Epicor Software Corporation

Data Processing Addendum (UK Version)

Based on the UK General Data Protection Regulation (UK GDPR)

This Data Processing Addendum ("**DPA**") forms part of the Epicor Master Customer Agreement (or other such titled written or electronic agreement addressing the same subject matter) between **Epicor Software (UK) Limited** (**Epicor**) and Customer (the "**Agreement**") whereby Customer acquires, and Epicor provides, services. This DPA reflects the parties' agreement with regard to the Processing of Personal Data as regulated under the UK GDPR.

By executing and submitting an Order Form, Statement of Work, or the Amendment to existing agreements that references the Agreement (which incorporates this DPA), Customer agrees to this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent Epicor processes Personal Data for which such Authorized Affiliates qualify as the Controller. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In providing the Services (defined below) to Customer pursuant to the Agreement, Epicor may Process Personal Data on behalf of Customer, and the parties agree to comply with the following provisions with respect to any Personal Data.

INSTRUCTIONS ON HOW TO EXECUTE THIS DPA WITH EPICOR

1. This DPA consists of distinct parts:

   (a) this body and its set of definitions and provisions;

   (b) **Schedule 1**: scope of processing of Personal Data; and

   (c) **Schedule 2**: the International Data Transfer Agreement (version A1.0, in force on and from 21 March 2022 as issued by the Information Commissioner's Office).

2. Customer must send the completed and signed Order Form, Statement of Work, or Amendment to Epicor in compliance with the instructions provided by Epicor. Upon receipt by Epicor of the validly completed Order Form, Statement of Work, or Amendment, this DPA shall come into effect and legally bind the parties.

APPLICATION OF THIS DPA

If the Customer entity signing this DPA is a party to the Agreement, then this DPA is an addendum to, and forms part of, the Agreement. In such case, the Epicor entity (i.e., either **Epicor Software (UK) Limited** or an Affiliate of Epicor) that is party to the Agreement, is party to this DPA.

If the Customer entity signing this DPA has executed an Order Form with Epicor or its Affiliate pursuant to the Agreement, but is not itself a party to the Agreement, then this DPA is an addendum to that Order Form and applicable renewal Order Forms, and the Epicor entity that is a party to such Order Form is a party to this DPA.

If the Customer entity signing this DPA is neither a party to an Order Form nor the Agreement, then this DPA is not valid and therefore is not legally binding. Such entity should request that the Customer entity which is a party to the Agreement execute this DPA.

DPA DEFINITIONS

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the Customer entity signing this Agreement. "**Control**" for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Authorized Affiliate" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and Epicor but has not signed its own Order Form with Epicor and is not a "Customer" as defined under the Agreement.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Data Protection Laws and Regulations" means all laws and regulations, including laws and regulations of the United Kingdom, applicable to the Processing of Personal Data under the Agreement, including (without limitation): (i) the UK GDPR; (ii) the Data Protection Act 2018; (iii) Data Protection (Charges and Information) Regulations 2018; (iv) the Privacy and Electronic Communications (EC Directive) Regulations 2003; (v) any other legislation in force in the UK from time to time in respect of data protection and privacy guidance and (vi) codes of practice issued from time to time by the Information Commissioner's Office, in each case as amended, updated or replaced from time to time; and (vii) guidance and codes of practice issued by the European Data Protection Board or the Article 29 Working Party prior to 1 Jan 2021.

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"Epicor" means the Epicor entity which is a party to this DPA, as specified in the section "Application of this DPA" above, being **Epicor Software (UK) Limited**, a company registered in England and Wales under Company Number: 02338274 with its registered address located at 6 Arlington Square West, Bracknell, Berkshire RG12 1PU, or an Affiliate of Epicor, as applicable.

"Epicor Group" means Epicor and its Affiliates engaged in the Processing of Personal Data.

"**UK GDPR**" means EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as incorporated into domestic United Kingdom law by the European Union (Withdrawal Agreement) Act 2020 and amended by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020.

"**Order Form**" means Epicor's standard order form documentation, including without limitation, written Orders and Statements of Work, for acquiring Services.

"**Personal Data"** means any information regulated by the UK GDPR relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is regulated by the UK GDPR and submitted by or on behalf of Customer or an Authorized Affiliate to Epicor in connection with providing the Services.

"Processing" (including its root word, "Process") means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means the entity which Processes Personal Data on behalf of the Controller.

"Restricted Transfer" means a transfer of Personal Data which is covered by Chapter V of the UK GDPR.

"Services" means software support services, professional consulting services or software subscription services acquired by Customer from Epicor pursuant to an Order Form.

"International Data Transfer Agreement" or "IDTA" means the agreement set forth at **Schedule 2** to this DPA executed by and between Customer and Epicor (the terms and conditions of which are incorporated herein) pursuant to Chapter V of the UK GDPR (as defined in section 3 (10) of the Data Protection Act 2018) together with Article 46 (1) of the UK GDPR for the transfer of personal data to processors established in third countries (known as a **Restricted Transfer**) which do not ensure an adequate level of data protection.

“Sub-processor” means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of a Processor.

“Supervisory Authority” means the UK Information Commissioner.

“Trust & Compliance Documentation” means the Documentation applicable to the specific Services purchased by Customer, as may be updated periodically, and accessible via Epicor’s website at www.Epicor.com/company/compliance , or as otherwise made reasonably available by Epicor.

DPA TERMS

Epicor and Customer hereby enter into this DPA effective as of the execution of an Order Form, Statement of Work, or the Amendment that references this DPA. This DPA is incorporated into and forms part of the Agreement.

1. **Provision of the Services.** Epicor provides the Services to Customer under the Agreement. In connection with the Services, the parties anticipate that Epicor may Process Customer’s data which may include Personal Data relating to Data Subjects.

2. **The Parties’ Roles**. Customer, as Controller, appoints Epicor as a Processor to process the Personal Data on Customer's behalf. In some circumstances Customer may be a Processor, in which case Customer appoints Epicor as Customer's sub-processor, which shall not change the obligations of either Customer or Epicor under this DPA, as Epicor will remain a Processor with respect to Customer in such event. Subject to clause 9 below, Epicor or members of the Epicor Group may be or otherwise may engage Sub-processors pursuant to the requirements of this DPA.

3. **Customer Responsibilities.** Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer’s instructions to Epicor for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

4. **Processing Purposes.** Epicor shall keep Personal Data confidential and shall only Process Personal Data on behalf of and in accordance with Customer’s documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented, reasonable instructions provided by Customer (for example, via email) where such instructions are consistent with the terms of the Agreement. Epicor shall not be required to comply with or observe Customer’s instructions if such instructions would violate the UK GDPR but shall notify Customer promptly if Epicor considers that the Customer’s instructions violate such laws.

5. **Scope of Processing.** The subject-matter of Processing of Personal Data by Epicor is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in **Schedule 1** to this DPA.

6. **Data Subject Requests.** To the extent legally permitted and required, Epicor shall promptly notify Customer if Epicor receives a request from a Data Subject to exercise the Data Subject’s right of access, right to rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, objection to the Processing, or its right not to be subject to an automated individual decision making (“**Data Subject Request**”) with respect to Personal Data in a manner other than the Data Subject using Epicor-provided self-help tools. Factoring into account the nature of the Processing, Epicor shall assist Customer by appropriate organizational and technical measures, insofar as this is possible, for the fulfilment of Customer’s obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Epicor shall, upon Customer’s

request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent that Epicor is legally authorized to do so, and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any reasonable costs arising from Epicor's provision of such assistance.

7. **Epicor Personnel.** Epicor shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training regarding their responsibilities, and have executed written confidentiality agreements. Epicor shall take commercially reasonable steps to ensure the reliability of any Epicor personnel engaged in the Processing of Personal Data. Epicor shall ensure that Epicor's access to Personal Data is limited to those personnel assisting in the provision of the Services in accordance with the Agreement.

8. **Data Protection Officer.** Epicor shall have appointed, or shall appoint, a data protection officer if and whereby such appointment is required by Data Protection Laws and Regulations. Any such appointed person may be reached through legalpersonnel-emea@epicor.com

9. **Epicor's Sub-processors**. Customer has authorized the use of Sub- processors to assist Epicor with respect to the performance of Epicor's obligations under the Agreement. Upon written request of Customer, Epicor will provide to Customer a list of its then current Sub-processors. Customer acknowledges and agrees that (a) Epicor's Affiliates may be retained as Sub-processors; and (b) Epicor and Epicor's Affiliates respectively may engage third party Sub-processors in connection with the provision of the Services. On Epicor's Compliance webpage (accessible via www.Epicor.com/company/compliance under the **"Sub-Processors**" link), Customer may find a mechanism to subscribe to notifications of new Sub-processors for each of the applicable Services, to which Customer shall subscribe, and if Customer subscribes, Epicor shall provide notification of a new Sub-processor(s) before authorizing any new Subprocessor(s) to process Personal Data in connection with the provision of the applicable Services. In order to exercise its right to object to Epicor's use of a new Sub-processor, Customer shall notify Epicor promptly in writing within ten (10) business days after receipt of Epicor's notice in accordance with the instructions accessible via www.Epicor.com/company/compliance If Customer does not object within such ten (10) business days, such new Sub-processor shall be deemed accepted. In the event Customer objects to a new Sub-processor, and that objection is not unreasonable, Epicor will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing Customer's Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Epicor is unable to make available such change within a reasonable time period, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those aspects of the Services which cannot be provided by Epicor without the use of the objected-to new Sub-processor by providing written notice to Epicor. Epicor will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services.

10. **Liability for Sub-processors.** Epicor shall be liable for the acts and omissions of its Sub-processors to the same extent Epicor would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

11. **Security Measures.** Epicor shall maintain appropriate organizational and technical measures for protection of the security (including protection against unauthorized or unlawful Processing, and against unlawful or accidental destruction, alteration or damage or loss, unauthorized disclosure of, or access to, Personal Data), confidentiality, and integrity of Personal Data, as set forth in Epicor's applicable Trust & Compliance Documentation available at https://www.epicor.com/en-uk/company/compliance/ Epicor regularly monitors compliance with these measures. Epicor will not materially decrease the overall security of the Services during Customer's and/or Authorized Affiliates' subscription term.

12. **Third-Party Certifications and Audit Results.** Epicor has attained the third-party certifications and audit results set forth in the Trust & Compliance Documentation. Upon Customer's written request at reasonable intervals,

and subject to the confidentiality obligations set forth in the Agreement, Epicor shall make available to Customer a copy of Epicor's then most recent third-party certifications or audit results, as applicable.

13. **Notifications Regarding Personal Data**. Epicor has in place reasonable and appropriate security incident management policies and procedures, as specified in the Trust & Compliance Documentation and shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Epicor or its Sub-processors of which Epicor becomes aware (hereinafter, a "**Personal Data Incident**"), as required to assist Customer in ensuring compliance with its obligations to notify the Supervisory Authority in the event of Personal Data Incident. Epicor shall make reasonable efforts to identify the cause of such Personal Data Incident, and take those steps as Epicor deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident, to the extent that the remediation is within Epicor's reasonable control. The obligations set forth herein shall not apply to incidents that are caused by either Customer or Customer's Users.

14. **Return of Personal Data.** Epicor shall return Personal Data to Customer and, to the extent allowed by applicable law, delete Personal Data in accordance with the procedures and time periods specified in the Trust & Compliance Documentation, unless the retention of the data is requested from Epicor according to mandatory statutory laws.

15. **Authorized Affiliates.** The parties agree that, by executing the DPA, Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliate(s), thereby establishing a separate DPA between Epicor and each such Authorized Affiliate, subject to the provisions of the Agreement. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. An Authorized Affiliate is not and does not become a party to the Agreement and is only a party to the DPA. All access to and use of the Services by Authorized Affiliate(s) must comply with the terms and conditions of the Agreement and any violation thereof by an Authorized Affiliate shall be deemed a violation by Customer.

16. **Communications.** The Customer entity that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Epicor under this DPA and shall be entitled to transmit and receive any communication in relation to this DPA on behalf of its Authorized Affiliate(s).

17. **Exercise of Rights.** Where an Authorized Affiliate becomes a party to the DPA, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Epicor directly by itself, the parties agree that (i) solely the Customer entity that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer entity that is the contracting party to the Agreement shall exercise any such rights under this DPA in a combined manner for all of its Authorized Affiliates together, instead of doing so separately for each Authorized Affiliate.

18. **Liability.** Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Epicor, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. Epicor's and its Affiliates' total liability for all claims from Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Authorized Affiliates, and shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA. Each reference to the DPA herein means this DPA including the International Data Transfer Agreement.

19. **GDPR.** Epicor will Process Personal Data in accordance with the UK GDPR requirements directly applicable to Epicor's provision of the Services.

20. **Data Protection Impact Assessment.** Upon Customer's request, Epicor shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the UK GDPR to carry out a data protection impact assessment related to Customer's use of the Services to the extent such assessment is required under applicable law, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Epicor. Epicor shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 20 of this DPA, to the extent required under the UK GDPR. Notwithstanding the foregoing, the Parties acknowledge and agree that, in general, each believes that the nature, scope and scale of any data processing by Epicor does not and will not rise to the level of requiring a Data Protection Impact Assessment under applicable law.

21. **International Data Transfer Agreement**. The International Data Transfer Agreement applies to (i) the legal entity that has executed the International Data Transfer Agreement as a data exporter and its Authorized Affiliates and, (ii) all Affiliates of Customer established within the United Kingdom, which have signed Order Forms for the Services as the data exporter.

22. **Customer's Processing Instructions**. This DPA and the Agreement are Customer's complete and final instructions at the time of signature of the Agreement to Epicor for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of the International Data Transfer Agreement, the following is deemed an instruction by Customer to process Personal Data: (a) Processing in accordance with the Agreement, this DPA and applicable Order Form(s); (b) Processing initiated by Users in their use of the Services; and (c) Processing to comply with other reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement, this DPA and as well as the Data Protection Laws and Regulations.

23. **Audits**. The parties agree that audits, if requested by Customer, shall be carried out, in accordance with the following specifications:

a. Customer may audit Epicor's compliance with the terms of this Data Processing Addendum. Such audits shall be limited to no more than one per year unless the laws applicable to Customer provide for more frequent audits of Epicor's data centre facility that Processes Personal Data. If Customer wishes to utilize a third party to conduct the audit, the third party must be mutually agreed to by Customer and Epicor and such third party must execute a written confidentiality agreement acceptable to Epicor, acting reasonably, before conducting the audit.

b. To request an audit, Customer must prepare and submit an Audit Request Form to Epicor at least fifteen (15) days in advance of the proposed audit date. The Audit Request Form must include details surrounding the proposed start date, scope and duration of the audit. Epicor will review the completed Audit Request Form and provide any questions, concerns or comments to Customer. Epicor and Customer shall work together to agree upon the final plan (including without limitation start date, scope, and duration) for the audit. If Customer's requested audit scope is substantially addressed in a SSAE 16/ISAE 3402 Type 2, ISO, NIST, PCI DSS, HIPAA or similar audit report previously performed on Epicor's behalf by a qualified third-party auditor within the twelve months prior to Customer's request and Epicor confirms that no known known material changes in the audited controls exist, then Customer shall accept those findings in place of requesting a further audit of the controls covered by the report.

c. Customer's audit shall be conducted during the regular business hours of the applicable facility, shall be subject to Epicor and facility policies, and may not unreasonably interfere with Epicor or the facility's business activities.

d. Customer will provide Epicor with a copy of any audit reports generated in connection with any audit under this Section 23(d), unless doing so is expressly prohibited by law. Customer may only utilize the audit reports for the purposes of meeting its regulatory audit requirements and/or confirming Epicor's compliance with the Data Processing Addendum requirements. The audit reports and any related documentation shall be considered Confidential Information of the parties under the terms of the Agreement.

e. Any Customer audits that are not met with existing reports shall be conducted entirely at Customer's expense, including without limitation Epicor’s internal reasonable costs of participating in such audits. Any request by Customer for Epicor to provide assistance with a Customer audit shall be considered a separate service if such audit assistance requires the use of resources different from or in addition to those required for the provision of the Services. Customer's written approval and agreement to pay any related fees or reasonable costs incurred by Epicor for such audit assistance shall be granted and provided to Epicor before Epicor is requested to perform such audit assistance.

24. **Order of Precedence.** This DPA is incorporated into and forms part of the Agreement. For matters not addressed under this DPA, the terms of the Agreement apply. With respect to the rights and obligation of the parties vis-à-vis each other, in the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA will control. In the event of a conflict between the terms of the DPA and the International Data Transfer Agreement, the International Data Transfer Agreement will prevail.

SCHEDULE 1

Scope of Processing

A. LIST OF PARTIES

1. Data exporter(s):

Name of Data Exporter (Customer)	Address	Contact person's name, position and contact details:	Activities relevant to the data transferred under these Clauses:	Role	Signature	Date of Signature
Customer named in an Epicor Order. *[Note Customer enters the DPA for and/or on behalf of its Affiliates.]*	Customer Address on Epicor Order	Customer Contact details as set out in the Epicor Order	Processing, by Epicor (meaning **Epicor Software (UK) Limited**) (and/or its Affiliates), of Personal Data submitted by or on behalf of Customer (as the data exporter) to enable Epicor (and/or its Affiliates) to perform Epicor's contractual obligations under a Cloud based services agreement and/or perform software maintenance and support services.	Controller	By executing an Epicor Order, Customer is deemed to have signed the DPA and International Data Transfer Agreement	Same date as Customer's signature on an Epicor Order

2. Other Data Exporters:

Not applicable. Single Data Exporter. See above

Data importer(s):

Name of Data Importer (Epicor and its Affiliates)	Address	Contact person's name, position and contact details:	Activities relevant to the data transferred under these Clauses:	Role	Signature	Date of Signature
Epicor Software (UK) Limited and/or its international affiliates as listed at https://www.epicor.com/en-uk/company/compliance/affiliates/ (together "**Epicor**")	**c/o 6 Arlington Square West Bracknell Berkshire RG12 1PU Attention: Legal Department** **804 Las Cimas Parkway, Austin, Texas 78746 Attention: Legal Department**	**Epicor Software (UK) Limited 6 Arlington Square West Bracknell Berkshire RG12 1PU Attention: Legal Department e-mail:** legalpersonnel-emea@epicor.com	Processing, by Epicor (and/or its Affiliates), of Personal Data submitted by or on behalf of Customer (as the data exporter) to enable Epicor (and/or its Affiliates) to perform Epicor's contractual obligations under a Cloud based services agreement and/or perform software maintenance and support services.	Processor	By executing an Epicor Order, Epicor and/or the relevant Epicor Affiliates is deemed to have signed the DPA and the International Data Transfer Agreement	Same date as Epicor's authorized signature on an Epicor Order

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data Exporter (named above and on an Epicor Order) may submit Personal Data to the Services, the extent of which is determined and controlled by the Data Exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects who are natural persons:

- **Customers, prospective customers, business partners, and vendors of the Data Exporter.**
- **Employees, former employees or contact persons of Data Exporter customers, business partners, and vendors.**
- **Employees, agents, advisors, contractors, or any user authorized by the Data Exporter to use the Services.**

Categories of personal data transferred

Data Exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the Data Exporter in its sole discretion, and which may include, but is not limited to the following categories of personal data:

- **First and last name**
- **Family member names (spouse, dependents, partner)**
- **Business contact information (company name, email, phone, physical business address)**
- **Personal contact information (name, email, phone, physical address)**
- **Government issued ID**
- **Job title**
- **Compensation**
- **Bank account details**
- **Benefits**
- **Employee performance**
- **Employment application details (employment history, education, certifications)**
- **Personal life data (in the form of security questions and answers)**
- **User login credentials (user IDs, passwords)**
- **System usage activity by users**

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 Personal Data transferred concern the following special categories of data (please specify): **NONE**

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

Continuous transfer during term of the Agreement

Nature of the processing

The objective of Processing of Personal Data by the Data Importer is the performance of the Services pursuant to the Agreement.

Purpose(s) of the data transfer and further processing

Necessary to fulfil contractual obligations under 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

Duration of the Services and/or term of Agreement plus 6 years (statute of limitation period)

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

Subject Matter of processing	**Processing of the categories of Personal Data listed above**
Nature of Processing	**To fulfil contractual obligations under the Agreement**
Duration of Processing	**Duration of the Services and/or term of the Agreement, plus 6 years (statute of limitations period)**

______

C. TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Epicor shall maintain appropriate organizational and technical measures for protection of the security (including protection against unauthorized or unlawful Processing, and against unlawful or accidental destruction, alteration or damage or loss, unauthorized disclosure of, or access to, Personal Data), confidentiality, and integrity of Personal Data, as set forth in Epicor's applicable Compliance Documentation located at www.epicor.com/company/compliance **Epicor regularly monitors compliance with these measures. Epicor will not materially decrease the overall security of the Services during Customer's and/or Authorized Affiliates' subscription term.**

D. LIST OF SUB-PROCESSORS

The Controller/ Data Exporter has authorized the use of the following sub-processors:

https://www.epicor.com/en-uk/company/compliance/sub-processors/

Name	**Purpose**	**Country**
Amazon Web Services	Cloud hosting services	USA
AT&T	US datacenter hosting facility	USA
Avaya	Technical support	USA
CDW	UK datacenter network provider	UK
CenturyLink	Global network provider	USA
Cisco Systems	Global network provider	USA
Deutsch Telecom	Technical support	Germany
Freppa	Technical support	Germany
Iron Mountain	Backup data storage	USA
Lenovo	Global computer technical support	USA
Microsoft Azure	Cloud hosting services	Global
Riverbed	Global network provider	USA
ServiceNow	Technical support	USA
Teamviewer	Technical support	USA
Telstra	UK and Australia datacenter hosting facility	UK & Australia
Webex	Technical support	USA

EPICOR

SCHEDULE 2

International Data Transfer Agreement VERSION A1.0, in force 21 March 2022

ico.
Information Commissioner's Office

Standard Data Protection Clauses to be issued by the Commissioner under S119A (1) Data Protection Act 2018

International Data Transfer Agreement VERSION A1.0, in force 21 March 2022

This IDTA 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 and signatures

Start date	**Effective Date of the Epicor Master Customer Agreement Master Terms and Conditions, as supplemented by a relevant Product Supplement (the terms and conditions of which are available for download from https://www.epicor.com/en-us/company/customer-agreements/ which terms and conditions are incorporated by reference into an Order)**	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: **Customer named on an Order** Trading name (if different): N/A Main address (if a company registered address): **Same address as set forth on an Order** Official registration number (if any) (company number or similar identifier): **Company Number registered with Companies House**	Full legal name: **Epicor Software (UK) Limited** Trading name (if different): N/A Main address (if a company registered address): **6 Arlington Square West, Bracknell, Berkshire RG12 1PU** Official registration number (if any) (company number or similar identifier): **02338274**
Key Contact	Full Name (optional): **Same as shown on Order**	Full Name (optional): **Epicor Legal Department**

	Job Title: **Same as on Order** Contact details including email: **Same as on Order**	Job Title: **Legal Department** Contact details including email: legalpersonnel-emea@epicor.com
Importer Data Subject Contact	**Customer's Legal Department or, if no Legal Department, Managing Director**	Job Title: **Epicor Legal Department** Contact details including email: legalpersonnel-emea@epicor.com
Signatures confirming each Party agrees to be bound by this IDTA	Signed for and on behalf of the **Exporter** set out above **BY SIGNING THE EPICOR ORDER (AND/OR THE EPICOR MASTER CUSTOMER AGREEMENT OR EPICOR STATEMENT OF WORK OR EPICOR OTHER DOCUMENT INCLUDING A WORK AUTHORISATION) TO WHICH THIS INTERNATIONAL DATA TRANSFER AGREEMENT IS INCORPORATED, EXPORTER IS DEEMED TO HAVE SIGNED THIS INTERNATIONAL DATA TRANSFER AGREEMENT**	Signed for and on behalf of the **Importer** set out above **BY ACCEPTING EXPORTER'S ORDER (WHICH REFERENCES EPICOR'S MASTER CUSTOMER AGREEMENT) AND/OR BY SIGNING EPICOR'S STATEMENT OF WORK OR OTHER DOCUMENT (INCLUDING A WORK AUTHORISATION TO WHICH THIS INTERNATONAL DATA TRANSFER AGREEMENT IS INCORPORATED), IMPORTER IS DEEMED TO HAVE SIGNED THIS INTERNATIONAL DATA TRANSFER AGREEMENT**

Table 2: Transfer Details

UK country's law that governs the IDTA:	□ **England and Wales** □ ~~Northern Ireland~~ □ ~~Scotland~~
Primary place for legal claims to be made by the Parties	□ **England and Wales** □ ~~Northern Ireland~~ □ ~~Scotland~~
The status of the Exporter	In relation to the Processing of the Transferred Data: □ **Exporter is a Controller** □ ~~Exporter is a Processor or Sub-Processor~~
The status of the Importer	In relation to the Processing of the Transferred Data: □ ~~Importer is a Controller~~ □ **Importer is the Exporter's Processor or Sub-Processor** □ ~~Importer is **not** the Exporter's Processor or Sub-Processor (and the Importer has been instructed by a Third Party Controller)~~
Whether UK GDPR applies to the Importer	□ **UK GDPR applies to the Importer's Processing of the Transferred Data** □ ~~UK GDPR does not apply to the Importer's Processing of the Transferred Data~~

Linked Agreement	**If the Importer is the Exporter's Processor or Sub-Processor** – the agreement(s) between the Parties which sets out the Processor's or Sub-Processor's instructions for Processing the Transferred Data: Name of agreement: **Data Processing Addendum** Date of agreement: **same as the Effective Date of the Epicor Master Customer Agreement Master Terms and Conditions, as supplemented by a relevant Product Supplement (the terms and conditions of which are available for download from https://www.epicor.com/en-us/company/customer-agreements/ which terms and conditions are incorporated by reference into an Order)** Parties to the agreement: **(1) Exporter named on an Order (2) Epicor Software (UK) Limited** Reference (if any): N/A **Other agreements** – any agreement(s) between the Parties which set out additional obligations in relation to the Transferred Data, such as a data sharing agreement or service agreement: Name of agreement: **Epicor Master Customer Agreement Master Terms and Conditions, as supplemented by a relevant Product Supplement (the terms and conditions of which are available for download from https://www.epicor.com/en-us/company/customer-agreements/ which terms and conditions are incorporated by reference into an Order)** Date of agreement: **Date of signed Order** Parties to the agreement: **(1) Exporter named on an Order (2) Epicor Software (UK) Limited** Reference (if any): N/A **If the Exporter is a Processor or Sub-Processor** – the agreement(s) between the Exporter and the Party(s) which sets out the Exporter's instructions for Processing the Transferred Data: Name of agreement: **N/A** Date of agreement: **N/A** Parties to the agreement: **N/A** Reference (if any): **N/A**
Term	The Importer may Process the Transferred Data for the following time period: □ **the period for which the Linked Agreement is in force** □ ~~time period:~~ □ ~~(only if the Importer is a Controller or not the Exporter's Processor or Sub-Processor) no longer than is necessary for the Purpose.~~
Ending the IDTA before the end of the Term	□ **the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA or the Parties agree in writing.** □ ~~the Parties can end the IDTA before the end of the Term by serving:~~ ~~months' written notice, as set out in Section 29 (How to end this IDTA without there being a breach).~~
Ending the IDTA when the Approved IDTA changes	Which Parties may end the IDTA as set out in Section 29.2: □ ~~Importer~~ □ **Exporter**

	☐ ~~neither Party~~
Can the Importer make further transfers of the Transferred Data?	☐ **The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).** ☐ ~~The Importer MAY NOT transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with Section 16.1 (Transferring on the Transferred Data).~~
Specific restrictions when the Importer may transfer on the Transferred Data	The Importer MAY ONLY forward the Transferred Data in accordance with Section 16.1: ☐ ~~if the Exporter tells it in writing that it may do so.~~ ☐ ~~to:~~ ☐ ~~to the authorised receivers (or the categories of authorised receivers) set out in:~~ ☐ **there are no specific restrictions.**
Review Dates	☐ ~~No review is needed as this is a one-off transfer and the Importer does not retain any Transferred Data~~ ~~First review date:~~ The Parties must review the Security Requirements at least once: ☐ ~~each month(s)~~ ☐ ~~each quarter~~ ☐ ~~each 6 months~~ ☐ ~~each year~~ ☐ ~~each year(s)~~ ☐ **each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment**

Table 3: Transferred Data

Transferred Data	The personal data to be sent to the Importer under this IDTA consists of: ☐ **The categories of Transferred Data will update automatically if the information is updated in the Linked Agreement referred to.** ☐ ~~The categories of Transferred Data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.~~
Special Categories of Personal Data and criminal convictions and offences	The Transferred Data includes data relating to: ☐ ~~racial or ethnic origin~~ ☐ ~~political opinions~~ ☐ ~~religious or philosophical beliefs~~ ☐ ~~trade union membership~~ ☐ ~~genetic data~~ ☐ ~~biometric data for the purpose of uniquely identifying a natural person~~ ☐ ~~physical or mental health~~

	~~☐ sex life or sexual orientation~~ ~~☐ criminal convictions and offences~~ ☐ **none of the above** ☐ **set out in: Schedule 1 to DPA** ~~And:~~ ~~☐ The categories of special category and criminal records data will update automatically if the information is updated in the Linked Agreement referred to.~~ ~~☐ The categories of special category and criminal records data will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.~~
Relevant Data Subjects	The Data Subjects of the Transferred Data are: ☐ **The categories of Data Subjects will update automatically if the information is updated in the Linked Agreement referred to.** ☐ ~~The categories of Data Subjects will not update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.~~
Purpose	☐ ~~The Importer may Process the Transferred Data for the following purposes:~~ ☐ The Importer may Process the Transferred Data for the purposes set out in: **the Linked Agreement (Data Processing Addendum and Appendices thereto)** In both cases, any other purposes which are compatible with the purposes set out above. ☐ **The purposes will update automatically if the information is updated in the Linked Agreement referred to.** ☐ ~~The purposes will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.~~

Table 4: Security Requirements

Security of Transmission	An overview of Importer's Information Security Program is available at: https://www.epicor.com/en-uk/company/compliance/
Security of Storage	An overview of Importer's Information Security Program is available at: https://www.epicor.com/en-uk/company/compliance/
Security of Processing	An overview of Importer's Information Security Program is available at: https://www.epicor.com/en-uk/company/compliance/
Organisational security measures	An overview of Importer's Information Security Program is available at: https://www.epicor.com/en-uk/company/compliance/
Technical security minimum requirements	An overview of Importer's Information Security Program is available at: https://www.epicor.com/en-uk/company/compliance/

Updates to the Security Requirements	☐ **The Security Requirements will update automatically if the information is updated in the Linked Agreement referred to.** ☐ ~~The Security Requirements will NOT update automatically if the information is updated in the Linked Agreement referred to. The Parties must agree a change under Section 5.3.~~

Part 2: Extra Protection Clauses

Extra Protection Clauses:	**None required**
(i) Extra technical security protections	**None required**
(ii) Extra organisational protections	**None required**
(iii) Extra contractual protections	**None required**

Part 3: Commercial Clauses

Commercial Clauses	**No additional commercial clauses are incorporated**

Part 4: Mandatory Clauses

Information that helps you to understand this IDTA

1. This IDTA and Linked Agreements

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

1.2 This IDTA is made up of:

1.2.1 Part one: Tables;

1.2.2 Part two: Extra Protection Clauses;

1.2.3 Part three: Commercial Clauses; and

1.2.4 Part four: Mandatory Clauses.

1.3 The IDTA starts on the Start Date and ends as set out in Sections 29 or 30.

1.4 If the Importer is a Processor or Sub-Processor instructed by the Exporter: the Exporter must ensure that, on or before the Start Date and during the Term, there is a Linked Agreement which is enforceable between the Parties and which complies with Article 28 UK GDPR (and which they will ensure continues to comply with Article 28 UK GDPR).

1.5 References to the Linked Agreement or to the Commercial Clauses are to that Linked Agreement or to those Commercial Clauses only in so far as they are consistent with the Mandatory Clauses.

2. Legal Meaning of Words

2.1 If a word starts with a capital letter it has the specific meaning set out in the Legal Glossary in Section 36.

2.2 To make it easier to read and understand, this IDTA contains headings and guidance notes. Those are not part of the binding contract which forms the IDTA.

3. You have provided all the information required

3.1 The Parties must ensure that the information contained in Part one: Tables is correct and complete at the Start Date and during the Term.

3.2 In Table 2: Transfer Details, if the selection that the Parties are Controllers, Processors or Sub-Processors is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws) then:

3.2.1 the terms and conditions of the Approved IDTA which apply to the correct option which was not selected will apply; and

3.2.2 the Parties and any Relevant Data Subjects are entitled to enforce the terms and conditions of the Approved IDTA which apply to that correct option.

3.3 In Table 2: Transfer Details, if the selection that the UK GDPR applies is wrong (either as a matter of fact or as a result of applying the UK Data Protection Laws), then the terms and conditions of the IDTA will still apply to the greatest extent possible.

4. How to sign the IDTA

4.1 The Parties may choose to each sign (or execute):

4.1.1 the same copy of this IDTA;

4.1.2 two copies of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement;

4.1.3 a separate, identical copy of the IDTA. In that case, each identical copy is still an original of this IDTA, and together all those copies form one agreement,

unless signing (or executing) in this way would mean that the IDTA would not be binding on the Parties under Local Laws.

5. Changing this IDTA

5.1 Each Party must not change the Mandatory Clauses as set out in the Approved IDTA, except only:

5.1.1 to ensure correct cross-referencing: cross-references to Part one: Tables (or any Table), Part two: Extra Protections, and/or Part three: Commercial Clauses can be changed where the Parties have set out the information in a different format, so that the cross-reference is to the correct location of the same information, or where clauses have been removed as they do not apply, as set out below;

5.1.2 to remove those Sections which are expressly stated not to apply to the selections made by the Parties in Table 2: Transfer Details, that the Parties are Controllers, Processors or Sub-Processors and/or that the Importer is subject to, or not subject to, the UK GDPR. The Exporter and Importer understand and acknowledge that any removed Sections may still apply and form a part of this IDTA if they have been removed incorrectly, including because the wrong selection is made in Table 2: Transfer Details;

5.1.3 so the IDTA operates as a multi-party agreement if there are more than two Parties to the IDTA. This may include nominating a lead Party or lead Parties which can make decisions on behalf of some or all of the other Parties which relate to this IDTA (including reviewing Table 4: Security Requirements and Part two: Extra Protection Clauses, and making updates to Part one: Tables (or any Table), Part two: Extra Protection Clauses, and/or Part three: Commercial Clauses); and/or

5.1.4 to update the IDTA to set out in writing any changes made to the Approved IDTA under Section 5.4, if the Parties want to. The changes will apply automatically without updating them as described in Section 5.4;

provided that the changes do not reduce the Appropriate Safeguards.

5.2 If the Parties wish to change the format of the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of the Approved IDTA, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

5.3 If the Parties wish to change the information included in Part one: Tables, Part two: Extra Protection Clauses or Part three: Commercial Clauses of this IDTA (or the equivalent information), they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

5.4 From time to time, the ICO may publish a revised Approved IDTA which:

5.4.1 makes reasonable and proportionate changes to the Approved IDTA, including correcting errors in the Approved IDTA; and/or

5.4.2 reflects changes to UK Data Protection Laws.

The revised Approved IDTA will specify the start date from which the changes to the Approved IDTA are effective and whether an additional Review Date is required as a result of the changes. This IDTA is automatically amended as set out in the revised Approved IDTA from the start date specified.

6. Understanding this IDTA

6.1 This IDTA 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.

6.2 If there is any inconsistency or conflict between UK Data Protection Laws and this IDTA, the UK Data Protection Laws apply.

6.3 If the meaning of the IDTA is unclear or there is more than one meaning, the meaning which most closely aligns with the UK Data Protection Laws applies.

6.4 Nothing in the IDTA (including the Commercial Clauses or the Linked Agreement) limits or excludes either Party's liability to Relevant Data Subjects or to the ICO under this IDTA or under UK Data Protection Laws.

6.5 If any wording in Parts one, two or three contradicts the Mandatory Clauses, and/or seeks to limit or exclude any liability to Relevant Data Subjects or to the ICO, then that wording will not apply.

6.6 The Parties may include provisions in the Linked Agreement which provide the Parties with enhanced rights otherwise covered by this IDTA. These enhanced rights may be subject to commercial terms, including payment, under the Linked Agreement, but this will not affect the rights granted under this IDTA.

6.7 If there is any inconsistency or conflict between this IDTA and a Linked Agreement or any other agreement, this IDTA overrides that Linked Agreement or any other agreements, even if those agreements have been negotiated by the Parties. The exceptions to this are where (and in so far as):

6.7.1 the inconsistent or conflicting terms of the Linked Agreement or other agreement provide greater protection for the Relevant Data Subject's rights, in which case those terms will override the IDTA; and

6.7.2 a Party acts as Processor and the inconsistent or conflicting terms of the Linked Agreement are obligations on that Party expressly required by Article 28 UK GDPR, in which case those terms will override the inconsistent or conflicting terms of the IDTA in relation to Processing by that Party as Processor.

6.8 The words "include", "includes", "including", "in particular" are used to set out examples and not to set out a finite list.

6.9 References to:

6.9.1 singular or plural words or people, also includes the plural or singular of those words or people;

6.9.2 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 IDTA has been signed; and

6.9.3 any obligation not to do something, includes an obligation not to allow or cause that thing to be done by anyone else.

7. Which laws apply to this IDTA

7.1 This IDTA is governed by the laws of the UK country set out in Table 2: Transfer Details. If no selection has been made, it is the laws of England and Wales. This does not apply to Section 35 which is always governed by the laws of England and Wales.

How this IDTA provides Appropriate Safeguards

8. The Appropriate Safeguards

8.1 The purpose of this IDTA is to ensure that the Transferred Data has Appropriate Safeguards when Processed by the Importer during the Term. This standard is met when and for so long as:

8.1.1 both Parties comply with the IDTA, including the Security Requirements and any Extra Protection Clauses; and

8.1.2 the Security Requirements and any Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach, including considering any Special Category Data within the Transferred Data.

8.2 The Exporter must:

8.2.1 ensure and demonstrate that this IDTA (including any Security Requirements and Extra Protection Clauses) provides Appropriate Safeguards; and

8.2.2 (if the Importer reasonably requests) provide it with a copy of any TRA.

8.3 The Importer must:

8.3.1 before receiving any Transferred Data, provide the Exporter with all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including any information which may reasonably be required for the Exporter to carry out any TRA (the "Importer Information");

8.3.2 co-operate with the Exporter to ensure compliance with the Exporter's obligations under the UK Data Protection Laws;

8.3.3 review whether any Importer Information has changed, and whether any Local Laws contradict its obligations in this IDTA and take reasonable steps to verify this, on a regular basis. These reviews must be at least as frequent as the Review Dates; and

8.3.4 inform the Exporter as soon as it becomes aware of any Importer Information changing, and/or any Local Laws which may prevent or limit the Importer complying with its obligations in this IDTA. This information then forms part of the Importer Information.

8.4 The Importer must ensure that at the Start Date and during the Term:

8.4.1 the Importer Information is accurate;

8.4.2 it has taken reasonable steps to verify whether there are any Local Laws which contradict its obligations in this IDTA or any additional information regarding Local Laws which may be relevant to this IDTA.

8.5 Each Party must ensure that the Security Requirements and Extra Protection Clauses provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

9. Reviews to ensure the Appropriate Safeguards continue

9.1 Each Party must:

9.1.1 review this IDTA (including the Security Requirements and Extra Protection Clauses and the Importer Information) at regular intervals, to ensure that the IDTA remains accurate and up to date and continues to provide the Appropriate Safeguards. Each Party will carry out these reviews as frequently as the relevant Review Dates or sooner; and

9.1.2 inform the other party in writing as soon as it becomes aware if any information contained in either this IDTA, any TRA or Importer Information is no longer accurate and up to date.

9.2 If, at any time, the IDTA no longer provides Appropriate Safeguards the Parties must Without Undue Delay:

9.2.1 pause transfers and Processing of Transferred Data whilst a change to the Tables is agreed. The Importer may retain a copy of the Transferred Data during this pause, in which case the Importer must carry out any Processing required to maintain, so far as possible, the measures it was taking to achieve the Appropriate Safeguards prior to the time the IDTA no longer provided Appropriate Safeguards, but no other Processing;

9.2.2 agree a change to Part one: Tables or Part two: Extra Protection Clauses which will maintain the Appropriate Safeguards (in accordance with Section 5); and

9.2.3 where a change to Part one: Tables or Part two: Extra Protection Clauses which maintains the Appropriate Safeguards cannot be agreed, the Exporter must end this IDTA by written notice on the Importer.

10. The ICO

10.1 Each Party agrees to comply with any reasonable requests made by the ICO in relation to this IDTA or its Processing of the Transferred Data.

10.2 The Exporter will provide a copy of any TRA, the Importer Information and this IDTA to the ICO, if the ICO requests.

10.3 The Importer will provide a copy of any Importer Information and this IDTA to the ICO, if the ICO requests.

The Exporter

11. Exporter’s obligations

11.1 The Exporter agrees that UK Data Protection Laws apply to its Processing of the Transferred Data, including transferring it to the Importer.

11.2 The Exporter must:

11.2.1 comply with the UK Data Protection Laws in transferring the Transferred Data to the Importer;

11.2.2 comply with the Linked Agreement as it relates to its transferring the Transferred Data to the Importer; and

11.2.3 carry out reasonable checks on the Importer’s ability to comply with this IDTA, and take appropriate action including under Section 9.2, Section 29 or Section 30, if at any time it no longer considers that the Importer is able to comply with this IDTA or to provide Appropriate Safeguards.

11.3 The Exporter must comply with all its obligations in the IDTA, including any in the Security Requirements, and any Extra Protection Clauses and any Commercial Clauses.

11.4 The Exporter must co-operate with reasonable requests of the Importer to pass on notices or other information to and from Relevant Data Subjects or any Third Party Controller where it is not reasonably practical for the Importer to do so. The Exporter may pass these on via a third party if it is reasonable to do so.

11.5 The Exporter must co-operate with and provide reasonable assistance to the Importer, so that the Importer is able to comply with its obligations to the Relevant Data Subjects under Local Law and this IDTA.

The Importer

12. General Importer obligations

12.1 The Importer must:

12.1.1 only Process the Transferred Data for the Purpose;

12.1.2 comply with all its obligations in the IDTA, including in the Security Requirements, any Extra Protection Clauses and any Commercial Clauses;

12.1.3 comply with all its obligations in the Linked Agreement which relate to its Processing of the Transferred Data;

12.1.4 keep a written record of its Processing of the Transferred Data, which demonstrate its compliance with this IDTA, and provide this written record if asked to do so by the Exporter;

12.1.5 if the Linked Agreement includes rights for the Exporter to obtain information or carry out an audit, provide the Exporter with the same rights in relation to this IDTA; and

12.1.6 if the ICO requests, provide the ICO with the information it would be required on request to provide to the Exporter under this Section 12.1 (including the written record of its Processing, and the results of audits and inspections).

12.2 The Importer must co-operate with and provide reasonable assistance to the Exporter and any Third Party Controller, so that the Exporter and any Third Party Controller are able to comply with their obligations under UK Data Protection Laws and this IDTA.

13. Importer's obligations if it is subject to the UK Data Protection Laws

13.1 If the Importer's Processing of the Transferred Data is subject to UK Data Protection Laws, it agrees that:

13.1.1 UK Data Protection Laws apply to its Processing of the Transferred Data, and the ICO has jurisdiction over it in that respect; and

13.1.2 it has and will comply with the UK Data Protection Laws in relation to the Processing of the Transferred Data.

13.2 If Section 13.1 applies and the Importer complies with Section 13.1, it does not need to comply with:

- Section 14 (Importer's obligations to comply with key data protection principles);
- Section 15 (What happens if there is an Importer Personal Data Breach);
- Section 15 (How Relevant Data Subjects can exercise their data subject rights); and
- Section 21 (How Relevant Data Subjects can exercise their data subject rights – if the Importer is the Exporter's Processor or Sub-Processor).

14. Importer's obligations to comply with key data protection principles

14.1 The Importer does not need to comply with this Section 14 if it is the Exporter's Processor or Sub-Processor.

14.2 The Importer must:

14.2.1 ensure that the Transferred Data it Processes is adequate, relevant and limited to what is necessary for the Purpose;

14.2.2 ensure that the Transferred Data it Processes is accurate and (where necessary) kept up to date, and (where appropriate considering the Purposes) correct or delete any inaccurate Transferred Data it becomes aware of Without Undue Delay; and

14.2.3 ensure that it Processes the Transferred Data for no longer than is reasonably necessary for the Purpose.

15. What happens if there is an Importer Personal Data Breach

15.1 If there is an Importer Personal Data Breach, the Importer must:

15.1.1 take reasonable steps to fix it, including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again. If the Importer is the Exporter's Processor or Sub-Processor: these steps must comply with the Exporter's instructions and the Linked Agreement and be in co-operation with the Exporter and any Third Party Controller; and

15.1.2 ensure that the Security Requirements continue to provide (or are changed in accordance with this IDTA so they do provide) a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

15.2 If the Importer is a Processor or Sub-Processor: if there is an Importer Personal Data Breach, the Importer must:

15.2.1 notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

15.2.1.1 a description of the nature of the Importer Personal Data Breach;

15.2.1.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;

15.2.1.3 likely consequences of the Importer Personal Data Breach;

15.2.1.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;

15.2.1.5 contact point for more information; and

15.2.1.6 any other information reasonably requested by the Exporter,

15.2.2 if it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay; and

15.2.3 assist the Exporter (and any Third Party Controller) so the Exporter (or any Third Party Controller) can inform Relevant Data Subjects or the ICO or any other relevant regulator or authority about the Importer Personal Data Breach Without Undue Delay.

15.3 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a risk to the rights or freedoms of any Relevant Data Subject the Importer must notify the Exporter Without Undue Delay after becoming aware of the breach, providing the following information:

15.3.1 a description of the nature of the Importer Personal Data Breach;

15.3.2 (if and when possible) the categories and approximate number of Data Subjects and Transferred Data records concerned;

15.3.3 likely consequences of the Importer Personal Data Breach;

15.3.4 steps taken (or proposed to be taken) to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Appropriate Safeguards are in place;

15.3.5 contact point for more information; and

15.3.6 any other information reasonably requested by the Exporter.

If it is not possible for the Importer to provide all the above information at the same time, it may do so in phases, Without Undue Delay.

15.4 If the Importer is a Controller: if the Importer Personal Data Breach is likely to result in a high risk to the rights or freedoms of any Relevant Data Subject, the Importer must inform those Relevant Data Subjects Without Undue Delay, except in so far as it requires disproportionate effort, and provided the Importer ensures that there is a public communication or similar measures whereby Relevant Data Subjects are informed in an equally effective manner.

15.5 The Importer must keep a written record of all relevant facts relating to the Importer Personal Data Breach, which it will provide to the Exporter and the ICO on request.

This record must include the steps it takes to fix the Importer Personal Data Breach (including to minimise the harmful effects on Relevant Data Subjects, stop it from continuing, and prevent it happening again) and to ensure that Security Requirements continue to provide a level of security which is appropriate to the risk of a Personal Data Breach occurring and the impact on Relevant Data Subjects of such a Personal Data Breach.

16. Transferring on the Transferred Data

16.1 The Importer may only transfer on the Transferred Data to a third party if it is permitted to do so in Table 2: Transfer Details Table, the transfer is for the Purpose, the transfer does not breach the Linked Agreement, and one or more of the following apply:

16.1.1 the third party has entered into a written contract with the Importer containing the same level of protection for Data Subjects as contained in this IDTA (based on the role of the recipient as controller or processor), and the Importer has conducted a risk assessment to ensure that the Appropriate Safeguards will be protected by that contract; or

16.1.2 the third party has been added to this IDTA as a Party; or

16.1.3 if the Importer was in the UK, transferring on the Transferred Data would comply with Article 46 UK GDPR; or

16.1.4 if the Importer was in the UK transferring on the Transferred Data would comply with one of the exceptions in Article 49 UK GDPR; or

16.1.5 the transfer is to the UK or an Adequate Country.

16.2 The Importer does not need to comply with Section 16.1 if it is transferring on Transferred Data and/or allowing access to the Transferred Data in accordance with Section 23 (Access Requests and Direct Access).

17. Importer’s responsibility if it authorises others to perform its obligations

17.1 The Importer may sub-contract its obligations in this IDTA to a Processor or Sub-Processor (provided it complies with Section 16).

17.2 If the Importer is the Exporter’s Processor or Sub-Processor: it must also comply with the Linked Agreement or be with the written consent of the Exporter.

17.3 The Importer must ensure that any person or third party acting under its authority, including a Processor or Sub-Processor, must only Process the Transferred Data on its instructions.

17.4 The Importer remains fully liable to the Exporter, the ICO and Relevant Data Subjects for its obligations under this IDTA where it has sub-contracted any obligations to its Processors and Sub-Processors or authorised an employee or other person to perform them (and references to the Importer in this context will include references to its Processors, Sub-Processors or authorised persons).

18. The right to a copy of the IDTA

18.1 If a Party receives a request from a Relevant Data Subject for a copy of this IDTA:

18.1.1 it will provide the IDTA to the Relevant Data Subject and inform the other Party, as soon as reasonably possible;

18.1.2 it does not need to provide copies of the Linked Agreement, but it must provide all the information from those Linked Agreements referenced in the Tables;

18.1.3 it may redact information in the Tables or the information provided from the Linked Agreement if it is reasonably necessary to protect business secrets or confidential information, so long as it provides the Relevant Data Subject with a summary of those redactions so that the Relevant Data Subject can understand the content of the Tables or the information provided from the Linked Agreement.

19. The right to Information about the Importer and its Processing

19.1 The Importer does not need to comply with this Section 19 if it is the Exporter’s Processor or Sub-Processor.

19.2 The Importer must ensure that each Relevant Data Subject is provided with details of:

- the Importer (including contact details and the Importer Data Subject Contact);
- the Purposes; and
- any recipients (or categories of recipients) of the Transferred Data;

The Importer can demonstrate it has complied with this Section 19.2 if the information is given (or has already been given) to the Relevant Data Subjects by the Exporter or another party.

The Importer does not need to comply with this Section 19.2 in so far as to do so would be impossible or involve a disproportionate effort, in which case, the Importer must make the information publicly available.

19.3 The Importer must keep the details of the Importer Data Subject Contact up to date and publicly available. This includes notifying the Exporter in writing of any such changes.

19.4 The Importer must make sure those contact details are always easy to access for all Relevant Data Subjects and be able to easily communicate with Data Subjects in the English language Without Undue Delay.

20. How Relevant Data Subjects can exercise their data subject rights

20.1 The Importer does not need to comply with this Section 20 if it is the Exporter’s Processor or Sub-Processor.

20.2 If an individual requests, the Importer must confirm whether it is Processing their Personal Data as part of the Transferred Data.

20.3 The following Sections of this Section 20, relate to a Relevant Data Subject’s Personal Data which forms part of the Transferred Data the Importer is Processing.

20.4 If the Relevant Data Subject requests, the Importer must provide them with a copy of their Transferred Data:

20.4.1 Without Undue Delay (and in any event within one month);

20.4.2 at no greater cost to the Relevant Data Subject than it would be able to charge if it were subject to the UK Data Protection Laws;

20.4.3 in clear and plain English that is easy to understand; and

20.4.4 in an easily accessible form

together with

20.4.5 (if needed) a clear and plain English explanation of the Transferred Data so that it is understandable to the Relevant Data Subject; and

20.4.6 information that the Relevant Data Subject has the right to bring a claim for compensation under this IDTA.

20.5 If a Relevant Data Subject requests, the Importer must:

20.5.1 rectify inaccurate or incomplete Transferred Data;

20.5.2 erase Transferred Data if it is being Processed in breach of this IDTA;

20.5.3 cease using it for direct marketing purposes; and

20.5.4 comply with any other reasonable request of the Relevant Data Subject, which the Importer would be required to comply with if it were subject to the UK Data Protection Laws.

20.6 The Importer must not use the Transferred Data to make decisions about the Relevant Data Subject based solely on automated processing, including profiling (the "Decision-Making"), which produce legal effects concerning the Relevant Data Subject or similarly significantly affects them, except if it is permitted by Local Law and:

20.6.1 the Relevant Data Subject has given their explicit consent to such Decision-Making; or

20.6.2 Local Law has safeguards which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK; or

20.6.3 the Extra Protection Clauses provide safeguards for the Decision-Making which provide sufficiently similar protection for the Relevant Data Subjects in relation to such Decision-Making, as to the relevant protection the Relevant Data Subject would have if such Decision-Making was in the UK.

21. How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor

21.1 Where the Importer is the Exporter's Processor or Sub-Processor: If the Importer receives a request directly from an individual which relates to the Transferred Data it must pass that request on to the Exporter Without Undue Delay. The Importer must only respond to that individual as authorised by the Exporter or any Third Party Controller.

22. Rights of Relevant Data Subjects are subject to the exemptions in the UK Data Protection Laws

22.1 The Importer is not required to respond to requests or provide information or notifications under Sections 18, 19, 20, 21 and 23 if:

22.1.1 it is unable to reasonably verify the identity of an individual making the request; or

22.1.2 the requests are manifestly unfounded or excessive, including where requests are repetitive. In that case the Importer may refuse the request or may charge the Relevant Data Subject a reasonable fee; or

22.1.3 a relevant exemption would be available under UK Data Protection Laws, were the Importer subject to the UK Data Protection Laws.

If the Importer refuses an individual's request or charges a fee under Section 22.1.2 it will set out in writing the reasons for its refusal or charge, and inform the Relevant Data Subject that they are entitled to bring a claim for compensation under this IDTA in the case of any breach of this IDTA.

How to give third parties access to Transferred Data under Local Laws

23. Access requests and direct access

23.1 In this Section 23 an "Access Request" is a legally binding request (except for requests only binding by contract law) to access any Transferred Data and "Direct Access" means direct access to any Transferred Data by public authorities of which the Importer is aware.

23.2 The Importer may disclose any requested Transferred Data in so far as it receives an Access Request, unless in the circumstances it is reasonable for it to challenge that Access Request on the basis there are significant grounds to believe that it is unlawful.

23.3 In so far as Local Laws allow and it is reasonable to do so, the Importer will Without Undue Delay provide the following with relevant information about any Access Request or Direct Access: the Exporter; any Third Party Controller; and where the Importer is a Controller, any Relevant Data Subjects.

23.4 In so far as Local Laws allow, the Importer must:

23.4.1 make and keep a written record of Access Requests and Direct Access, including (if known): the dates, the identity of the requestor/accessor, the purpose of the Access Request or Direct Access, the type of data requested or accessed, whether it was challenged or appealed, and the outcome; and the Transferred Data which was provided or accessed; and

23.4.2 provide a copy of this written record to the Exporter on each Review Date and any time the Exporter or the ICO reasonably requests.

24. Giving notice

24.1 If a Party is required to notify any other Party in this IDTA it will be marked for the attention of the relevant Key Contact and sent by e-mail to the e-mail address given for the Key Contact.

24.2 If the notice is sent in accordance with Section 24.1, it will be deemed to have been delivered at the time the e-mail was sent, or if that time is outside of the receiving Party's normal business hours, the receiving Party's next normal business day, and provided no notice of non-delivery or bounce back is received.

24.3 The Parties agree that any Party can update their Key Contact details by giving 14 days' (or more) notice in writing to the other Party.

25. General clauses

25.1 In relation to the transfer of the Transferred Data to the Importer and the Importer's Processing of the Transferred Data, this IDTA and any Linked Agreement:

25.1.1 contain all the terms and conditions agreed by the Parties; and

25.1.2 override all previous contacts and arrangements, whether oral or in writing.

25.2 If one Party made any oral or written statements to the other before entering into this IDTA (which are not written in this IDTA) the other Party confirms that it has not relied on those statements and that it will not have a legal remedy if those statements are untrue or incorrect, unless the statement was made fraudulently.

25.3 Neither Party may novate, assign or obtain a legal charge over this IDTA (in whole or in part) without the written consent of the other Party, which may be set out in the Linked Agreement.

25.4 Except as set out in Section 17.1, neither Party may sub contract its obligations under this IDTA without the written consent of the other Party, which may be set out in the Linked Agreement.

25.5 This IDTA does not make the Parties a partnership, nor appoint one Party to act as the agent of the other Party.

25.6 If any Section (or part of a Section) of this IDTA is or becomes illegal, invalid or unenforceable, that will not affect the legality, validity and enforceability of any other Section (or the rest of that Section) of this IDTA.

25.7 If a Party does not enforce, or delays enforcing, its rights or remedies under or in relation to this IDTA, this will not be a waiver of those rights or remedies. In addition, it will not restrict that Party's ability to enforce those or any other right or remedy in future.

25.8 If a Party chooses to waive enforcing a right or remedy under or in relation to this IDTA, then this waiver will only be effective if it is made in writing. Where a Party provides such a written waiver:

25.8.1 it only applies in so far as it explicitly waives specific rights or remedies;

25.8.2 it shall not prevent that Party from exercising those rights or remedies in the future (unless it has explicitly waived its ability to do so); and

25.8.3 it will not prevent that Party from enforcing any other right or remedy in future.

What happens if there is a breach of this IDTA?

26. Breaches of this IDTA

26.1 Each Party must notify the other Party in writing (and with all relevant details) if it:

26.1.1 has breached this IDTA; or

26.1.2 it should reasonably anticipate that it may breach this IDTA, and provide any information about this which the other Party reasonably requests.

26.2 In this IDTA "Significant Harmful Impact" means that there is more than a minimal risk of a breach of the IDTA causing (directly or indirectly) significant damage to any Relevant Data Subject or the other Party.

27. Breaches of this IDTA by the Importer

27.1 If the Importer has breached this IDTA, and this has a Significant Harmful Impact, the Importer must take steps Without Undue Delay to end the Significant Harmful Impact, and if that is not possible to reduce the Significant Harmful Impact as much as possible.

27.2 Until there is no ongoing Significant Harmful Impact on Relevant Data Subjects:

27.2.1 the Exporter must suspend sending Transferred Data to the Importer;

27.2.2 If the Importer is the Exporter's Processor or Sub-Processor: if the Exporter requests, the importer must securely delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter); and

27.2.3 if the Importer has transferred on the Transferred Data to a third party receiver under Section 16, and the breach has a Significant Harmful Impact on Relevant Data Subject when it is Processed by or on behalf of that third party receiver, the Importer must:

27.2.3.1 notify the third party receiver of the breach and suspend sending it Transferred Data; and

27.2.3.2 if the third party receiver is the Importer's Processor or Sub-Processor: make the third party receiver securely delete all Transferred Data being Processed by it or on its behalf, or securely return it to the Importer (or a third party named by the Importer).

27.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Exporter must end this IDTA under Section 30.1.

28. Breaches of this IDTA by the Exporter

28.1 If the Exporter has breached this IDTA, and this has a Significant Harmful Impact, the Exporter must take steps Without Undue Delay to end the Significant Harmful Impact and if that is not possible to reduce the Significant Harmful Impact as much as possible.

28.2 Until there is no ongoing risk of a Significant Harmful Impact on Relevant Data Subjects, the Exporter must suspend sending Transferred Data to the Importer.

28.3 If the breach cannot be corrected Without Undue Delay, so there is no ongoing Significant Harmful Impact on Relevant Data Subjects, the Importer must end this IDTA under Section 30.1.

Ending the IDTA

29. How to end this IDTA without there being a breach

29.1 The IDTA will end:

29.1.1 at the end of the Term stated in Table 2: Transfer Details; or

29.1.2 if in Table 2: Transfer Details, the Parties can end this IDTA by providing written notice to the other: at the end of the notice period stated;

29.1.3 at any time that the Parties agree in writing that it will end; or

29.1.4 at the time set out in Section 29.2.

29.2 If the ICO issues a revised Approved IDTA under Section 5.4, if any Party selected in Table 2 "Ending the IDTA when the Approved IDTA changes", will as a direct result of the changes in the Approved IDTA have a substantial, disproportionate and demonstrable increase in:

29.2.1 its direct costs of performing its obligations under the IDTA; and/or

29.2.2 its risk under the IDTA,

and in either case it has first taken reasonable steps to reduce that cost or risk so that it is not substantial and disproportionate, that Party may end the IDTA 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 IDTA.

30. How to end this IDTA if there is a breach

30.1 A Party may end this IDTA immediately by giving the other Party written notice if:

30.1.1 the other Party has breached this IDTA and this has a Significant Harmful Impact. This includes repeated minor breaches which taken together have a Significant Harmful Impact, and

30.1.1.1 the breach can be corrected so there is no Significant Harmful Impact, and the other Party has failed to do so Without Undue Delay (which cannot be more than 14 days of being required to do so in writing); or

30.1.1.2 the breach and its Significant Harmful Impact cannot be corrected;

30.1.2 the Importer can no longer comply with Section 8.3, as there are Local Laws which mean it cannot comply with this IDTA and this has a Significant Harmful Impact.

31. What must the Parties do when the IDTA ends?

31.1 If the parties wish to bring this IDTA to an end or this IDTA ends in accordance with any provision in this IDTA, but the Importer must comply with a Local Law which requires it to continue to keep any Transferred Data then this IDTA will remain in force in respect of any retained Transferred Data for as long as the retained Transferred Data is retained, and the Importer must:

31.1.1 notify the Exporter Without Undue Delay, including details of the relevant Local Law and the required retention period;

31.1.2 retain only the minimum amount of Transferred Data it needs to comply with that Local Law, and the Parties must ensure they maintain the Appropriate Safeguards, and change the Tables and Extra Protection Clauses, together with any TRA to reflect this; and

31.1.3 stop Processing the Transferred Data as soon as permitted by that Local Law and the IDTA will then end and the rest of this Section 29 will apply.

31.2 When this IDTA ends (no matter what the reason is):

31.2.1 the Exporter must stop sending Transferred Data to the Importer; and

31.2.2 if the Importer is the Exporter's Processor or Sub-Processor: the Importer must delete all Transferred Data or securely return it to the Exporter (or a third party named by the Exporter), as instructed by the Exporter;

31.2.3 if the Importer is a Controller and/or not the Exporter's Processor or Sub-Processor: the Importer must securely delete all Transferred Data.

31.2.4 the following provisions will continue in force after this IDTA ends (no matter what the reason is):

- **Section 1** (This IDTA and Linked Agreements);
- **Section 2** (Legal Meaning of Words);
- **Section 6** (Understanding this IDTA);
- **Section 7** (Which laws apply to this IDTA);
- **Section 10** (The ICO);
- Sections 11.1 and 11.4 (Exporter's obligations);
- Sections 12.1.2, 12.1.3, 12.1.4, 12.1.5 and 12.1.6 (General Importer obligations);
- Section 13.1 (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 17** (Importer's responsibility if it authorised others to perform its obligations);
- **Section 24** (Giving notice);
- **Section 25** (General clauses);
- **Section 31** (What must the Parties do when the IDTA ends);
- **Section 32** (Your liability);
- **Section 33** (How Relevant Data Subjects and the ICO may bring legal claims);
- **Section 34** (Courts legal claims can be brought in);
- **Section 35** (Arbitration); and
- **Section 36** (Legal Glossary).

How to bring a legal claim under this IDTA

32. Your liability

32.1 The Parties remain fully liable to Relevant Data Subjects for fulfilling their obligations under this IDTA and (if they apply) under UK Data Protection Laws.

32.2 Each Party (in this Section, "Party One") agrees to be fully liable to Relevant Data Subjects for the entire damage suffered by the Relevant Data Subject, caused directly or indirectly by:

32.2.1 Party One's breach of this IDTA; and/or

32.2.2 where Party One is a Processor, Party One's breach of any provisions regarding its Processing of the Transferred Data in the Linked Agreement;

32.2.3 where Party One is a Controller, a breach of this IDTA by the other Party if it involves Party One's Processing of the Transferred Data (no matter how minimal)

in each case unless Party One can prove it is not in any way responsible for the event giving rise to the damage.

32.3 If one Party has paid compensation to a Relevant Data Subject under Section 32.2, it is entitled to claim back from the other Party that part of the compensation corresponding to the other Party's responsibility for the damage, so that the compensation is fairly divided between the Parties.

32.4 The Parties do not exclude or restrict their liability under this IDTA or UK Data Protection Laws, on the basis that they have authorised anyone who is not a Party (including a Processor) to perform any of their obligations, and they will remain responsible for performing those obligations.

33. How Relevant Data Subjects and the ICO may bring legal claims

33.1 The Relevant Data Subjects are entitled to bring claims against the Exporter and/or Importer for breach of the following (including where their Processing of the Transferred Data is involved in a breach of the following by either Party):

- **Section 1** (This IDTA and Linked Agreements);
- **Section 3** (You have provided all the information required by Part one: Tables and Part two: Extra Protection Clauses);
- **Section 8** (The Appropriate Safeguards);
- **Section 9** (Reviews to ensure the Appropriate Safeguards continue);
- **Section 11** (Exporter's obligations);
- **Section 12** (General Importer Obligations);
- **Section 13** (Importer's obligations if it is subject to UK Data Protection Laws);
- **Section 14** (Importer's obligations to comply with key data protection laws);
- **Section 15** (What happens if there is an Importer Personal Data Breach);
- **Section 16** (Transferring on the Transferred Data);
- **Section 17** (Importer's responsibility if it authorises others to perform its obligations);
- **Section 18** (The right to a copy of the IDTA);
- **Section 19** (The Importer's contact details for the Relevant Data Subjects);
- **Section 20** (How Relevant Data Subjects can exercise their data subject rights);
- **Section 21** (How Relevant Data Subjects can exercise their data subject rights– if the Importer is the Exporter's Processor or Sub-Processor);
- **Section 23** (Access Requests and Direct Access);
- **Section 26** (Breaches of this IDTA);
- **Section 27** (Breaches of this IDTA by the Importer);
- **Section 28** (Breaches of this IDTA by the Exporter);
- **Section 30** (How to end this IDTA if there is a breach);
- **Section 31** (What must the Parties do when the IDTA ends); and
- any other provision of the IDTA which expressly or by implication benefits the Relevant Data Subjects.

33.2 The ICO is entitled to bring claims against the Exporter and/or Importer for breach of the following Sections: Section 10 (The ICO), Sections 11.1 and 11.2 (Exporter's obligations), Section 12.1.6 (General Importer obligations) and Section 13 (Importer's obligations if it is subject to UK Data Protection Laws).

33.3 No one else (who is not a Party) can enforce any part of this IDTA (including under the Contracts (Rights of Third Parties) Act 1999).

33.4 The Parties do not need the consent of any Relevant Data Subject or the ICO to make changes to this IDTA, but any changes must be made in accordance with its terms.

33.5 In bringing a claim under this IDTA, a Relevant Data Subject may be represented by a not-for-profit body, organisation or association under the same conditions set out in Article 80(1) UK GDPR and sections 187 to 190 of the Data Protection Act 2018.

34. Courts legal claims can be brought in

34.1 The courts of the UK country set out in Table 2: Transfer Details have non-exclusive jurisdiction over any claim in connection with this IDTA (including non-contractual claims).

34.2 The Exporter may bring a claim against the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.

34.3 The Importer may only bring a claim against the Exporter in connection with this IDTA (including non-contractual claims) in the courts of the UK country set out in the Table 2: Transfer Details

34.4 Relevant Data Subjects and the ICO may bring a claim against the Exporter and/or the Importer in connection with this IDTA (including non-contractual claims) in any court in any country with jurisdiction to hear the claim.

34.5 Each Party agrees to provide to the other Party reasonable updates about any claims or complaints brought against it by a Relevant Data Subject or the ICO in connection with the Transferred Data (including claims in arbitration).

35. Arbitration

35.1 Instead of bringing a claim in a court under Section 34, any Party, or a Relevant Data Subject may elect to refer any dispute arising out of or in connection with this IDTA (including non-contractual claims) to final resolution by arbitration under the Rules of the London Court of International Arbitration, and those Rules are deemed to be incorporated by reference into this Section 35.

35.2 The Parties agree to submit to any arbitration started by another Party or by a Relevant Data Subject in accordance with this Section 35.

35.3 There must be only one arbitrator. The arbitrator (1) must be a lawyer qualified to practice law in one or more of England and Wales, or Scotland, or Northern Ireland and (2) must have experience of acting or advising on disputes relating to UK Data Protection Laws.

35.4 London shall be the seat or legal place of arbitration. It does not matter if the Parties selected a different UK country as the ‘primary place for legal claims to be made’ in Table 2: Transfer Details.

35.5 The English language must be used in the arbitral proceedings.

35.6 English law governs this Section 35. This applies regardless of whether or not the parties selected a different UK country’s law as the ‘UK country’s law that governs the IDTA’ in Table 2: Transfer Details.

36. Legal Glossary

Word or Phrase	**Legal definition** **(this is how this word or phrase must be interpreted in the IDTA)**
Access Request	As defined in Section 23, as a legally binding request (except for requests only binding by contract law) to access any Transferred Data.
Adequate Country	A third country, or: • a territory; • one or more sectors or organisations within a third country; • an international organisation;

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
	which the Secretary of State has specified by regulations provides an adequate level of protection of Personal Data in accordance with Section 17A of the Data Protection Act 2018.
Appropriate Safeguards	The standard of protection over the Transferred Data and of the Relevant Data Subject's 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 IDTA	The template IDTA A1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4.
Commercial Clauses	The commercial clauses set out in Part three.
Controller	As defined in the UK GDPR.
Damage	All material and non-material loss and damage.
Data Subject	As defined in the UK GDPR.
Decision-Making	As defined in Section 20.6, as decisions about the Relevant Data Subjects based solely on automated processing, including profiling, using the Transferred Data.
Direct Access	As defined in Section 23 as direct access to any Transferred Data by public authorities of which the Importer is aware.
Exporter	The exporter identified in Table 1: Parties & Signature.
Extra Protection Clauses	The clauses set out in Part two: Extra Protection Clauses.
ICO	The Information Commissioner.
Importer	The importer identified in Table 1: Parties & Signature.
Importer Data Subject Contact	The Importer Data Subject Contact identified in Table 1: Parties & Signature, which may be updated in accordance with Section 19.
Importer Information	As defined in Section 8.3.1, as all relevant information regarding Local Laws and practices and the protections and risks which apply to the Transferred Data when it is Processed by the Importer, including for the Exporter to carry out any TRA.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Importer Personal Data Breach	A 'personal data breach' as defined in UK GDPR, in relation to the Transferred Data when Processed by the Importer.
Linked Agreement	The linked agreements set out in Table 2: Transfer Details (if any).
Local Laws	Laws which are not the laws of the UK and which bind the Importer.
Mandatory Clauses	Part four: Mandatory Clauses of this IDTA.
Notice Period	As set out in Table 2: Transfer Details.
Party/Parties	The parties to this IDTA as set out in Table 1: Parties & Signature.
Personal Data	As defined in the UK GDPR.
Personal Data Breach	As defined in the UK GDPR.
Processing	As defined in the UK GDPR. When the IDTA refers to Processing by the Importer, this includes where a third party Sub-Processor of the Importer is Processing on the Importer's behalf.
Processor	As defined in the UK GDPR.
Purpose	The 'Purpose' set out in Table 2: Transfer Details, including any purposes which are not incompatible with the purposes stated or referred to.
Relevant Data Subject	A Data Subject of the Transferred Data.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR
Review Dates	The review dates or period for the Security Requirements set out in Table 2: Transfer Details, and any review dates set out in any revised Approved IDTA.
Significant Harmful Impact	As defined in Section 26.2 as where there is more than a minimal risk of the breach causing (directly or indirectly) significant harm to any Relevant Data Subject or the other Party.
Special Category Data	As described in the UK GDPR, together with criminal conviction or criminal offence data.
Start Date	As set out in Table 1: Parties and signature.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
Sub-Processor	A Processor appointed by another Processor to Process Personal Data on its behalf. This includes Sub-Processors of any level, for example a Sub-Sub-Processor.
Tables	The Tables set out in Part one of this IDTA.
Term	As set out in Table 2: Transfer Details.
Third Party Controller	The Controller of the Transferred Data where the Exporter is a Processor or Sub-Processor If there is not a Third Party Controller this can be disregarded.
Transfer Risk Assessment or TRA	A risk assessment in so far as it is required by UK Data Protection Laws to demonstrate that the IDTA provides the Appropriate Safeguards
Transferred Data	Any Personal Data which the Parties transfer, or intend to transfer under this IDTA, as described in Table 2: Transfer Details
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.
Without Undue Delay	Without undue delay, as that phase is interpreted in the UK GDPR.

Alternative Part 4 Mandatory Clauses:

Mandatory Clauses	Part 4: Mandatory Clauses of the Approved IDTA, being the template IDTA A.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 5.4 of those Mandatory Clauses.