Vendor Data Processing Addendum (EU, UK and California version)

MODULE ONE: CONTROLLER TO CONTROLLER

FOR INDEPENDENT CONTROLLERS

(Updated 1 November 2023)

*Compliant with the General Data Protection Regulation (**EU GDPR**) and European Commission Decision (EU) 2021/914 - Standard Contractual Clauses (**Controller to Controller**) and the UK International Data Transfer Agreement in force on and from 21 March 2022*

This Data Processing Addendum ("**DPA**") forms part of (and is incorporated into) the agreements between Epicor and Vendor ("**Independent Controller)**" for the provision of content subscription 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 regulated by the following data protection laws:

Country/ Region	**Applicable Data Protection Law**
European Union and member states	EU GDPR (as defined below)
European Economic Area and member states	EU GDPR (as defined below)
Switzerland	EU GDPR (as defined below)
United Kingdom	UK GDPR (as defined below)
United States of America:	CCPA, as amended by CPRA (both as defined below) CDPA (Virginia); CPA (Colorado); CTDPA (Connecticut); and UCPA (Utah), when effective

Independent Controller 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 Independent Controller processes Personal Data for which such Authorized Affiliates qualify as a Controller under the EU GDPR and/or the UK GDPR and/or as a Business under US Data Protection Laws.

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**: the EU Standard Contractual Clauses: Module One: Controller to Controller (as updated and issued by the EU Commission on 4th June 2021), and Appendices I-II thereto; and

   (c) **Schedule 2**: the UK Addendum to the EU Standard Contractual Clauses.

APPLICATION OF THIS DPA

For the avoidance of doubt, both Epicor and the Independent Controller are independent controllers who determine their own purposes and means of the processing of Personal Data. Neither of the Parties processes the Personal Data on behalf of the other Party and this DPA does not constitute a data processing agreement within the meaning of Article 28 of the EU GDPR and the UK GDPR. If, for the purposes of the Agreement, it becomes necessary that the Independent Controller process Personal Data on behalf of Epicor, the Parties shall enter into a separate data processing agreement within the meaning of Article 28 of the EU GDPR and the UK GDPR.

DPA DEFINITIONS

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

"**Applicable Data Protection Laws and Regulations**" means the US Data Protection Laws, EU GDPR, the UK GDPR, the UK Data Protection Legislation (as defined below), CCPA (as amended by CPRA) and all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, including Switzerland as well as the laws of the UAE, India and China applicable to the Processing of Personal Data under this DPA and the Agreement.

"**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 Independent Controller but has not signed its own Agreement with Independent Controller.

"Business" has the same meaning as set forth at §1798.140 (Definitions) of the California Civil Code (effective 1 January 2023) that being:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the **State of California**, and that satisfies one or more of the following thresholds:

(A) As of January 1, of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, sells, or shares the personal information of 100,000 or more consumers or, households.

(C) Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information.

(2) Any entity that controls or is controlled by a business, as defined in paragraph (1), and that shares common branding with the business and with whom the business shares consumers' personal information. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark that the average consumer would understand that two or more entities are commonly owned.

(3) A joint venture or partnership composed of businesses in which each business has at least a 40 percent interest. For purposes of this title, the joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business, except that personal information in the possession of each business and disclosed to the joint venture or partnership shall not be shared with the other business.

(4) A person that does business in California, that is not covered by paragraph (1), (2), or (3) and that voluntarily certifies to the California Privacy Protection Agency that it is in compliance with, and agrees to be bound by, this title.

"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data and includes Epicor and the Independent Controller. For the purposes of the Agreement and this DPA, the term "**Controller**" includes "**business"** as that term is defined by CCPA, as amended by CPRA.

"**Customer Data"** has the same meaning as under the Agreement.

"CCPA" means the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199) and CPRA, the CCPA Regulations (Cal. Code Regs. tit. 11, §§ 999.300 to 999.337), and any related regulations or guidance provided by the California Attorney General. Terms defined in the CCPA, including personal information and business purposes, carry the same meaning in this DPA.

"CPRA" means the California Privacy Rights Act of 2020.

"Data Discloser" means Epicor.

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates and includes "consumers" as defined under US Data Protection Laws.

"**Epicor**" means the Epicor entity, which is a party to this DPA, as specified in the Agreement between the parties, or, if no Epicor Authorized Affiliate is specified in the Agreement, Epicor Software Corporation, a company incorporated in Delaware and its primary address as 804 Las Cimas Parkway, Austin Texas 78746, and/or any Affiliates of Epicor, a list of which is available at *https://www.epicor.com/en-uk/company/compliance/affiliates/*, as applicable.

"**EU GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (as applicable and in force across the European Union) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) as amended, replaced or superseded.

"**Personal Data**" has the same meaning as under the EU GDPR and the UK GDPR and includes the term '**Personal Information**' as defined under US Data Protection Laws and without affecting the foregoing, means any information relating to (i) an identified or identifiable natural person (including a consumer or household) 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**).

"**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.

"EU Standard Contractual Clauses" means the agreement executed by and between Epicor and Independent Controller set forth at **Schedule 1** and incorporated herein by reference, pursuant to the European Commission's decision **(EU) 2021/914 of 4th June 2021** on Standard Contractual Clauses, Module 1.

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

"**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the EU GDPR and/or the Information Commissioner's Office (**ICO**) pursuant to the DPA 2018 (defined below) and/or the UK GDPR.

"UK Addendum" means the United Kingdom's Data Transfer Addendum to the EU Standard Contractual Clauses available at *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/* a completed version of which is set forth at **Schedule 2** to this DPA.

UK Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time in the United Kingdom including without limitation the UK GDPR; the Data

Protection Act 2018 (and regulations made thereunder) (**DPA 2018**); the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the Commissioner or other relevant regulatory authority and which are applicable to a party.

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

"US Data Protection Laws" means all laws and regulations applicable in the United States of America (Federal and State), including (i) the California Consumer Privacy Act (the "**CCPA**"), as amended by the California Privacy Rights Act ("**CPRA**"), as well as any regulations and guidance that may be issued thereunder; and, where applicable, (ii) the Virginia Consumer Data Protection Act ("**CDPA**"); (iii) the Colorado Privacy Act ("**CPA**"); (iv) the Connecticut Data Privacy Act ("**CTDPA**"); and the Utah Consumer Privacy Act (**"UCPA**") when effective; and, in each case, as may be amended or superseded from time to time.

DPA TERMS

This DPA is incorporated into and forms part of the Agreement.

1. **Provision of the Services and Parties' Roles**. Independent Controller provides the Services to Epicor under the Agreement. In connection with the Services, the parties anticipate that Epicor, when acting as a Controller (and as a **Data Discloser**), will need to disclose Personal Data to Independent Controller (and as a Data Receiver) and which Independent Controller is, due to the nature of the Services provided by Independent Controller, categorized under Applicable Data Protection Laws and Regulations as an independent Controller.

   Personal Data. Each party considers that (i) a data sharing framework, as set forth in this DPA, is necessary so that each Party can comply with its respective legal obligations as a Controller under Applicable Data Protection Laws and Regulations; and (ii) the data sharing framework set forth in this DPA (and Schedules hereto) is fair and will not unduly infringe the Data Subject's fundamental rights, freedoms and interests.

2. **Epicor Responsibilities**. Epicor shall, in its use of the Services, Process Personal Data in accordance with the requirements of the Applicable Data Protection Laws and Regulations. As between the parties, Epicor shall have sole responsibility for the accuracy, quality, and legality of the Personal Data disclosed by Epicor as a Data Discloser to Independent Controller (as a Data Receiver) and the means by which Epicor acquired the Personal Data.

3. **Independent Controller Responsibilities**. Independent Controller shall keep the Personal Data (that it obtains as an independent Data Controller) confidential and shall Process the Personal Data

(that it obtains as an independent Data Controller) in accordance with the requirements of the Applicable Data Protection Laws and Regulations and its Privacy Policy that is available here: https://www.idc.com/about/privacy.

4. **Processing in California/ United States.** Independent Controller shall not “sell” (as such term is defined by the CCPA) Personal Data.

5. **Data Subject Requests**. Each Party is responsible for maintaining a record of Data Subject Rights Requests, the decisions made and any information that was exchanged. Each Party is solely responsible to responding to Data Subjects Rights Requests it receives.

6. **Independent Controller Personnel**. Independent Controller 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. Independent Controller shall take commercially reasonable steps to ensure the reliability of any Independent Controller personnel engaged in the Processing of Personal Data.

7. **Transfers of Personal Data to Third Countries**. If either Party transfers Personal Data to any Third Countries, it shall ensure that the requirements of Article 45 or 46 of the EU GDPR and UK GDPR are met.

8. **Security Measures**. Both Parties 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, the Personal Data), confidentiality, and integrity of the Personal Data. Both Parties shall regularly monitor compliance with these measures.

9. **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 Independent Controller 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.

10. **Communications**. The Epicor entity that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Independent Controller 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).

11. **Exercise of Rights**. The Epicor entity that is the contracting party to the Agreement shall be solely entitled to exercise the rights and seek remedies under this DPA.

12. **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 Professional

Independent Controller, 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.

13. **EU GDPR**. Both Parties will Process Personal Data in accordance with the EU GDPR requirements directly applicable to them.

14. **UK GDPR**. Both Parties will Process Personal Data in accordance with the UK Data Protection Legislation and UK GDPR requirements directly applicable to them.

15. **EU Standard Contractual Clauses and UK Addendum thereto**. The EU Standard Contractual Clauses (as supplemented by the UK Addendum) apply to (i) the legal entity that has executed the EU Standard Contractual Clauses and the UK Addendum as a data exporter and its Authorized Affiliates and, (ii) all Affiliates of Epicor established within the European Economic Area, Switzerland and the United Kingdom, which have signed Order Forms for the Services. For the purpose of the EU Standard Contractual Clauses the aforementioned entities shall be deemed "data exporters." The parties will be deemed to have executed the EU Standard Contractual Clauses set forth at **Schedule 1** (as supplemented by the UK Addendum set forth at Schedule 2) the terms and conditions of which are incorporated herein and form a part of this DPA.

16. **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 EU Standard Contractual Clauses (as supplemented by the UK Addendum), the EU Standard Contractual Clauses (as supplemented by the UK Addendum) will prevail.

SIGNATURES

Independent Controller	Epicor
By entering into the Agreement with Epicor and/or by submitting a completed vendor DPA Assessment through OneTrust, Independent Controller is deemed to have signed this DPA.	**The Epicor entity named in the Epicor Master Services Agreement and/or Order / Statement of Work** **By entering into the Agreement with Independent Controller and/or approving a completed vendor DPA Assessment through OneTrust, Epicor is deemed to have signed this DPA.**
Signature	Signature
Printed Name	Printed Name
Title	Title

Date	Date

SCHEDULE 1

As updated by the European Commission on 4 June 2021 and in force from 27 June 2021

for

Module One: Controller to Controller

EU STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the

Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.5 (e) and Clause 8.9(b);

(iii) N/A

(iv) Clause 12(a) and (d);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject’s prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation ([2]) of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter ‘personal data breach’). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union ([3]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

N/A

Clause 10

Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. ([4]) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

(a) **Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its**

Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([5]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the **Republic of Ireland** .

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the **Republic of Ireland.**

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

MODULE ONE: Controller to Controller

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 entity and/or entities/ affiliates listed on a Independent Controller order or SoW	Epicor's address set out on Independent Controller Order or SoW or similar agreement or document entered into by and between Epicor (as the Data Exporter/ Controller) and Independent Controller, (as the Data Importer).	Epicor Software Corporation c/o 6 Arlington Square West, Bracknell, Berkshire RG12 1PU United Kingdom	Processing of Personal Data submitted by an Epicor Employee/ Contractor/ Customer submitting Personal Data to Epicor's websites (where Epicor is acting a Data Controller) to enable Epicor (and/or its affiliates) to perform Epicor's contractual obligations when Epicor is acting as Data Controller, to provide services as an employer and/or as a Data Controller. To the extent Independent Controller is Processing Personal Data where Epicor is a Controller, Epicor's employees and contractors (and where applicable Customers who submit their Personal Data to Epcor's websites) can enforce against the data importer 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 Controller	Epicor, by signing the Data Processing Addendum.	Date of signature of the Data Processing Addendum.

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 (Professional Independent Controller)	Address	Contact person's name, position and contact details:	Activities relevant to the data transferred under these Clauses:	Role	Signature	Date of Signature
Independent Controller named on Independent Controller order (or SoW) or in Epicor's Master Services Agreement or similar agreement or document entered into by and between Epicor (as the Data Exporter/ Controller) and Independent Controller, (as the Data Receiver/ Data Importer)	Independent Controller's address on Independent Controller order (or SoW) and/or executed Epicor Master Services Agreement	Same details as set forth on Independent Controller's order (or SoW) or similar agreement or document entered into by and between Epicor (as the Data Exporter/ Controller) and Independent Controller, (as the Data Importer)	Processing of Personal Data submitted by an Epicor Employee/ Contractor/ Customer submitting Personal Data to Epicor's websites (where Epicor is acting a Data Controller) to enable Epicor (and/or its affiliates) to perform Epicor's contractual obligations when Epicor is acting as Data Controller, to provide services as an employer and/or as a Data Controller. To the extent Independent Controller is Processing Personal Data where Epicor is a Controller, Epicor's employees and contractors (and where applicable Customers who submit their Personal Data to Epcor's websites) can enforce against the data importer 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 Controller	Independent Controller by signing the Data Processing Addendum.	Date of signature of the Data Processing Addendum.

2. Other Data Exporters:

Not applicable. See above

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer Controller to Controller

Categories of data subjects whose personal data is transferred

Epicor (as the data exporter and Controller) may transfer Personal Data to (and share with) Independent Controller for the purpose of the Services, and which may include, but is not limited to the following categories of data subjects who are natural persons:

- **Employees, former employees or contact persons of Epicor's and its affiliates customers, business partners, and Professional Independent Controllers.**
- **Agents, advisors, contractors, or any user authorized by Epicor.**

Categories of personal data transferred

Epicor (as data exporter and Data Controller) may transfer Personal Data with Independent Controller for the purpose of the Services, and which may include, but is not limited to the following categories of Personal Data:

- **First and last name**
- **Business contact information (name, email, phone)**
- **Job title**
- **Employer name**
- **User login credentials (user IDs, passwords)**

Sensitive data transferred (if applicable) *and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

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 Independent Controller;**
- **Continuous Transfer during Employee's/ contractor's employment with Epicor.**

Nature of the processing

Contractual

Subscription-based, cloud-hosted service.

Purpose(s) of the data transfer and further processing

To enable Independent Controller to provide the Service to Epicor.

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

- **Duration of the Services Agreement and in accordance with Independent Controller's Privacy Policy available on Independent Controller's website and/or online portal**

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

Subject Matter of the processing	**To enable the Independent Controller to provide the Service and in accordance with the Independent Controller's Privacy Policy**
Nature of processing	**Processing to enable Epicor's employees/ contractors to access and use the online subscription services.**
Duration of the processing	**To enable the Independent Controller to provide the Services and in accordance with the Independent Controller's Privacy Policy**

C. COMPETENT SUPERVISORY AUTHORITY MODULE ONE:

Transfer Controller to Controller

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 ONE: Transfer Controller to Controller

Independent Controller 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/ Independent Controller regularly monitors compliance with these safeguards. Independent Controller will not materially decrease the overall security of their Services during the term of the Agreement.

SCHEDULE 2

UK Addendum to the EU Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Start date	**Effective Date of the DPA**	
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, United Kingdom** Official registration number (if any) (company number or similar identifier): **02338274**	Full legal name: **Independent Controller named as a party to the Agreement and the DPA (to which this UK Addendum is a Schedule)** Trading name (if different): N/A Main address (if a company registered address): **same address as in the Agreement** Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): **Legal Department** Job Title: **Legal Department** Contact details including email: ***LegalPersonnel-EMEA@epicor.com***	Full Name (optional): **same contact as in independent controller order form, Epicor purchase order of similar document.** Job: **N/A** Contact details including email: **same contact as in independent controller order form, Epicor purchase order of similar document.**
Signature (if required for the purposes of Section 2)	**By signing the Agreement and the DPA (to which this UK Addendum is attached) Data Exporter is deemed to have signed this UK Addendum**	**By signing the Agreement and the DPA (to which this UK Addendum is attached), Data Importer is deemed to have signed this UK Addendum**

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	**(Module 1: Controller to Controller)**	**Option applied**	**Option not applied**	N/A	N/A	N/A
2						
3						
4						

Table 3: Appendix Information

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

Annex 1A: List of Parties: **As set forth at Part A (List of Parties) to Annex I of the EU SCCs**

Annex 1B: Description of Transfer: **As set forth at Part B (Description of Transfer) to Annex I of the EU SCCs**

Annex II: Technical and organizational measures including technical and organizational measures to ensure the security of the data: **As set forth at Annex II of the EU SCCs**

Annex III: List of Sub processors (Modules 2 and 3 only): **N/A**

Table 4: Ending this Addendum when the Approved Addendum Changes

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

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.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (*OJ L 295, 21.11.2018, p. 39*), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[4] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.