



## **Epicor Software Canada**

### **Canada Data Processing Addendum (DPA)**

(Updated June 2024)

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 and Customer whereby Customer acquires, and Epicor provides Services (the “**Agreement**”) and this DPA reflects the parties’ agreement with regard to the Processing of Personal Information, as defined under PIPEDA.

By executing this DPA, Customer 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 Epicor processes Personal Information 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 to Customer pursuant to the Agreement, Epicor may Process Personal Information on behalf of Customer, and the parties agree to comply with the following provisions with respect to any Personal Information.

#### **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 and Annexes I-III thereto.
2. **To complete this DPA, Customer must complete the information in the signature box and sign on Page 7.**
3. Customer must send the completed and signed DPA to Epicor by email, indicating Customer’s Epicor Client ID/Serial Number (as set out on the applicable Epicor Order Form) in the body of the email to [legalpersonnel-emea@epicor.com](mailto:legalpersonnel-emea@epicor.com) Upon receipt of the validly completed DPA by Epicor at this email address, 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 Applicable Data Protection Laws and Regulations; 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 Information.

“**Applicable Data Protection Laws and Regulations**” means all laws and regulations, including PIPEDA and all Canadian federal and provincial laws, rules, regulations, industry standards, codes and practices with which Epicor is required or has voluntarily agreed to comply when performing the Services as each relate to the protection of Personal Information and as applicable to the Processing of Personal Information under the Agreement.

“**Data Subject**” means the identified or identifiable person to whom Personal Information 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 807 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 Information.

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

“**Personal Information**” means any information regulated by PIPEDA 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 Information or personally identifiable information under Applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is submitted by or on behalf of Customer or an Authorized Affiliate to Epicor in connection with providing the Services.

“**PIPEDA**” means the Personal Information protection and Electronic Documents Act (S.C. 2000, c.5)

“**Processing**” (including its root word, “**Process**”) means any operation or set of operations which is performed upon Personal Information, 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 Information on behalf of the Controller.

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

“**Sub-processor**” means any Processor engaged by Epicor or a member of the Epicor Group.

“**Supervisory Authority**” means the Office of the Privacy Commissioner (OPC) an independent public authority which is established under PIPEDA that has investigatory authority and jurisdiction over Epicor and Customer when Epicor Processors Personal Information belonging to a Customer.

“**Trust & Compliance Documentation**” means the documentation applicable to Epicor’s compliance with Applicable Data Protection Laws, as may be updated periodically, and accessible via Epicor’s website at [Compliance | Epicor UK](#) or as otherwise made reasonably available by Epicor.

“Users” has the same meaning as under the Agreement.

## DPA TERMS

Epicor and the signatory at the address below (“Customer”) hereby enter into this DPA effective as of the date of last signature. 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 Personal Information relating to Data Subjects.
2. **The Parties’ Roles.** Customer, as Controller, appoints Epicor as a Processor to process the Personal Information 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. 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 Information in accordance with the requirements of Applicable Data Protection Laws and Regulations. Customer’s instructions to Epicor for the Processing of Personal Information shall comply with Applicable Data Protection Laws and Regulations. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Information and the means by which Customer acquired Personal Information.
4. **Processing Purposes.** Epicor shall keep Personal Information confidential and shall only Process Personal Information 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 Applicable Data Protection Laws and Regulations.
5. **Scope of Processing.** The subject-matter of Processing of Personal Information 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 Information and categories of Data Subjects Processed under this DPA are further specified at **Annex I**.
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 individual rights under PIPEDA (“Data Subject Request”) with respect to Personal Information 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 Applicable 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 costs arising from Epicor’s provision of such assistance.
7. **Epicor Personnel.** Epicor shall ensure that its personnel engaged in the Processing of Personal Information are informed of the confidential nature of the Personal Information, 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 Information. Epicor shall ensure that Epicor’s access

to Personal Information 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 Applicable Data Protection Laws and Regulations. Any such appointed person may be reached through [legalpersonnel-EMEA@epicor.com](mailto:legalpersonnel-EMEA@epicor.com)
9. **Epicor's Sub-processors.** Customer has instructed or authorized the use of Sub-processors (as listed at <https://www.epicor.com/en-uk/company/compliance/sub-processors/>) to assist Epicor with respect to the performance of Epicor's obligations under the Agreement. Customer acknowledges and agrees that (a) Epicor's Affiliates (as listed at [Trust & Compliance Documentation](#)) 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 [Trust & Compliance Documentation](#)) 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 Sub-processor(s) to process Personal Information 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 [Trust & Compliance Documentation](#) 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 Information by the objected-to new Sub-processor without unreasonably burdening Customer. If Epicor is unable to make available such change within a reasonable time period, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those aspects of the Services which cannot be provided by Epicor without the use of the objected-to new Sub-processor by providing written notice to Epicor. Epicor will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services.
10. **Liability for Sub-processors.** Epicor shall be liable for the acts and omissions of its Sub-processors to the same extent Epicor would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.
11. **Security Measures.** Epicor shall maintain appropriate organizational and technical measures for protection of the security (including protection against unauthorized or unlawful Processing, and against unlawful or accidental destruction, alteration or damage or loss, unauthorized disclosure of, or access to, Personal Information), confidentiality, and integrity of Personal Information, as set forth in Epicor's applicable [Trust & Compliance Documentation](#). 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, an overview of which is 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 Information.** 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 Information transmitted, stored or otherwise Processed by Epicor or its Sub-processors of which Epicor becomes aware (hereinafter, a "Personal Information Incident"), as required to assist Customer in ensuring

compliance with its obligations (if any) to notify the Supervisory Authority in the event of Personal Information breach. Epicor shall make reasonable efforts to identify the cause of such Personal Information Incident and take those steps as Epicor deems necessary and reasonable in order to remediate the cause of such a Personal Information 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 Information.** Epicor shall return Personal Information to Customer and, to the extent allowed by applicable law, delete Personal Information 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 its Appendices.
19. **PIPEDA.** Epicor will Process Personal Information in accordance with PIPEDA and Applicable Data Protection Laws and Regulations (or other requirements) directly applicable to Epicor's provision of the Services to Customer and/or Epicor's Processing of Personal Information.
20. **Data Protection Impact Assessment.** Upon Customer's request, Epicor shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation (if any) under PIPEDA 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 PIPEDA. 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 arise to the level of requiring a Data Protection Impact Assessment under applicable law.

21. **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 Information. Any additional or alternate instructions must be agreed upon separately. For the purposes of this DPA, the following is deemed an instruction by Customer to process Personal Information: (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.
22. **Audits.** The parties agree that the audits shall be carried out in accordance with the following specifications:
  - (a) Customer may audit Epicor's compliance with the terms of this Data Processing Agreement. 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 Information. 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 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 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 Agreement 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 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 Subscription Services. Customer's written approval and agreement to pay any related fees or costs incurred by Epicor for such audit assistance shall be granted and provided to Epicor before Epicor is requested to perform such audit assistance.

**23. 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.

Agreed by Customer:

Signature: \_\_\_\_\_

By: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Agreed by Epicor:

Signature: \_\_\_\_\_

By: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

## ANNEX I

### A. LIST OF PARTIES

#### 1. Customer:

Name of Customer	Address	Contact person's name, position and contact details:	Activities relevant to the data transferred to Epicor:	Role	Signature	Date of Signature
Customer named in an Epicor Order. [Note Customer enters this DPA for and/or on behalf of its Affiliates.]	Customer Address on Epicor Order	Customer Contact details as set out in the Epicor Order	Processing, by Epicor (and/or its Affiliates), of Personal Information submitted by or on behalf of Customer (as the data exporter) to enable Epicor (and/or its Affiliates) to perform Epicor's contractual obligations under a Cloud based services agreement and/or perform software maintenance and support services.	Controller	By executing an Epicor Order, Customer is deemed to have signed this Annex 1	Same date as Customer's signature on Epicor Order Form

#### Epicor:

Name of Epicor and its Affiliates	Address	Contact person's name, position and contact details:	Activities relevant to the data transferred to Epicor:	Role	Signature	Date of Signature
Epicor Software Canada Ltd and/or its international affiliates as listed at <a href="https://www.epicor.com/en-uk/company/compliance/affiliates/">https://www.epicor.com/en-uk/company/compliance/affiliates/</a>	c/o 45 Vogell Rd, Ste 200, Richmond Hill, ON, Canada, L4B 3P6  <u>Attention: Legal Department</u>	<u>Attention: Legal Department</u> e-mail: <a href="mailto:legalpersonnel-emea@epicor.com">legalpersonnel-emea@epicor.com</a>	Processing, by Epicor (and/or its Affiliates), of Personal Information submitted by or on behalf of Customer (as the data exporter) to enable Epicor (and/or its Affiliates) to perform Epicor's contractual obligations under a Cloud based services agreement and/or perform software maintenance and support services.	Processor	By executing an Epicor Order, Epicor and/or the relevant Epicor Affiliates is deemed to have signed this Annex 1	Same date as Epicor's authorized signature on an Epicor Order Form

### B. DESCRIPTION OF TRANSFER

*Categories of data subjects whose Personal Information is transferred and Processed by Epicor*

**Customer may submit Personal Information to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to Personal Information relating to the following categories of Data Subjects who are natural persons:**

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



*Categories of Personal Information transferred to Epicor*

**Customer may submit Personal Information to the Services, the extent of which is determined and controlled by the Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal**

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

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

The Personal Information transferred concern the following special categories of data/ sensitive data (please specify): **NONE**

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

**Continuous transfer**

*Nature of the processing*

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

*Purpose(s) of the data transfer and further processing*

**Necessary to fulfill contractual obligations under the Agreement.**

*The period for which the Personal Information will be retained, or, if that is not possible, the criteria used to determine that period*

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

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

<b>Subject Matter of processing</b>	<b>Processing of the categories of Personal Information listed above</b>
<b>Nature of Processing</b>	<b>To fulfill contractual obligations under the Agreement</b>
<b>Duration of Processing</b>	<b>Duration of the Services and/or term of the Agreement, plus 6 years (statute of limitations period)</b>

## ANNEX II

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

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

**Epicor shall maintain appropriate organizational and technical measures for protection of the security (including protection against unauthorized or unlawful Processing, and against unlawful or accidental destruction, alteration or damage or loss, unauthorized disclosure of, or access to, Personal Information), confidentiality, and integrity of Personal Information, as set forth in Epicor's applicable Compliance Documentation located at [Compliance | Epicor UK](#). 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.**

ANNEX III

LIST OF SUB-PROCESSORS

The Controller has authorized the use of the following sub-processors: <https://www.epicor.com/en-uk/company/compliance/sub-processors/>

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