Epicor Software Corporation
Vendor Data Processing Addendum (UK Version)
(Updated 10 March 2022)

Based on the UK General Data Protection Regulation (UK GDPR) and s 119A (1) Data Protection Act 2018

This Data Processing Addendum ("**DPA**") (which is effective on and from the effective date of the Vendor Agreement to which it is attached and/or incorporated) forms part of the agreements between **Epicor Software (UK) Limited (Epicor)** and "**Vendor**," for the provision of Vendor's Services to Epicor (identified collectively either as the "Services" or otherwise in the applicable agreement, and hereinafter defined as the "**Services**"), wherein such agreements are hereinafter collectively defined as the "**Agreement**," and whereby this DPA reflects the parties' agreement with regard to the Processing of Personal Data by Vendor as regulated by the United Kingdom's version of the General Data Protection Regulation (UK GDPR) (as defined below).

By competing (and submitting) Epicor's Vendors Data Processing Agreement assessment (that references this DPA and its terms) through OneTrust, Vendor acknowledges that it is entering into 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 Vendor processes Personal Data for which such Authorized Affiliates qualify as a Processor. In providing the Services (as defined below) to Epicor pursuant to the Agreement, Vendor may Process Personal Data on behalf of Epicor, 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, which incorporates Annexes I to III of the EU Standard Contractual Clauses (in force on and from 27 June 2021)

   (c) the Standard Data Protection Clauses (issued by the Information Commissioner under s 119 A (1) of the Data Protection Act 2018) otherwise known as an International Data Transfer Agreement (version A1.0 in force on and from 21 March 2022); and

   (d) the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0, in force 21 March 2022).

2. **By completing (and submitting) Epicor's Vendor Data Processing Agreement assessment (that references this DPA and its terms) through OneTrust, Vendor agrees to be bound by the terms and conditions of this DPA.**

3. **Upon receipt and approval, by Epicor, of a validly submitted DPA through OneTrust, this DPA shall come into effect and legally bind the parties.**

APPLICATION OF THIS DPA

If the Vendor entity completing the DPA Assessment through OneTrust 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 that is party to the Agreement is party to this DPA.

If the Vendor entity completing the DPA Assessment through OneTrust is not a party to the Agreement, then this DPA is not valid and therefore is not legally binding. Such entity should request that the Vendor entity who 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 of a Party signing the Agreement and/or this DPA. "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 Epicor Affiliate which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Epicor and Vendor but has not signed its own Agreement with Vendor.

"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data and may include Epicor.

"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 January 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 above and in the signature block below) and in the absence thereof **Epicor Software (UK) Limited**, a company incorporated under the laws of England and Wales and its primary address at 6 Arlington Square West, Bracknell, Berkshire RG12 1PU.

"**Epicor Data**" means all electronic data submitted by or on behalf of Epicor, or an Authorized Affiliate, to Vendor as part of the Services.

"**UK GDPR**" has the meaning given to it in section 3 (10) (as supplemented by section 205(4) of the Data Protection Act 2018.

"**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 Epicor or an Authorized Affiliate to Vendor in connection with Vendor 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 a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the controller, including Vendor when Epicor is in the role of a Controller.

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

"Services" means software support Services, professional consulting Services or other Services provided by Vendor and/or performed by Vendor for and on behalf of Epicor and its affiliates.

"**Standard Contractual Clauses**" means the Standard Data Protection Clauses (issued by the Information Commissioner under s 119 A (1) of the Data Protection Act 2018) otherwise known as an International Data Transfer Agreement (version A1.0 in force on and from 21 March 2022); as supplemented by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0, in force 21 March 2022) 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, including Vendor when Epicor is in the role of a Processor and any Sub-processors engaged by Vendor in connection with the Epicor Data.

"**Supervisory Authority**" means the UK Information Commissioner Office (ICO).

DPA TERMS

Epicor and Vendor hereby enter into this DPA effective as of the date Vendor submits it completed Vendor DPA Assessment through OneTrust. This DPA is incorporated into and forms part of the Agreement.

1. **Provision of the Services**. Vendor provides the Services to Epicor under the Agreement. In connection with the Services, the parties anticipate that Vendor may Process Epicor Data that contains Personal Data relating to Data Subjects.

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

3. **Epicor Responsibilities**. Epicor 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, Epicor's instructions to Vendor for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. As between the parties, Epicor shall have sole responsibility for the accuracy, quality, and legality of Personal Data provided to Vendor and the means by which Epicor acquired Personal Data.

4. **Processing Purposes**. Vendor shall keep Personal Data confidential and shall only Process Personal Data on behalf of and in accordance with Epicor's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Epicor in its use of the Services; and (iii) Processing to comply with other documented, reasonable instructions provided by Epicor (for example, via email) where such instructions are consistent with the terms of the Agreement. Vendor shall not be required to comply with or observe Epicor's instructions if such instructions would violate the UK GDPR or other UK law or data protection provisions.

5. **Scope of Processing**. The subject-matter of Processing of Personal Data by Vendor 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, Vendor shall promptly notify Epicor if Vendor 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"). Factoring into account the nature of the Processing, Vendor shall assist Epicor by appropriate organizational and technical measures, insofar as this is possible, for the fulfilment of Epicor's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations and its agreements with its customers. In addition, to the extent Epicor, in its use of the Services, does not have the ability to address a Data Subject Request, Vendor shall, upon Epicor's request, provide commercially reasonable efforts to assist Epicor in responding to such Data Subject Request, to the extent that Vendor is legally authorized to do so, and the response to such Data Subject Request is required under Data Protection Laws and Regulations and Epicor's agreements with its customers.

7. **Vendor Personnel**. Vendor 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. Vendor shall take commercially reasonable steps to ensure the reliability of any Vendor personnel engaged in the Processing of Personal Data. Vendor shall ensure that Vendor'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**. Vendor shall have appointed, or shall appoint, a data protection officer if and whereby such appointment is required by Data Protection Laws and Regulations.

9. **Vendor's Sub-processors**. Epicor has instructed or authorized the use of Sub- processors to assist Vendor with respect to the performance of Vendor's obligations under the Agreement. Upon written request of Epicor, Vendor will provide to Epicor a list of its then-current Sub-processors. Epicor acknowledges and agrees that (a) Vendor's Affiliates may be retained as Sub-processors; and (b) Vendor and Vendor's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Vendor shall provide notification to Epicor of any and all new Sub-processors before authorizing any and all new Sub-processors to process Personal Data in connection with the provision of the applicable Services. In order to exercise its right to object to Vendor's use of a new Sub-processor, Epicor shall notify Vendor promptly in writing within thirty (30) business days after receipt of Vendor's notice. In the event Epicor objects to a new Sub-processor, and that objection is not unreasonable, Vendor will use reasonable efforts to make available to Epicor a change in the Services or recommend a commercially reasonable change to Epicor's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Epicor. If Vendor is unable to make available such change within a reasonable time period, which shall not exceed thirty (30) days of Epicor's objection, Epicor may terminate the applicable Order Form(s) with respect only to those aspects of the Services which cannot be provided by Vendor without the use of the objected-to new Sub-processor by providing written notice to Vendor. Vendor will refund Epicor 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. The parties agree that the copies of the Sub-processor agreements that must be provided by Vendor to Epicor pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Vendor beforehand; and, that such copies will be provided by Vendor, in a manner to be determined in its discretion, only upon request by Epicor.

10. **Liability for Sub-processors**. Vendor shall be liable for the acts and omissions of its Sub-processors to the same extent Vendor 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**. Vendor 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, Epicor Data), confidentiality, and integrity of Epicor Data. Vendor regularly monitors compliance with these measures. Vendor will not materially decrease the overall security of the Services during Epicor's and/or Authorized Affiliates' subscription term.

12. **Third-Party Certifications and Audit Results**. Upon Epicor's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Vendor shall make available to Epicor a copy of Vendor's then-most recent third-party certifications or audit results, as applicable.

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

14. **Return of Epicor Data**. Vendor shall return Epicor Data to Epicor and, to the extent allowed by applicable law, delete Epicor Data upon Epicor's request, unless the retention of the data is requested from Vendor according to mandatory statutory laws.

15. **Authorized Affiliates**. The parties agree that, by executing the DPA, Epicor 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 Vendor 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 Epicor.

16. **Communications**. The Epicor entity that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Vendor 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.

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 Vendor, 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. Each reference to the DPA herein means this DPA including its Appendices.

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

20. **Data Protection Impact Assessment**. Upon Epicor's request, Vendor shall provide Epicor with reasonable cooperation and assistance needed to fulfil Epicor's obligation under the UK GDPR to carry out a data protection impact assessment related to Epicor's use of the Services to the extent such assessment is required under applicable law, to the extent Epicor does not otherwise have access to the relevant information, and to the extent such information is available to Vendor. Vendor shall provide reasonable assistance to Epicor in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 21 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 Vendor does not and will not rise to the level of requiring a Data Protection Impact Assessment under applicable law.

21. **Standard Contractual Clauses**. The Standard Contractual Clauses (set forth at **Schedule 2** to this DPA) apply to the legal entity that is bound by the Standard Contractual Clauses as a data exporter (being Epicor Software (UK) Limited) and the vendor entity (and all Affiliates) that is bound by the Standard Contractual Clauses as a data importer. **By agreeing to the terms of this DPA through OneTrust**, the parties will be deemed to have executed the Standard Contractual Clauses (set forth at Schedule 2 to this DPA), the terms and conditions of which are incorporated herein by reference and form a part of this DPA.

22. **Epicor's Processing Instructions**. This DPA and the Agreement are Epicor's complete and final instructions at the time of signature of the Agreement to Vendor for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by Epicor to process Personal Data: (a) Processing in accordance with the Agreement and applicable Order Form(s); (b) Processing initiated by Epicor in its use of the Services; and (c) Processing to comply with other reasonable instructions provided by Epicor (e.g., via email) where such instructions are consistent with the terms of the Agreement.

23 **Audits**. The parties agree that the audits shall be carried out in accordance with the following specifications: following Epicor's written request, and subject to the confidentiality obligations set forth in the Agreement, Vendor shall make available to Epicor information regarding Vendor's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits to the extent that Vendor makes them generally available to its customers. Epicor may contact Vendor in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. Epicor shall reimburse Vendor for any time expended for any such on-site audit at the Vendor's then-current professional Services rates, which shall be made available to Epicor upon request. Before the commencement of any such on-site audit, Epicor and Vendor shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Epicor shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by Vendor. Epicor shall promptly notify Vendor and provide information about any actual or suspected non-compliance discovered during an audit.

24 **Data Deletion**. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Vendor to Epicor only upon Epicor's request.

25 **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 obligations 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 Standard Contractual Clauses, the Standard Contractual Clauses will prevail.

[SIGNATURES APPEAR ON NEXT PAGE]

Vendor	**Epicor Software (UK) Limited**
By entering into the Agreement with Epicor and/or by submitting a completed Vendor DPA Assessment through OneTrust, Vendor is deemed to have signed this DPA.	**By entering into the Agreement with Vendor and/or approving a completed Vendor DPA Assessment through OneTrust, Epicor is deemed to have signed this DPA.**
By:	By:
Print Name:	Print Name:
Title:	Title:
Date:	Date:

SCHEDULE 1 TO DPA

ANNEX I

A. LIST OF PARTIES

MODULE THREE: Transfer processor to processor

Data Exporter (s)

Name of Data Exporter	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 ("Epicor")	Epicor's address set out on Vendor Order or SoW	Epicor Software (UK) Limited 6 Arlington Square West, Bracknell, Berkshire RG12 1PU United Kingdom	Processing of Epicor Data and/or Personal Data submitted by a Customer (where Epicor is acting as a Data Processor) or by an Epicor Employee/ Contractor (where Epicor is acting a Data Controller) to enable Epicor (and/or its affiliates) to perform Epicor's contractual obligations under a Cloud based services agreement; perform software maintenance and support services to Customer and/or, when Epicor is acting as Data Controller, to provide services as an employer. To the extent Vendor/Contractor is Processing Personal Data for Epicor where Epicor is a Processor for its customers, Epicor's customers can enforce against the data importer or any subsequent sub-processor clauses 3 (Third Party Beneficiaries), 8 (Data Protection Safeguards) and 10 (Data Subject Rights), clause 12 (Liability) and clauses 14 (Local Laws and Practices Affecting Compliance with the Clauses) to 18 (Choice of Forum and Jurisdicton) of the Standard Contract Clauses as third-party beneficiary.	Data Procesor and/or, where applicable, Data Controller	Epicor, by signing the vendor Order and/or the relevant Epicor Master services Agreement is deemed to have signed this Annex 1	Same date as Epicor's signature to Vendor's order and/or Epicor's signature to Epicor's Master Services Agreement

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Data Importer(s):

Name of Data Importer (Vendor)	Address	Contact person's name, position and contact details:	Activities relevant to the data transferred under these Clauses:	Role	Signature	Date of Signature
Vendor/Contractor named on Vendor/Contractor order (or SoW) or in Epicor's Master Services Agreement/ Independent Contractor Agreement	Vendor's/Contractor's address on Vendor order (or SoW) and/or executed Epicor Master Services Agreement/ Independent Contractor Agreement	Same details as set forth on Vendor's/Contractor's order (or SoW)	Processing of Epicor Data and/or Personal Data submitted by a Customer (where Epicor is acting as a Data Processor) or by an Epicor Employee/ Contractor (where Epicor is acting a Data Controller) to enable Epicor (and/or its affiliates) to perform Epicor's contractual obligations under a Cloud based services agreement; perform software maintenance and support services to Customer and/or, when Epicor is acting as Data Controller, to provide services as an employer. To the extent Vendor/ Contractor is Processing Personal Data for Epicor where Epicor is a Processor for its customers, Epicor's customers can enforce against the data importer or any subsequent sub-processor clauses 3 (Third Party Beneficiaries), 8 (Data Protection Safeguards) and 10 (Data Subject Rights), clause 12 (Liability) and clauses 14 (Local Laws and Practices Affecting Compliance with the Clauses) to 18 (Choice of Forum and Jurisdicton) of the Standard Contract Clauses as third-party beneficiary.	Processor and/or, where applicable, Joint Data Controller	**Vendor/Contractor, by signing the vendor Order (o SoW) and/or the relevant Epicor Master Services Agreement (or any amendment thereto) is deemed to have signed this Annex 1** **Further, by submitting a completed Vendor DPA Assessment through OneTrust, Vendor is deemed to have signed this Annex 1.**	Same date as Vendor's/Conractor's signature to Vendor's order and/or vendor's/ Contractor's signature to Epicor's Master Services Agreement/ Indepdendent Conrractor Agreement.

2. Other Data Exporters:

Not applicable. See above

B. DESCRIPTION OF TRANSFER

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred

Epicor (as the data exporter) may share/transfer Epicor Data (including Personal Data) with Vendor/Contractor, the extent of which is determined and controlled by Epicor (as the Data Processor and/or Data Controller) 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 Epicor and its affiliates.**
- **Employees, former employees or contact persons of Epicor's and its affiliates customers, business partners, and vendors.**
- **Agents, advisors, contractors, or any user authorized by Epicor .**

Categories of personal data transferred

Epicor (as data exporter) may submit Epicor Data (including Personal Data) to Vendor, the extent of which is determined and controlled by Epicor (as the Data Processor and/or Data Controller) 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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None

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

- **Continuous Transfer during the Term of the Services Agreement with Customer;**
- **Continuous Transfer during Employee's/ contractor's employment with Epicor.**

Nature of the processing

Contractual

Purpose(s) of the data transfer and further processing

To comply with

(1) Epicor's contractual obligations as a Data Processor under a Services Agreement between Epicor and Customer; and/or

(2) to comply with Epicor's obligations as a Data Controller.

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

- **Where Epicor acts as a Data Processor: Duration of the Services Agreement with the relevant Customer, plus 6 years (statute of limitations period)**
- **Where Epicor acts as a Data Controller: duration of employee/ contractors' engagement with Epicor, plus 6 years**

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

Subject Matter of the processing	**Processing of the categories of Personal Data listed above**
Nature of processing	**To fulfill contractual obligations**

Duration of the processing	**Duration of the Services Agreement plus 6 years (statute of limitations period)**

C. COMPETENT SUPERVISORY AUTHORITY

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

Epicor's Supervisory Authority: The Data Protection Office of the Slovak Republic (the **'Slovak Office'**) is:
***Úrad na ochranu osobných údajov Slovenskej republiky* (Official Slovak Name)**
***Hraničná* 12**
820 07, *Bratislava* 27
Slovak Republic
The Slovak Office is the supervisory authority and is responsible for overseeing the Slovak Data Protection Act and the EU GDPR in Slovakia.

Article 27 EU Representative:

Name	Epicor Entity	Address
Marian Janci Director of Finance	**Epicor Software Slovakia, s.r.o.**	Žižkova 22B Bratislava 81102 Slovak Republic

ANNEX II

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

MODULE THREE: Transfer processor to processor

Vendor shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Epicor Data, including Personal Data equal to the technical safeguards ensured by Epicor and listed at https://www.epicor.com/en-uk/company/compliance/ On request, a detailed description of such safeguards shall be provided to Epicor. Vendor regularly monitors compliance with these safeguards. Vendor will not materially decrease the overall security of their Services during the term of the Agreement.

ANNEX III

LIST OF SUB-PROCESSORS

MODULE THREE: Transfer processor to processor

Clause 9 (a) OPTION 1: If Specific Prior Authorization is elected pursuant to Clause 9 (a) Option 1, the Controller has authorized the following specific sub-processors:

Name	Purpose	Country

Clause 9 (a) OPTION 2: The controller 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

SCHEDULE 2

Standard Contractual Clauses (processors)

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

International Data Transfer Agreement ("IDTA")

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.

(a) **Part 1: Tables**

(i) **Table 1: Parties and signatures**

Start date	**Effective Date of the Agreement**	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	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**	Full legal name: **Name of vendor stated on a Statement of Work, Order or the Agreement** Trading name (if different): N/A Main address (if a company registered address): **Same as on the Statement of Work and/or the Agreement** Official registration number (if any) (company number or similar identifier): N/A
Key Contact	Full Name (optional): Epicor Legal Department Job Title: Legal Department Contact details including email: LegalPersonnel-EMEA@epicor.com	Full Name (optional): **Name of vendor stated on a Statement of Work, Order or the Agreement** Job Title: **Vendor** Contact details including email: **see the Statement of Work and/or Order**

Importer Data Subject Contact	Contact details including email: LegalPersonnel-EMEA@epicor.com	Job Title: Legal Department Contact details including email: **same as the Statement of Work**
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 AGREEMENT (TO WHICH THIS IDTA IS INCORPORATED) AND/OR STATEMENT OF WORK OR ORDER, AND BY APPROVING THE VENDOR'S COMPLETED VENDOR DPA ASSESSMENT THROUGH ONETRUST, EPICOR IS DEEMED TO HAVE SIGNED THIS INTERNATIONAL DATA TRANSFER AGREEMENT**	Signed for and on behalf of the **Importer** set out above **BY SIGNING THE AGREEMENT (TO WHICH THIS IDTA IS INCORPORATED) AND/OR STATEMENT OF WORK OR ORDER, AND BY SUBMITTING A COMPLETED VENDOR DPA ASSESSMENT THROUGH ONETRUST, VENDOR IS DEEMED TO HAVE SIGNED THIS INTERNATIONAL DATA TRANSFER AGREEMENT**

(ii) **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: **Date of completion and submission of OneTrust DPA assessment**

	Parties to the agreement: **(1) Epicor Software (UK) Limited and (2) Vendor named on the relevant Agreement and/or Statement of Work and/or Order** 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: **Service Agreement with Vendor** Date of agreement: **Date of Epicor's signature** Parties to the agreement: **(1) Epicor Software (UK) Limited and (2) Vendor named on the relevant Services Agreement and/or Statement of Work and/or Order** 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: **Epicor's Master Customer Agreement Master Terms and Conditions and relevant Product Supplement, available for download from https://www.epicor.com/en-us/company/customer-agreements/ (as modified by an MCA Supplement, if applicable)** Date of agreement: **Same as the date of an Epicor Order** Parties to the agreement: **(1) Epicor Software (UK) Limited and (2) Customer named on an Epicor Order** 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 two year(s)** ☐ ~~each time there is a change to the Transferred Data, Purposes, Importer Information, TRA or risk assessment~~

(iii) 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:~~ 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 Data Processing Addendum (Linked Agreement)** 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.~~

(iv) **Table 4: Security Requirements**

Security of Transmission	***Vendor shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Epicor Data, including Personal Data equal to the technical safeguards ensured by Epicor and listed at https://www.epicor.com/en-uk/company/compliance/ On request, a detailed description of such safeguards shall be provided to Epicor. Vendor regularly monitors compliance with these safeguards. Vendor will not materially decrease the overall security of their Services during the term of the Agreement.***
Security of Storage	***Vendor shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Epicor Data, including Personal Data equal to the technical safeguards ensured by Epicor and listed at https://www.epicor.com/en-uk/company/compliance/ On request, a detailed description of such safeguards shall be provided to Epicor. Vendor regularly monitors compliance with these safeguards. Vendor will not materially decrease the overall security of their Services during the term of the Agreement.***
Security of Processing	***Vendor shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Epicor Data, including Personal Data equal to the technical safeguards ensured by Epicor and listed at https://www.epicor.com/en-uk/company/compliance/ On request, a detailed description of such safeguards shall be provided to Epicor. Vendor regularly monitors compliance with these safeguards. Vendor will not materially decrease the overall security of their Services during the term of the Agreement.***

Organisational security measures	***Vendor shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Epicor Data, including Personal Data equal to the technical safeguards ensured by Epicor and listed at https://www.epicor.com/en-uk/company/compliance/ On request, a detailed description of such safeguards shall be provided to Epicor. Vendor regularly monitors compliance with these safeguards. Vendor will not materially decrease the overall security of their Services during the term of the Agreement.***
Technical security minimum requirements	***Vendor shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Epicor Data, including Personal Data equal to the technical safeguards ensured by Epicor and listed at https://www.epicor.com/en-uk/company/compliance/ On request, a detailed description of such safeguards shall be provided to Epicor. Vendor regularly monitors compliance with these safeguards. Vendor will not materially decrease the overall security of their Services during the term of the Agreement.***
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.~~

(b) **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**

(c) **Part 3: Commercial Clauses**

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

(d) **Part 4: Mandatory Clauses**

(i) **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.

(ii) 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.

(iii) 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.

(iv) 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).

(v) What rights do individuals have?

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.

(vi) 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 bounceback 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.

(vii) 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.

(viii) 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).

(ix) 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; 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.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
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.
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.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the IDTA)
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.
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.

Word or Phrase	Legal definition (this is how this word or phrase must be interpreted in the 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.

(e) **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.

ADDENDUM

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

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

VERSION B1.0, in force 21 March 2022

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

(a) Part 1: Tables

(i) Table 1: Parties

Start date	**Effective Date of the Agreement**	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	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**	Full legal name: **Name of vendor stated on a Statement of Work, Order or the Agreement** Trading name (if different): N/A Main address (if a company registered address): **Same as on the Statement of Work and/or the Agreement** Official registration number (if any) (company number or similar identifier): N/A
Key Contact	Full Name (optional): Epicor Legal Department Job Title: Legal Department Contact details including email: LegalPersonnel-EMEA@epicor.com	Full Name (optional): **Name of vendor stated on a Statement of Work, Order or the Agreement** Job Title: **Vendor** Contact details including email: **see the Statement of Work and/or Order**
Signature (if required for the purposes of Section 2)	Signed for and on behalf of the **Exporter** set out above **BY SIGNING THE AGREEMENT (TO WHICH THIS ADDENDUM IS INCORPORATED) AND/OR STATEMENT OF WORK OR ORDER, AND BY APPROVING THE VENDOR'S COMPLETED VENDOR DPA**	Signed for and on behalf of the **Importer** set out above **BY SIGNING THE AGREEMENT (TO WHICH THIS ADDENDUM IS INCORPORATED) AND/OR STATEMENT OF WORK OR ORDER, AND BY SUBMITTING A COMPLETED VENDOR DPA ASSESSMENT**

	ASSESSMENT THROUGH ONETRUST, EPICOR IS DEEMED TO HAVE SIGNED THIS ADDENDUM	**THROUGH ONETRUST, VENDOR IS DEEMED TO HAVE SIGNED THIS ADDENDUM**

(ii) **Table 2: Selected SCCs, Modules and Selected Clauses**

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

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	Not Applicable	Not Applicable	Not Applicable			
2	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	
3	**Processor to Processor**	**Clause 7 (Docking Clause) is adopted and incorporated**	**Option is deleted**	**Option 2: General Authorisation**	**Five (5) Business Days**	
4	Not Applicable	Not Applicable	Not Applicable			Not Applicable

(iii) **Table 3: Appendix Information**

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

Annex 1A: List of Parties: **A copy of the Annex I to III to the EU Standard Contractual Clauses (in force on and from 27 June 2021) is set forth at Annex 1 to the Data Processing Addendum (Linked Agreement)**

Annex 1B: Description of Transfer: **A copy of the Annex I to III to the EU Standard Contractual Clauses (in force on and from 27 June 2021) is set forth at Annex 1 to the Data Processing Addendum (Linked Agreement)**

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: **A copy of the Annex I to III to the EU Standard Contractual Clauses (in force on and from 27 June 2021) is set forth at Annex 1 to the Data Processing Addendum (Linked Agreement)**

Annex III: List of Sub processors (Modules 2 and 3 only): **A copy of the Annex I to III to the EU Standard Contractual Clauses (in force on and from 27 June 2021) is set forth at Annex 1 to the Data Processing Addendum (Linked Agreement)**

(iv) **Table 4: Ending this Addendum when the Approved Addendum Changes**

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

(b) Part 2: Mandatory Clauses

(i) **Entering into this Addendum**

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

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

(ii) **Interpretation of this Addendum**

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.

Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

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

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

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

(iii) Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

(iv) Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

    c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

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

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

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

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

        "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

        "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

    g. References to Regulation (EU) 2018/1725 are removed;

    h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

    i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

    j. Clause 13(a) and Part C of Annex I are not used;

    k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

    l. In Clause 16(e), subsection (i) is replaced with:

        "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

    m. Clause 17 is replaced with:

        "These Clauses are governed by the laws of England and Wales.";

    n. Clause 18 is replaced with:

        "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

    o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

        (v) Amendments to this Addendum

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

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

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

(c) **Alternative Part 2 Mandatory Clauses:**

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