As updated by the European Commission on 4 June 2021 and in force from 27 June 2021
for
Module Two: Controller to Processor

Epicor Software Corporation

Data Processing Addendum

(Updated 31 August 2021)

*Based on the General Data Protection Regulation (EU GDPR) and European Commission Decision (EU)2021/914 - Standard Contractual Clauses (**Module Two: Transfer Controller to Processor**)*

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 Data.

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 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 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 Annexes I-III thereto.

2. **To complete this DPA, Customer must:**

   (a) Complete the information in the signature box and sign on Page 8;

   (b) Complete the information as the data exporter and sign Part A of Annex I.

   (c) Provide the details of Customer's Competent Supervisory Authority at Part C of Annex I

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 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.

As updated by the European Commission on 4 June 2021 and in force from 27 June 2021
for
Module Two: Controller to Processor

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 European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between 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 European Union, the European Economic Area and their member states (including Switzerland) applicable to the Processing of Personal Data under the Agreement.

"**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.

"EU GDPR" means the 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 and repealing Directive 95/46/EC (General Data Protection Regulation).

"**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 EU 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 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 included herein, pursuant to the European Commission's decision (EU) 2021/914 dated **4 June 2021** (in force on and from 27 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 any Processor engaged by Epicor or a member of the Epicor Group.

"**Supervisory Authority**" means an independent public authority which is established by an EU Member State pursuant to the EU GDPR.

"**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 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 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. 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 EU GDPR or other EU law or EU member state data protection provisions.

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 at Annex I to the Standard Contractual Clauses.

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, object 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 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 instructed or authorized the use of Sub-processors (as listed at Annex III to the Standard Contractual Clauses) 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 https://www.epicor.com/en-uk/company/compliance/) 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 Sub-processor(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 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 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. 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 breach. 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 its Appendices.

19. **EU GDPR**. Epicor will Process Personal Data in accordance with the EU 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 EU 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 EU 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 arise 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 European Economic Area and Switzerland which have signed Order Forms for the Services. For the purpose of the Standard Contractual Clauses the aforementioned entities shall be deemed "data exporters."

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 sub-section (a) of Sub-Clause 8.1 (Instructions) 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 sub-sections (c) and (d) to sub-clause 8.9 (Documentation and Compliance) 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 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 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 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.

(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 sub-clause 8.5 (Duration of processing and erasure or return of data) 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.

Agreed by Customer:	Agreed by Epicor:
Signature: _____	Signature: _____
By: _____	By: _____
Title: _____	Title: _____
Date: _____	Date: _____

As updated by the European Commission on 4 June 2021 and in force from 27 June 2021
for
Module Two: Controller to Processor

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third-party beneficiaries

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

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

(1) [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 October2018 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 legalact 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.

(ii) Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

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

(iv) Clause 12 – Clause 12(a), (d) and (f); Clause 13;

(v) Clause 15.1(c), (d) and (e); Clause 16(e);

(vi) Clause 18 –Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE TWO: Transfer controller to processor

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 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 organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, 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.

(2) [2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal marketto 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.

(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

MODULE TWO: Transfer controller to processor

(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 **five (5) business 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

MODULE TWO: Transfer controller to processor

(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 authorized 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 organizational 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 authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

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

MODULE TWO: Transfer controller to processor

(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, organization 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

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(a) **Where the data exporter is established in an EU Member State:** The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in **Annex I.C,** shall act as competent supervisory authority.

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.

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) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, 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

MODULE TWO: Transfer controller to processor

(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 organizational 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 organizational 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

(4) [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.

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

MODULE TWO: Transfer controller to processor

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 minimization

(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

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow 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

MODULE TWO: Transfer controller to processor

(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.

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

Module Two: Controller to Processor

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

1. Data exporter(s):

Name of Data Exporter (Customer)	Address	Contact person's name, position and contact details:	Activities relevant to the data transferred under these Clauses:	Role	Signature	Date of Signature
Customer named in an Epicor Order. [Note Customer enters these Standard Contractual Clauses 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 Data 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

2. Other Data Exporters:

Not applicable. Single Data Exporter. See above

Data importer(s):

Name of Data Importer (Epicor and its Affiliates)	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 Corporation and//or its international affiliates as listed at https://www.epicor.com/en-uk/company/compliance/affiliates/	**c/o** **804 Las Cimas Parkway, Austin, Texas 78746** **Attention: Legal Department** **6 Arlington Square West Bracknell Berkshire RG12 1PU** **Attention: Legal Department**	**Epicor Software (UK) Limited** **6 Arlington Square West Bracknell Berkshire RG12 1PU** **Attention: Legal Department** **e-mail: legalpersonnel-emea@epicor.com**	Processing, by Epicor (and/or its Affiliates), of Personal Data 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

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred

Data Exporter (named above) may submit Personal Data to the Services, 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 Services.**

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

Module Two: Controller to Processor

Categories of personal data transferred

Data Exporter may submit Personal Data to the Services, 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**
- **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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The Personal Data transferred concern the following special categories of 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 Data 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 data 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

Subject Matter of processing	**Processing of the categories of Personal Data listed above**
Nature of Processing	**To fulfill contractual obligations under the Agreement**
Duration of Processing	**Duration of the Services and/or term of the 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

The Supervisory Authority in a Member State that has been assessed by Customer (as data exporter) to be the most appropriate Supervisory Authority applicable to Customer's business in the European Union and/or applicable to the data subjects whose personal data is transferred under these Clauses.

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

Module Two: Controller to Processor

ANNEX II

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

MODULE TWO: Transfer controller to processor

Description of the technical and organisational 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 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.

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

Module Two: Controller to Processor

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

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