requirement.

2.17. Where requested by You, We shall demonstrate Our compliance with the foregoing clauses 2.2 to 2.16 inclusive, and shall allow for and contribute to audits (including inspections) conducted by You or another auditor mandated by You (where such persons are subject to binding obligations of confidentiality) on a frequency of no more than once per annum (save where requested by the relevant supervisory authority) and in accordance with the Audit Conditions.

2.18. In the event that We consider that Your instructions relating to processing of Your personal data under the Agreement infringes Data Protection Legislation We shall inform You as soon as we become aware and You shall reconsider Your instruction considering the Data Protection Legislation and Our reasoning (where such reasoning is provided). We shall not be obliged to process any of Your personal data in relation to such instructions until You notify Us that Your instructions are non-infringing or amend Your instructions to make them non- infringing and notify Us accordingly. Further, where We request the same, You shall sign a waiver provided by Us which will absolve Us of any liability associated with Us following Your processing instruction.

2.19. Without prejudice to any other provision in the Agreement which may apply, You shall for the Licence Term have in place and maintain any and all appropriate consents from the relevant data subjects and or an appropriate lawful basis for processing the personal data of the data subjects affected by the Agreement.

2.20. We shall for the Licence Term use reasonable endeavours to assist You in meeting Your obligations under Articles 32 to 36 (inclusive).

2.21. Where You consider it necessary to amend this Data Processor Agreement as a result of any changes in law relating to the protection or treatment of personal data, You shall notify Us of the same. Thereafter the parties shall act reasonably and in good faith in agreeing appropriate amendments to this Data Processor Agreement to ensure compliance with such law.

2.22. Nothing in these Terms and Conditions is intended to govern the processing of personal data as it relates to personal data collected by Us (or a third party or agent instructed by Us) as an independent controller. For information on how We process personal data as an independent controller, please see Our privacy policy made available on Our website.

2.23. Some of Our Dext Products may have an API, allowing the transfer of data (which may include personal data) to and from a Dext Product to a third-party product ("**Third-Party API**") or a separate Dext Product (only where You have a licence to this separate Dext Product will the API be turned on). Whether a Third-Party API is turned on or off is at Your discretion, where it is turned on, You are authorising Us to share the relevant data through the Third-Party API and where relevant, receive data from the Third-Party API for input into the Dext Product. We are not liable or

responsible for the quality or accuracy of data shared to Us via a Third-Party API. Nor are We liable for what happens to the data once sent outbound via a Third-Party API (the "**Transferred API Data**"). For the avoidance of doubt, the Transferred API Data will be governed by the contract held between You and the relevant third-party.

3. DETAILS OF PROCESSING

3.1. Details of processing are as described in Appendix 1.

4. SECURITY STANDARDS

4.1. We are currently ISO27001 certified, and We undertake to maintain this or a similar certification providing at least the same standards for the Licence Term. ISO27001 certification demands best in class controls across:

4.1.1. Information security policies

4.1.2. Organisation of information security

4.1.3. Human resource security

4.1.4. Asset management

4.1.5. Access control

4.1.6. Cryptography

4.1.7. Physical and environmental security

4.1.8. Operations security

4.1.9. Communications security

4.1.10. System acquisition, development and maintenance

4.1.11. Supplier relationships

4.1.12. Information security incident management

4.1.13. Information security aspects of business continuity management

4.1.14. Compliance; with internal requirements, such as policies, and with external requirements, such as laws

4.2. Nothing in clause 4 to this Data Processor Agreement (or otherwise) shall prevent Us from replacing the ISO27001 certification with a certification of equivalent or enhanced standing.

APPENDIX 1: DETAILS OF PROCESSING OF YOUR PERSONAL DATA

This Appendix 1 to Data Processor Agreement includes certain details of the Processing of Your personal data: as required by Article 28(3) GDPR.

Data Exporter: You
Contact Details: Provided in the Order Confirmation.
Data Exporter Role: you are a controller.

Data Importer: Dext Software Limited.
Contact Details: Data Protection Officer c/o Legal Department, dpo@dext.com cc legal@dext.com
Data Importer Role: We are a processor.

Subject matter of the processing of Your personal data

The subject matter of the Processing of Your Personal Data is in order to provide the Dext Products under the Agreement including the Order Confirmation.

Duration of the processing of your personal data

The subject duration of the Processing of Your Personal Data is for the Licence Term plus the period until We delete Your Personal Data in accordance with our retention policy, which is set out in our privacy policy available on our website.

The nature and purpose of the processing of Your personal data

In order to fulfil Our obligations to You under the Agreement, provide the Dext product(s) as set forth in the Agreement including the Order Confirmation.

Categories of data subjects

The personal data processed relates to the following categories of data subjects:

- Your employees
- Your contractors
- Your directors
- Your Permitted Users
- Your Authorised Users

The types of Your personal data to be processed

- Identity Data includes: first name, last name, username or similar identifier, marital status, title, date of birth and gender.
- Contact Data includes: job description billing address, email address and telephone numbers.

- Transaction Data includes: details about payments, receipts or invoices; details about payments and other details of products and services purchased from Dext.
- Technical Data includes: internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices used to access the Dext website or Our mobile app.
- Profile Data includes: username and password, purchases or orders made, user preferences, feedback and survey responses.
- Usage Data includes: information about usage of the Dext website, app and Dext Products
- Marketing and Communications Data includes: user preferences in receiving marketing from Dext and its affiliates and user communication preferences.

International data transfers

We operate internationally, and as a result, may transfer the information we collect about you across international borders, including from the EEA or UK to the United States, for processing and storage. To the extent that the information we collect about you is transferred from the EEA or UK to territories/countries for which the EU Commission or UK Secretary of State (as applicable) has not made a finding that the legal framework in that territory/country provides adequate protection for individuals' rights and freedoms for their personal data, we may transfer such data consistent with applicable data protection laws based on prior assessment of the level of data protection afforded in the context of the transfer, including through the use of the EU Commission-approved or UK Secretary of State-approved (as applicable) Standard Contractual Clauses, if necessary in combination with additional safeguards.

Sub-processors

A list of Sub-processors We use can be found below. This list may be amended from time to time:

Name	Purpose	Jurisdiction	SSCs
AWS	Cloud services platform that is used for our database storage & to run all of our apps.	EU: AWS Ireland – active location; AWS Germany, Frankfurt – backup location.	N.A.
Fino	Provides integrated screen-scrapping technology to fetch invoice and bill data from a customer's account on other platforms. Through Fino, customers can connect to over 2,000 possible providers, such as Amazon, BT, Spotify, Thames Water and EE.	EU (AWS Ireland)	N.A.
Fivetran	Syncs Netsuite invoice data to Looker.	EU	N.A.
Google Cloud Platform (Cloud Vision)	This is used for our OCR data extraction service. No data is stored because it is a transient service, the data is processed in order to be extracted and then the files are immediately returned to us once processed. Google cloud does not keep copies of this data.	US (Google Cloud)	Yes
Honeybadger	This is the tool we use to report on errors on our website – e.g. if there is fault when logging in.	US (AWS us-east-1 region)	Yes
Looker	Business intelligence tool and big data analytics platform that helps with analysing and sharing real-time business analytics using dashboards.	EU	N.A.
Mailchimp / Mandrill	Allows us to send one-to-one transactional emails triggered by user actions, like requesting a password or placing an order.	EU: AWS Ireland	N.A.
Netsuite	Cloud based accounting system that helps us manage business finance and operations.	UK (London)	N.A.
OwnBackup	Backup tool for Salesforce.	UK	N.A.
Salesforce	Integrated Customer Relationship Management (CRM) platform used to manage interactions with customers and potential customers.	UK (London)	N.A.
Sentry	Application monitoring and error tracking	US	Yes
Snowflake	Cloud data warehouse that offers a data storage and analytics service.	EU (AWS Ireland)	N.A.
Storecove	Provides e-invoicing capability	EU	N.A.
Stripe	Processes customer payments	US	Yes
Twillo	Software that sends SMS on our behalf for features.	US	Yes

<div align="center">**APPENDIX 2**</div>

<div align="center">**TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**</div>

The technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) of the EU SCC's are those established and maintained under clause 4 of this Data Processor Agreement and includes without limitation those found at https://dext.com/uk/security as amended from time to time.

<div align="center">**APPENDIX 3**</div>
<div align="center">**UK Addendum**</div>

Table 1: Parties

Start Date	Data Processing Agreement Effective Date	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: As listed in the Order Confirmation	Full legal name: Dext Software Limited
	Trading name (if different): n/a	Trading name (if different):
	Main address (if a company registered address): As listed in the Order Confirmation	Main address (if a company registered address): Unit 1.2, Techspace Shoreditch. 25 Luke Street, London, EC2A 4DS
	Official registration number (if any) (company number or similar identifier): As listed in the Order Confirmation	Official registration number (if any) (company number or similar identifier): 07361080
Key contacts	Full name (optional): Legal Department	Full name (optional):
	Job title: As listed in the Order Confirmation	Job title: Legal Department
	Contact details including email: As listed in the Order Confirmation	Contact details including email: dpo@dext.com cc legal@dext.com
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☐ The version of the Approved EU SCCs, which this Addendum is appended to, detailed below, including the Appendix Information.

Date:

Reference (if any):

Other identifier (if any):

OR

☒ The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum.

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1				-	-	-
2	x	x		General authorisation	10 days	-
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 Appendix 1 of this Data Processor Agreement*
Annex 1B: Description of Transfer: *See Appendix 1 of this Data Processor Agreement*

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: *See Appendix 2 of this Data Processor Agreement*	

Table 4: Ending this Addendum when the Approved Addendum changes

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

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

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

Interpretation of this Addendum

0. 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:

   1. **Addendum**: This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.

   2. **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.

   3. **Appendix Information**: As set out in Table 3.

   4. **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) of the UK GDPR.

   5. **Approved Addendum**: The template Addendum issued by the ICO and laid before Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.

   6. **Approved EU SCCs**: EU SCCs.

   7. **ICO**: The Information Commissioner.

   8. **Restricted Transfer**: A transfer which is covered by Chapter V of the UK GDPR.

   9. **UK**: The United Kingdom of Great Britain and Northern Ireland.

   10. **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.

   11. **UK GDPR**: As defined in section 3 of the Data Protection Act 2018.

0. 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.

0. 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.

0. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

0. 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.

0. 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

0. 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.

0. 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.

0. 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

0. 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.

0. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

0. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

0. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

(a) references to the "**Clauses**" mean 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 1 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

0. 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.

0. 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.

0. 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.

0. 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.

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

Alternative Part 2 Mandatory Clauses

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with section 119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.