Vendor Data Processing Addendum (EU, UK and California version)
MODULE TWO: CONTROLLER TO PROCESSOR

(Updated 21 September 2022)

*Compliant with the General Data Protection Regulation (**EU GDPR**) and European Commission Decision (EU) 2021/914 - Standard Contractual Clauses (Controller to Processor) 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**,"(which term, for the avoidance of doubt, includes independent contractors and/or independent software vendors engaged by Epicor) for the provision of services to Epicor (identified collectively either as the **"Service**" or otherwise in the applicable agreement, and hereinafter defined as the "**Service**"), 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: State of California	CCPA, as amended by CPRA (both as defined below)

By completing (and submitting) Epicor's Vendor 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 under the EU GDPR and/or the UK GDPR and as a Service Provider under CCPA. In providing the Service 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**: the EU Standard Contractual Clauses (as updated and issued by the EU Commission on 4th June 2021), and Appendices I-III thereto;

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

   (d) **Schedule 3**: the Contract Clauses for Service Providers under CCPA, as amended by CPRA

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 (i.e., either Epicor or a subsidiary of Epicor) 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 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 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 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 Service 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. 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.

"CCPA Data" has the same meaning at set forth in this DPA

"CPRA" means the California Privacy Rights Act of 2020

"**Data Subject**" means the identified or identifiable person to whom Personal Data relates and includes "consumers" as defined under CCPA and/or CPRA.

"**Epicor**" means the Epicor entity, which is a party to this DPA, as specified in the Agreement between the parties, being Epicor, 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.

"**Epicor Data**" means all electronic data (including any Personal Data and/or Customer Data) submitted or transferred by Epicor (or on behalf of Epicor), or an Authorized Affiliate, to the Service. Epicor Data excludes

any Personal Data that is provided directly to the Vendor by a Data Subject by the Data Subject visiting Vendor's publicly facing website and/or voluntarily signing up to receive the Vendor's marketing materials (if any). Such Personal Data shall be governed by the Vendor's publicly available and posted privacy policy.

"**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 CCPA, as amended by CPRA 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**), where for each (i) or (ii) such data is Epicor Data.

"**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. For the purposes of the Agreement and this DPA, the term Processor includes "**Service Provider**" (as defined below) and as that term if defined pursuant to CCPA, as amended by CPRA.

"Service Provider" has the same meaning as under CCPA and, for the purposes of this DPA, the Vendor that is a named as a party to the Agreement (and this DPA) and that received personal information from Epicor and/or its Affiliates or contractors for a business purpose and under a written contract (including this DPA) which prohibits the Service Provider from retaining, using or disclosing the personal information for any purpose other than for performing the services specified in the contract (being the Agreement and/or this DPA)

"Service Provider Clauses" means the clauses set forth at **Schedule 3** to this DPA and incorporated herein by reference.

"EU Standard Contractual Clauses" means the agreement executed by and between Epicor and Vendor set forth at Schedule [ ] and incorporated herein by reference, pursuant to the European Commission's decision **(EU) 2021/914 of 4th June 2021** on Standard Contractual Clauses for the transfer of personal data to processors established in third countries 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 Epicor Data.

"**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 copy 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.

DPA TERMS

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

1. **Provision of the Service**. Vendor provides the Service to Epicor under the Agreement. In connection with the Service, 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 Service, Process Personal Data in accordance with the requirements of Applicable Data Protection Laws and Regulations. For the avoidance of doubt, Epicor's instructions to Vendor for the Processing of Personal Data shall comply with Applicable 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 (including Epicor Data) confidential and shall only Process Personal Data (including Epicor Data) on behalf of and in accordance with Epicor's documented instructions for the following purposes:

(i) Processing in accordance with the Agreement, this DPA and applicable Order Form(s);

(ii) Processing initiated by Epicor in its use of the Service;

(iii) (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 EU GDPR or other EU law or EU member state data protection provisions; and

(iv) as expressly permitted by UK Data Protection Legislation and/or Applicable Data Protection Laws and Regulations

5. Processing in California/ United States. To the extent "personal information" of "consumers" (as such terms are defined by **CCPA** contained within Epicor Data and processed by Vendor is subject to the CCPA ("**CCPA Data**"), the parties agree that Epicor and its Affiliates is a business and that it appoints Vendor as its Service Provider to process CCPA Data as permitted under the Agreement and this DPA. Vendor agrees that:

(a) it will process CCPA Data in accordance with the Agreement (and this DPA);

(b) it will not use or disclose CCPA Data for any other purpose other than for providing the Services or in connection with its rights and obligations under the Agreement (and this DPA), and

(c) it shall not "sell" (as such term is defined by the CCPA) CCPA Data.

If Vendor receives a request from a consumer to exercise a right such consumer has under the CCPA in relation to information relating to such consumer contained in and identified as Epicor Data and/or CCPA Data, Vendor will provide a copy of the request to Epicor and/or the applicable Epicor Affiliate. For the avoidance of doubt, Epicor will be responsible for handling and communicating with consumers in relation to such requests.

6. **Scope of Processing**. The subject-matter of Processing of Personal Data (including Epicor Data) by Vendor is the performance of the specific business purposes and Service pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data (including Epicor Data) and categories of Data Subjects Processed under this DPA are further specified in Annex 1 to the EU Standard Contractual Clauses and Appendix A to the Service Provider Clauses at Schedule 3.

7. **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 Applicable Data Protection Laws and Regulations and its agreements with its customers. In addition, to the extent Epicor, in its use of the Service, 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 Applicable Data Protection Laws and Regulations and Epicor's agreements with its customers.

8. **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 Service in accordance with the Agreement.

9. **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.

10. **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 Service. 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 Service. 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

Service or recommend a commercially reasonable change to Epicor's configuration or use of the Service 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 Service 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 Service. The parties agree that the copies of the Sub-processor agreements that must be provided by Vendor to Epicor pursuant to Clause 9 (c) 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.

11. **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.

12. **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 Service during Epicor's and/or Authorized Affiliates' subscription term.

13. **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.

14. **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.

15. **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.

16. **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 Service 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.

17. **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).

18. **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.

19. **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.

20. **EU GDPR**. Vendor will Process Personal Data in accordance with the EU GDPR requirements directly applicable to Vendor's provision of the Service.

21. **UK GDPR**. Vendor will Process Personal Data in accordance with the UK Data Protection Legislation and UK GDPR requirements directly applicable to Vendor's provision of the Service.

22. **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 EU GDPR and UK GDPR to carry out a data protection impact assessment related to Epicor's use of the Service 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 EU GDPR and/or 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.

23. **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 Service. For the purpose of the EU Standard Contractual Clauses the aforementioned entities shall be deemed "data exporters." **By agreeing to the terms of this DPA through OneTrust,** 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.

24. **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 sub-section (a) of sub-clause 8.1 (**Instructions)** of the EU 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 Service; 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.

25. **Audits**. The parties agree that the audits described in sub-sections (c) and (d) to sub-clause 8.9 (Documentation and Compliance) of the EU Standard Contractual Clauses 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. The provision in this section shall by no means derogate from or materially alter the provisions on audits as specified in the EU Standard Contractual Clauses.

26. **Data Deletion**. The parties agree that the certification of deletion of Personal Data that is described in sub-clause 8.5 (Duration of processing and erasure or return of data) of the EU Standard Contractual Clauses shall be provided by Vendor to Epicor only upon Epicor's request.

27. **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 (and its schedules) 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

Vendor	Epicor
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.	**The Epicor entity named in the Epicor Master Services Agreement and/or Order / Statement of Work** **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.**
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 Two: Controller to Processor

EU STANDARD CONTRACTUAL CLAUSES

Controller to Processor

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 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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

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

(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

[Not Used]

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 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 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, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the 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. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 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 data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties 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 subjects. 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. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) 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 breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 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 and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer 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 Regulation of (EU) 2016/679 with respect to the processing in question;

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) **OPTION 2: GENERAL WRITTEN AUTHORISATION** The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least **thirty (30) days** in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

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) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) 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 and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) 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.

(f) The Parties agree that if one Party is held liable under paragraph (e), 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.

(g) The data importer may not invoke the conduct of a 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 ([4]);

(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

OPTION 1: 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 TWO: Controller 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 entity and/or entities/ affiliates listed on a vendor order or SoW	Epicor's address set out on Vendor Order or SoW or similar agreement or document entered into by and between Epicor (as the Data Exporter/ Controller) and Vendor, (as the Data Importer).	Epicor Software Corporation c/o 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/ 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 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 and/or as a Data Controller. To the extent Vendor/Contractor is Processing Personal Data for Epicor where Epicor is a Controller for and/or on behalf of its employees and contractors, Epicor's employees and contractors (and where applicable Customers who submit their Personal Data to Epcor's websites) 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 Controller	Epicor, by signing the vendor Order and/or the relevant Epicor Master services Agreement is deemed to have signed this Annex 1 **Further, by approving a completed Vendor DPA Assessment through OneTrust, Epicor 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 or similar agreement or document entered into by and between Epicor (as the Data Exporter/ Controller) and Vendor, (as the Data Importer)	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) or similar agreement or document entered into by and between Epicor (as the Data Exporter/ Controller) and Vendor, (as the Data Importer)	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/ 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 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 and/or as a Data Controller. To the extent Vendor/Contractor is Processing Personal Data for Epicor where Epicor is a Controller for and/or on behalf of its employees/ contractors, (and some web-based Customers), Epicor's employees and contractors (and where applicable Customers who submit their Personal Data to Epcor's websites) 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/Contractr, 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 Conractor Agreement.

2. Other Data Exporters:

Not applicable. See above

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer Controller to Processor

Categories of data subjects whose personal data is transferred

Epicor (as the data exporter and Controller) may share/transfer Epicor Data (including Personal Data) with Vendor/Contractor, the extent of which is determined and controlled by Epicor (as the 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:

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

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

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 Vendor;**
- **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 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 Employment/ Consultancy Agreement plus 6 years (statute of limitations period)**

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer Controller 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 TWO: Transfer Controller 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 TWO: Transfer Controller to Processor

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

Name	Purpose	Country

Clause 9 (a) OPTION 2: Epicor, as a Controller, has authorized the use of the following sub-processors:

Name	Purpose	Country
Vendor has submitted a list of sub processors via OneTrust and/or made that list available to Epicor (as the Data Controller) via Vendor's public facing website or via an alternative means including submission by e-mail.		

SCHEDULE 2

UK Addendum to the EU Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Start date	**Effective Date of the Agreement to which the DPA is appended**	
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: **Vendor 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 Vendor Order, Epicor Purchase Order or similar document** Job: **N/A** Contact details including email: **same as in Vendor Order**
Signature (if required for the purposes of Section 2)	**By signing the Agreement and the DPA (to which this UK Addendum is incorporated by reference) Data Exporter is deemed to have signed this UK Addendum**	**By signing the Agreement and the DPA (to which this UK Addendum is incorporated by reference) and/or completing the DPA Assessment through OneTrust, 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 Authorization or General Authorization)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2	**(Module 2: Controller to Processor)**	**Deleted**	**Option not applied**	**Option 2 (General Authorization) applied**	**30 days in advance**	
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): **List to be provided to Epicor by Vendor**

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 **Error! Reference source not found.**: ☒ Importer ☒ Exporter

	☐ neither Party

1. make changes to this Addendum, but any changes must be made in accordance with its terms.

(a) **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 **Error! Reference source not found.** of those Mandatory Clauses.

SCHEDULE 3

CCPA CONTRACT CLAUSES FOR SERVICE PROVIDERS

1. **Definitions**. The following definitions and rules of interpretation apply in this Agreement:

(a) **CCPA** means the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199), 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 Agreement.

(b) **Contracted Business Purposes** means the services described in [the Agreement/Appendix A/[DESCRIPTION LOCATION]] [or any other purpose specifically identified in Appendix A] for which the service provider receives or accesses personal information.

(c) **"Customer"** for the purposes of this Schedule, Customer means Epicor and/or its Affiliates

2. **Service Provider's CCPA Obligations**

(a) Service Provider will only collect, use, retain, or disclose personal information for the Contracted Business Purposes for which Customer provides or permits personal information access [in accordance with the Customer's written instructions.

(b) Service Provider will not collect, use, retain, disclose, sell, or otherwise make personal information available for Service Provider's own commercial purposes or in a way that does not comply with the CCPA. If a law requires the Service Provider to disclose personal information for a purpose unrelated to the Contracted Business Purpose, the Service Provider must first inform the Customer of the legal requirement and give the Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

(c) Service Provider will limit personal information collection, use, retention, and disclosure to activities reasonably necessary and proportionate to achieve the Contracted Business Purposes or another compatible operational purpose.

(d) Service Provider must promptly comply with any Customer request or instruction [from Authorized Persons] requiring the Service Provider to provide, amend, transfer, or delete the personal information, or to stop, mitigate, or remedy any unauthorized processing.

(e) If the Contracted Business Purposes require the collection of personal information from individuals on the Customer's behalf, Service Provider will always provide a CCPA-compliant notice at collection that the Customer specifically pre-approves in writing. Service Provider will not modify or alter the notice in any way without the Customer's prior written consent.

(f) Service Provider will not attempt to or actually re-identify any previously aggregated, deidentified, or anonymized data and will contractually prohibit downstream data recipients from attempting to or actually re-identifying such data.

3. **Assistance with Customer's CCPA Obligations**

(a) Service Provider will reasonably cooperate and assist Customer with meeting the Customer's CCPA compliance obligations and responding to CCPA-related inquiries, including responding to verifiable consumer requests, taking into account the nature of the Service Provider's processing and the information available to the Service Provider.

(b) Service Provider must notify Customer immediately if it receives any complaint, notice, or communication that directly or indirectly relates either party's compliance with the CCPA. Specifically, the Service Provider must notify the Customer within five (5) working days if it receives a verifiable consumer request under the CCPA.

4. **Subcontracting**

(a) Service Provider may use subcontractor to provide the Contracted Business Services. Any subcontractor used must qualify as a service provider under the CCPA and Service Provider cannot make any disclosures to the subcontractor that the CCPA would treat as a sale.

(b) For each subcontractor used, Service Provider will give Customer an up-to-date list disclosing:

(i) The subcontractor's name, address, and contact information.

(ii) The type of services provided by the subcontractor.

(iii) The personal information categories disclosed to the subcontractor in the preceding 12 months.

(c) Service Provider remains fully liable to the Customer for the subcontractor's performance of its agreement obligations.

(d) Upon the Customer's written request, Service Provider will audit a subcontractor's compliance with its personal information obligations and provide the Customer with the audit results.

5. **CCPA Warranties and Certification**

(a) Both parties will comply with all applicable requirements of the CCPA when collecting, using, retaining, or disclosing personal information.

(b) Service Provider certifies that it understands this Agreement's and the CCPA's restrictions and prohibitions on selling personal information and retaining, using, or disclosing personal information outside of the parties' direct business relationship, and it will comply with them.

(c) Service Provider warrants that it has no reason to believe any CCPA requirements or restrictions prevent it from providing any of the Contracted Business Purposes or otherwise performing under this Agreement. Service Provider must promptly notify the Customer of any changes to the CCPA's requirements that may adversely affect its performance under the Agreement.

APPENDIX A

Personal Information Processing Purposes and Details

Contracted Business Purposes: as specified in the Agreement and/or any Statement of Work thereto

Service Provider Category: to be specified by Service Provider to Epicor by e-mail or via OneTrust Assessment

Personal Information Categories: This Agreement involves the following types of Personal Information, as defined and classified in CCPA Cal. Civ. Code § 1798.140(o).

Category	**Examples**	**Processed under this Agreement**
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers.	YES
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. Some personal information included in this category may overlap with other categories.	
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military status, genetic information (including familial genetic information).	NO
D. Commercial information.	Records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.	YES
E. Biometric information.	Genetic, physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information, such as fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data.	NO
F. Internet or other similar network activity.	Browsing history, search history, information on a consumer's interaction with a website, application, or advertisement.	YES
G. Geolocation data.	Physical location or movements.	NO
H. Sensory data.	Audio, electronic, visual, thermal, olfactory, or similar information.	NO
I. Professional or employment-related information.	Current or past job history or performance evaluations.	NO
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.	NO

1232g, 34 C.F.R. Part 99)).		
K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	NO

Types of Consumers: **Employees and/or contractors of Epicor and its Affiliates**

Approved Subcontractors: **as per the list submitted by Service Provider to Epicor and/or made available on Service Provider's public website**

[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] 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.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[4] 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.