



Epicor Software Corporation

Data Processing Addendum (UK Version)

Based on the UK General Data Protection Regulation (GDPR) and European Commission Decision 2010/87/EU - Standard Contractual Clauses (Processors), as modified by the UK Information Commissioner.

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

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

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

INSTRUCTIONS ON HOW TO EXECUTE THIS DPA WITH EPICOR

1. This DPA consists of distinct parts: this body and its set of definitions and provisions, the Standard Contractual Clauses, and Appendices 1-2.
2. Customer must confirm the information in Appendices 1-2.
3. Customer must send the completed and signed Order Form, Statement of Work, or Amendment to Epicor in compliance with the instructions provided by Epicor. Upon receipt by Epicor of the validly-completed Order Form, Statement of Work, or Amendment, this DPA shall come into effect and legally bind the parties.

APPLICATION OF THIS DPA

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

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

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

DPA DEFINITIONS

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

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

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

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

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

“Epicor” means the Epicor entity which is a party to this DPA, as specified in the section “Application of this DPA” above, being Epicor, a company incorporated in Delaware and its primary address as 804 Las Cimas Parkway, Austin Texas 78746, or an Affiliate of Epicor, as applicable.

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

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

“Order Form” means Epicor’s standard order form documentation, including without limitation, written Orders and Statements of Work, for acquiring Services.

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

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

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

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

“Standard Contractual Clauses” means the agreement executed by and between Customer and Epicor and incorporated herein, pursuant to the European Commission’s decision (C(2010)593) of 5 February 2010 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, as amended by the UK Information Commissioner following the UK’s departure from the European Union.

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

“Supervisory Authority” means the UK Information Commissioner.

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

DPA TERMS

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

1. **Provision of the Services.** Epicor provides the Services to Customer under the Agreement. In connection with the Services, the parties anticipate that Epicor may Process Customer’s data which may include Personal Data relating to Data Subjects.
2. **The Parties’ Roles.** Customer, as Controller, appoints Epicor as a Processor to process the Personal Data on Customer's behalf. In some circumstances Customer may be a Processor, in which case Customer appoints Epicor as Customer's sub-processor, which shall not change the obligations of either Customer or Epicor under this DPA, as Epicor will remain a Processor with respect to Customer in such event. Subject to clause 9 below, Epicor or members of the Epicor Group may be or otherwise may engage Sub-processors pursuant to the requirements of this DPA.
3. **Customer Responsibilities.** Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer’s instructions to Epicor for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.
4. **Processing Purposes.** Epicor shall keep Personal Data confidential and shall only Process Personal Data on behalf of and in accordance with Customer’s documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented, reasonable instructions provided by Customer (for example, via email) where such instructions are consistent with the terms of the Agreement. Epicor shall not be required to comply with or observe Customer’s instructions if such instructions would violate the UK GDPR but shall notify Customer promptly if Epicor considers that the Customer’s instructions violate such laws.
5. **Scope of Processing.** The subject-matter of Processing of Personal Data by Epicor is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Appendix 1 to this DPA.
6. **Data Subject Requests.** To the extent legally permitted and required, Epicor shall promptly notify Customer if Epicor receives a request from a Data Subject to exercise the Data Subject’s right of access, right to rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, objection to the Processing, or its right not to be subject to an automated individual decision making (“**Data Subject Request**”) with respect to Personal Data in a manner other than the Data Subject using Epicor-provided self-help tools. Factoring into account the nature of the Processing, Epicor shall assist Customer by appropriate organizational and technical measures, insofar as this is possible, for the fulfilment of Customer’s obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Epicor shall, upon Customer’s request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent that Epicor is legally authorized to do so, and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any reasonable costs arising from Epicor’s provision of such assistance.

7. **Epicor Personnel.** Epicor shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training regarding their responsibilities, and have executed written confidentiality agreements. Epicor shall take commercially reasonable steps to ensure the reliability of any Epicor personnel engaged in the Processing of Personal Data. Epicor shall ensure that Epicor's access to Personal Data is limited to those personnel assisting in the provision of the Services in accordance with the Agreement.
8. **Data Protection Officer.** Epicor shall have appointed, or shall appoint, a data protection officer if and whereby such appointment is required by Data Protection Laws and Regulations. Any such appointed person may be reached through legalpersonnel-emea@epicor.com
9. **Epicor's Sub-processors.** Customer has authorized the use of Sub-processors to assist Epicor with respect to the performance of Epicor's obligations under the Agreement. Upon written request of Customer, Epicor will provide to Customer a list of its then current Sub-processors. Customer acknowledges and agrees that (a) Epicor's Affiliates may be retained as Sub-processors; and (b) Epicor and Epicor's Affiliates respectively may engage third party Sub-processors in connection with the provision of the Services. On Epicor's Compliance webpage (accessible via www.Epicor.com/company/compliance under the "Sub-Processors" link), Customer may find a mechanism to subscribe to notifications of new Sub-processors for each of the applicable Services, to which Customer shall subscribe, and if Customer subscribes, Epicor shall provide notification of a new Sub-processor(s) before authorizing any new Subprocessor(s) to process Personal Data in connection with the provision of the applicable Services. In order to exercise its right to object to Epicor's use of a new Sub-processor, Customer shall notify Epicor promptly in writing within ten (10) business days after receipt of Epicor's notice in accordance with the instructions accessible via www.Epicor.com/company/compliance If Customer does not object within such ten (10) business days, such new Sub-processor shall be deemed accepted. In the event Customer objects to a new Sub-processor, and that objection is not unreasonable, Epicor will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing Customer's Personal Data by the objected-to new Sub-processor without unreasonably burdening Customer. If Epicor is unable to make available such change within a reasonable time period, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those aspects of the Services which cannot be provided by Epicor without the use of the objected-to new Sub-processor by providing written notice to Epicor. Epicor will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services. The parties agree that the copies of the Sub-processor agreements that must be provided by Epicor to Customer pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by Epicor beforehand; and, that such copies will be provided by Epicor, in a manner to be determined in its discretion, only upon request by Customer.
10. **Liability for Sub-processors.** Epicor shall be liable for the acts and omissions of its Sub-processors to the same extent Epicor would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.
11. **Security Measures.** Epicor shall maintain appropriate organizational and technical measures for protection of the security (including protection against unauthorized or unlawful Processing, and against unlawful or accidental destruction, alteration or damage or loss, unauthorized disclosure of, or access to, Personal Data), confidentiality, and integrity of Personal Data, as set forth in Epicor's applicable Trust & Compliance Documentation available at <https://www.epicor.com/en-uk/company/compliance/> Epicor regularly monitors compliance with these measures. Epicor will not materially decrease the overall security of the Services during Customer's and/or Authorized Affiliates' subscription term.
12. **Third-Party Certifications and Audit Results.** Epicor has attained the third-party certifications and audit results set forth in the Trust & Compliance Documentation. Upon Customer's written request

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

- 13. Notifications Regarding Personal Data.** Epicor has in place reasonable and appropriate security incident management policies and procedures, as specified in the Trust & Compliance Documentation and shall notify Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by Epicor or its Sub-processors of which Epicor becomes aware (hereinafter, a "**Personal Data Incident**"), as required to assist Customer in ensuring compliance with its obligations to notify the Supervisory Authority in the event of Personal Data Incident. Epicor shall make reasonable efforts to identify the cause of such Personal Data Incident, and take those steps as Epicor deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident, to the extent that the remediation is within Epicor's reasonable control. The obligations set forth herein shall not apply to incidents that are caused by either Customer or Customer's Users.
- 14. Return of Personal Data.** Epicor shall return Personal Data to Customer and, to the extent allowed by applicable law, delete Personal Data in accordance with the procedures and time periods specified in the Trust & Compliance Documentation, unless the retention of the data is requested from Epicor according to mandatory statutory laws.
- 15. Authorized Affiliates.** The parties agree that, by executing the DPA, Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliate(s), thereby establishing a separate DPA between Epicor and each such Authorized Affiliate, subject to the provisions of the Agreement. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. An Authorized Affiliate is not and does not become a party to the Agreement, and is only a party to the DPA. All access to and use of the Services by Authorized Affiliate(s) must comply with the terms and conditions of the Agreement and any violation thereof by an Authorized Affiliate shall be deemed a violation by Customer.
- 16. Communications.** The Customer entity that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Epicor under this DPA, and shall be entitled to transmit and receive any communication in relation to this DPA on behalf of its Authorized Affiliate(s).
- 17. Exercise of Rights.** Where an Authorized Affiliate becomes a party to the DPA, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Epicor directly by itself, the parties agree that (i) solely the Customer entity that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer entity that is the contracting party to the Agreement shall exercise any such rights under this DPA in a combined manner for all of its Authorized Affiliates together, instead of doing so separately for each Authorized Affiliate.
- 18. Liability.** Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and Epicor, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. Epicor's and its Affiliates' total liability for all claims from Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall apply in the aggregate for all claims under both the Agreement and all DPAs established under this Agreement, including by Customer and all Authorized Affiliates, and shall not be understood to apply individually and severally to Customer and/or to any

Authorized Affiliate that is a contractual party to any such DPA. Each reference to the DPA herein means this DPA including the Standard Contract Clauses and the Appendices.

19. **GDPR.** Epicor will Process Personal Data in accordance with the UK GDPR requirements directly applicable to Epicor's provision of the Services.
20. **Data Protection Impact Assessment.** Upon Customer's request, Epicor shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the UK GDPR to carry out a data protection impact assessment related to Customer's use of the Services to the extent such assessment is required under applicable law, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Epicor. Epicor shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this Section 20 of this DPA, to the extent required under the UK GDPR. Notwithstanding the foregoing, the Parties acknowledge and agree that, in general, each believes that the nature, scope and scale of any data processing by Epicor does not and will not rise to the level of requiring a Data Protection Impact Assessment under applicable law.
21. **Standard Contractual Clauses.** The Standard Contractual Clauses apply to (i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and its Authorized Affiliates and, (ii) all Affiliates of Customer established within the United Kingdom, which have signed Order Forms for the Services as the data exporter.
22. **Customer's Processing Instructions.** This DPA and the Agreement are Customer's complete and final instructions at the time of signature of the Agreement to Epicor for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by Customer to process Personal Data: (a) Processing in accordance with the Agreement and applicable Order Form(s); (b) Processing initiated by Users in their use of the Services and (c) Processing to comply with other reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement.
23. **Audits.** The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out, in accordance with the following specifications:
 - a. Customer may audit Epicor's compliance with the terms of this Data Processing Addendum. Such audits shall be limited to no more than one per year unless the laws applicable to Customer provide for more frequent audits of Epicor's data center facility that Processes Personal Data. If Customer wishes to utilize a third party to conduct the audit, the third party must be mutually agreed to by Customer and Epicor and such third party must execute a written confidentiality agreement acceptable to Epicor, acting reasonably, before conducting the audit.
 - b. To request an audit, Customer must prepare and submit an Audit Request Form to Epicor at least fifteen (15) days in advance of the proposed audit date. The Audit Request Form must include details surrounding the proposed start date, scope and duration of the audit. Epicor will review the completed Audit Request Form and provide any questions, concerns or comments to Customer. Epicor and Customer shall work together to agree upon the final plan (including without limitation start date, scope, and duration) for the audit. If Customer's requested audit scope is substantially addressed in a SSAE 16/ISAE 3402 Type 2, ISO, NIST, PCI DSS, HIPAA or similar audit report previously performed on Epicor's behalf by a qualified third-party auditor within the twelve months prior to Customer's request and Epicor confirms that no known known material changes in the audited controls exist, then Customer shall accept those findings in place of requesting a further audit of the controls covered by the report.
 - c. Customer's audit shall be conducted during the regular business hours of the applicable facility, shall be subject to Epicor and facility policies, and may not unreasonably interfere with Epicor or the facility's business activities.

- d. Customer will provide Epicor with a copy of any audit reports generated in connection with any audit under this Section 23(d), unless doing so is expressly prohibited by law. Customer may only utilize the audit reports for the purposes of meeting its regulatory audit requirements and/or confirming Epicor's compliance with the Data Processing Addendum requirements. The audit reports and any related documentation shall be considered Confidential Information of the parties under the terms of the Agreement.
 - e. Any Customer audits that are not met with existing reports shall be conducted entirely at Customer's expense, including without limitation Epicor's internal reasonable costs of participating in such audits. Any request by Customer for Epicor to provide assistance with a Customer audit shall be considered a separate service if such audit assistance requires the use of resources different from or in addition to those required for the provision of the Services. Customer's written approval and agreement to pay any related fees or reasonable costs incurred by Epicor for such audit assistance shall be granted and provided to Epicor before Epicor is requested to perform such audit assistance.
 - f. The provision in this Section 23 shall by no means derogate from or materially alter the provisions on audits as specified in the Standard Contractual Clauses.
- 24. Data Deletion.** The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by Epicor to Customer only upon Customer's request.
- 25. Order of Precedence.** This DPA is incorporated into and forms part of the Agreement. For matters not addressed under this DPA, the terms of the Agreement apply. With respect to the rights and obligation of the parties vis-à-vis each other, in the event of a conflict between the terms of the Agreement and this DPA, the terms of this DPA will control. In the event of a conflict between the terms of the DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will prevail.



Standard Contractual Clauses (processors)

[\(UK version approved by the Information Commissioner's Office\)](#)

Name of the data exporting organization: _____

Address: _____

Tel.: _____; fax: _____; e-mail _____

(the data **exporter**)

and

Name of the data importing organization: **Epicor Software (UK) Limited**

Address: **6 Arlington Square West, Bracknell, Berkshire RG12 1PU**

E-mail: legalpersonnel-emea@epicor.com

(the data **importer**)

each a “**party**”; together “the **parties**”,

HAVE AGREED on the following Contractual Clauses (the **Clauses**) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) *‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘Commissioner’* shall have the same meaning as in UK GDPR;
- (b) *‘the data exporter’* means the controller who transfers the personal data;
- (c) *‘the data importer’* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system covered by UK adequacy regulations issued under Section 17A Data protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;
- (d) *‘the sub processor’* means any processor engaged by the data importer or by any other sub processor of the data importer who agrees to receive from the data importer or from any other sub processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

- (e) ***‘the applicable data protection law’*** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK;
- (f) ***‘technical and organisational security measures’*** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub processor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not covered by adequacy regulations issued under Section 17A Data protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018;
- (g) to forward any notification received from the data importer or any sub processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract
- (c) that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorized access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the Commissioner;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of sub processing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the sub processor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any sub processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub processor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub processor agrees that the data subject may issue a claim against the data sub processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the Commissioner;
 - (b) to refer the dispute to the UK courts.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub processor preventing the conduct of an audit of the data importer, or any sub processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established; namely [England and Wales] [Scotland]

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub processor which imposes the same obligations on the sub processor as are imposed on the data importer under the Clauses¹. Where the sub processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub processor shall be limited to its own processing operations under the Clauses.

¹ This requirement may be satisfied by the sub processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

3. The provisions relating to data protection aspects for sub processing of the contract referred to in paragraph 1 shall be governed by the laws of the country of the UK where the data exporter is established.
4. The data exporter shall keep a list of sub processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the Commissioner.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the sub processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1

This Appendix forms part of the DPA and the Clauses. **By executing an Order Form, Statement of Work, or Amendment that references the DPA, the parties will be deemed to have signed this Appendix 1.**

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data exporter is the legal entity that has executed the Data Processing Addendum based on the Standard Contractual Clauses as a Data Exporter established within the European Economic area and Switzerland that have purchased the Services as defined in the Data Processing Addendum on the basis of one or more Order Form(s) as defined in the Data Processing Addendum.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Data importer, Epicor, is an industry-specific business software provider which Processes Personal Data submitted by or on behalf of data exporter upon the instruction of the data exporter in accordance with the terms of the Agreement and the Data Processing Addendum.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit Personal Data to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects who are natural persons:

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

Categories of data

The Personal Data transferred concern the following categories of data (please specify):

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

- **First and last name**

- **Business contact information (company name, email, phone, physical business address)**
- **Personal contact information (name, email, phone, physical address)**
- **Government issued ID**
- **Job title**
- **Compensation**
- **Benefits**
- **Employee performance**
- **User login credentials (user IDs, passwords)**
- **System usage activity by users**

Special categories of data (if appropriate)

The Personal Data transferred concern the following special categories of data (please specify):

[NONE]

[DELETE IF NOT APPLICABLE] *Data exporter may submit special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation) to the Service, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include Personal Data.]*

Processing operations

The Personal Data transferred will be subject to the following basic processing activities (please specify):

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

APPENDIX 2

This Appendix forms part of the DPA and the Clauses. **By executing an Order Form, Statement of Work, or Amendment that references the DPA, the parties will be deemed to have signed this Appendix 2.**

1. Technical and Organizational Security Measures

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