



DATA PROCESSING ADDENDUM **(GDPR, Privacy Shield, EU Standard Contractual Clauses)**

This Data Processing Addendum, including Attachment 1 “Standard Contractual Clauses” and Attachment 2 “Asure Information Security Policy” (“**DPA**”), is an addendum that forms part of the Limited Use Software License Agreement or the Subscription Agreement (the “**Agreement**”) between Asure (as defined below) (“**Asure**”) and the customer identified below (“**Customer**”). The obligations of each party also apply to its respective Affiliates who are, in Customer’s case, using the Service, and, in Asure’s case, providing the Service. Additionally, for clarity, Customer is responsible for coordinating all communication on behalf of itself and all Affiliates to Asure. In addition, all references to the Agreement are to the Agreement as amended by this DPA, as well as by any other amendment duly entered into by the parties.

This DPA reflects the parties’ agreement with regard to the Processing of Personal Data, in accordance with the requirements of Data Protection Laws (as defined below). All capitalized terms not defined in this Addendum will have the meaning set forth in the Agreement. In the course of providing the Services to Customer pursuant to the Agreement, Asure may Process Personal Data on behalf of Customer and the Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

EXECUTING THIS DPA:

1. This DPA consists of three parts: (a) the main body of the DPA; (b) Attachment 1 “Standard Contractual Clauses” (including Appendices 1 and 2); and (c) Attachment 2 “Asure Information Security Policy.”
2. This DPA has been signed by Asure. The Standard Contractual Clauses in Attachment 1 have also been signed by Asure.
3. To complete this DPA, Customer must:
 - a. Complete the information in the signature box and sign on Page 9.
 - b. Complete the information regarding the data exporter on Page 10.
 - c. Complete the information in the signature box and sign on Pages 15, 17 and 18.
4. Submit the completed and signed DPA to Asure via infosecteam@asuresoftware.com. Upon receipt of the validly completed DPA at this email address, this DPA will become legally binding.

HOW THIS DPA APPLIES

If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement. In that case, the Asure entity party to the Agreement is party to this DPA.

If the Customer entity signing the DPA is neither a party to an Order Form nor an Agreement directly with Asure, but is instead a Customer indirectly via an authorized reseller of Asure services, this DPA is not valid and is not legally binding. That entity should contact the authorized reseller to discuss whether any amendment to its agreement with that reseller may be required.



DATA PROCESSING TERMS

1. DEFINITIONS

“**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “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.

“**Asure**” means that Asure entity which is party to this DPA, as specified in “HOW THIS DPA Applies” including the following entities: Asure Software, Inc., a company incorporated in Delaware, Asure Software UK, Limited, a company registered in England and Wales, or Occupeye Limited, a company registered in England and Wales.

“**Asure Group**” means Asure and its Affiliates Processing Personal Data hereunder

“**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 Asure, but has not signed its own Order Form with Asure and is not a "Customer" as defined under the Agreement.

“**Customer Data**” means what is identified in the Agreement as “**Customer Data**” and not otherwise excluded.

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

“**Data Exporter**” has the meaning set forth in Clause 1 of Attachment 1 “Standard Contractual Clauses.”

“**Data Importer**” has the meaning set forth in Clause 1 of Attachment 1 “Standard Contractual Clauses.”

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

“**Data Protection Laws**” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, applicable to the Processing of Personal Data under the Agreement, including GDPR and any applicable Member State derogations enacted pursuant to GDPR.

“**Data Subject**” means the individual to whom Personal Data relates.

“**GDPR**” refers to 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).

“**Personal Data**” means any information relating to an identified or identifiable natural person that is submitted by or for Customer to Asure or collected and Processed by or for Customer using Asure’s SaaS Platform pursuant to the Agreement where such data is Customer Data.



“**Processing**” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

“**SaaS Platform**” means the online, web-based applications and platform provided by Asure under the Agreement.

“**Standard Contractual Clauses**” means the agreement executed by and between Customer and Asure Software, Inc. (attached hereto as Attachment 1), and approved by the European Commission’s decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

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

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

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller and Asure is a Processor, and that Asure, members of the Asure Group or Affiliates of Asure will engage Sub-processors pursuant to the requirements set out in Section 5 below.

2.2 Customer’s Processing of Personal Data. Customer shall, in its use of the SaaS Platform, Process Personal Data in accordance with the requirements of Data Protection Laws. Customer’s instructions for the Processing of Personal Data shall comply with Data Protection Laws and Asure shall promptly notify Customer if any instruction infringes an applicable Data Protection Law. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data, and the means by which Customer acquired Personal Data.

2.3 Asure’s Processing of Personal Data. Asure shall only Process Personal Data on behalf of and in accordance with Customer’s documented instructions, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by a law to which the Processor is subject and in such case, the Processor shall inform the Controller of the legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Asure shall treat Personal Data as Confidential Information. Customer instructs Asure to Process Personal Data for the following purposes:

- a. Processing in accordance with the Agreement and applicable Order Form(s);
- b. Processing initiated by users in their use of the SaaS Platform; and
- c. Processing to comply with other reasonable instructions by Customer that are consistent with the terms of the Agreement.

2.4 Details of the Processing. The subject-matter of Processing of Personal Data by Asure is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature



and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Attachment 1 “Standard Contractual Clauses” to this DPA.

3. RIGHTS OF DATA SUBJECTS

3.1 Data Subject Request. Asure agrees to promptly notify Customer, to the extent legally permitted, if it receives a request from a Data Subject to access, correct or delete that person’s Personal Data or if a Data Subject objects to the Processing of his or her Personal Data (“**Data Subject Request**”). Asure shall not respond to a Data Subject Request without Customer’s prior written consent, except to confirm that such request relates to Customer to which Customer hereby agrees. To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Asure shall, upon Customer’s request, provide commercially reasonable assistance to facilitate that Data Subject Request, to the extent Asure is legally permitted to do so, and provided that such Data Subject Request is exercised in accordance with Data Protection Laws. To the extent legally permitted, Customer is responsible for any costs arising from Asure’s provision of this assistance.

3.2 Data Subject Request. With effect after 25 May 2018, the following wording will replace Section 3.1 (Data Subject Request) above in its entirety: ***Data Subject Requests.** Asure agrees to promptly notify Customer, to the extent legally permitted, if Asure 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”). Taking into account the nature of the Processing, Asure will assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Asure shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to those Data Subject Request, to the extent Asure is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from Asure's providing that assistance.*

4. ASURE’S PERSONNEL

4.1 Confidentiality. Asure will ensure that personnel engaged in Processing Personal Data are informed of the confidential nature of Customer’s Personal Data, receive appropriate training on their responsibilities, have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Asure will ensure that these confidentiality obligations survive the termination of the personnel engagement.

4.2 Reliability. Asure will take commercially reasonable steps to ensure the reliability of any Asure personnel engaged in the Processing of Personal Data.

4.3 Limitation of Access. Asure will take reasonable steps to ensure that Asure’s access to Personal Data is limited to those personnel who require that access to perform legitimate business activities under this Agreement.

4.4 Data Protection Officer. Asure has appointed a data protection officer where that appointment is required by Data Protection Laws. The appointed person may be reached at infosecteam@asuresoftware.com.



5. SUB-PROCESSORS

5.1 Sub-processors Generally. Customer acknowledges and agrees that: (a) Asure's Affiliates may be retained as Sub-processors; and (b) Asure and Asure's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. Asure or an Asure Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this Agreement involving the protection of Customer Data, to the extent applicable to the nature of the Services provided by that Sub-processor.

5.2 List of Current Sub-processors and Notification of New Sub-processors. Asure agrees to make available to Customer the current list of Sub-processors for the Services. That Sub-processor lists includes the identities of those Sub-processors and their country of location ("**Sub-processor Lists**"). Customer may find (and this suffices as notice) on Asure's website at <http://www.asuresoftware.com/dpa/> a current list of Sub-processors for cloud services. Customer consents to the use of these Sub-processors. Asure will give at least 30 days prior written notice of any new Sub-Processor. Customer may object to Asure's use of a new Sub-Processor by notifying Asure promptly in writing within 10 days after receipt of such notice by submitting a notice to infosecteam@asuresoftware.com. In the event Customer objects to a new Sub-processor, Asure will use reasonable efforts to make available to Customer a reasonable change to configuration or use of the Services to avoid a Processing of Personal Data by the objected- to new Sub-processor. If Asure is unable to make available such a change within 30 days, Customer may terminate the applicable Order Form with respect only to those Services which cannot be provided by Asure without the use of the objected to Sub-Processor by providing written notice to Asure.

5.3 Liability. Asure remains liable for the acts and omissions of its Sub-processors to the same extent Asure would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set out in the Agreement.

5.4 Emergency Replacements. Asure may deploy Sub-processors as needed in its sole discretion to serve as Emergency Replacements to maintain and support the SaaS Platform. "**Emergency Replacement**" refers to a sudden replacement of a Sub-processor where a change is outside of Asure's reasonable control (e.g., an existing Sub-processor ceases business, abruptly discontinues services to Asure, or breaches its contractual duties owed to Asure). In that case, Asure will inform Customer of the replacement Sub-processor as soon as reasonably possible, and the process to formally appoint, and reject, that Sub-processor under Section 5.2 shall be triggered.

6. SECURITY

6.1 Controls for the Protection of Personal Data. Asure will maintain administrative, technical and organizational measures designed to protect the security, confidentiality, and integrity of Customer's Personal Data in accordance with Article 32 of the GDPR. Asure will also maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Personal Data), confidentiality and integrity of Customer Personal Data. Asure monitors compliance with these controls, and Asure will not materially diminish the overall security of the SaaS Platform services during the term of the Agreement.

6.2 Third-Party Certification and Audits. Asure has obtained third-party certifications and audits. Upon Customer's written request, and at reasonable intervals, Asure may provide a copy of Asure's



then most recent third-party certification or audit, as applicable, or any summaries that Asure readily makes available to its Customers (or Customer's independent, third-party auditor that is not a competitor of Asure).

7. CUSTOMER PERSONAL DATA BREACH MANAGEMENT AND NOTIFICATION

Asure maintains security incident management policies and procedures, and agrees to comply with all applicable laws and regulations requiring notifications to Customer after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data transmitted, stored, or otherwise Processed by Asure or its Sub-processors of which Asure becomes aware (a "**Customer Data Incident**"). Asure shall make reasonable efforts to identify the cause of that Customer Data Incident and take those steps as Asure deems necessary and reasonable to remediate the cause of this Customer Data Incident to the extent the remediation is within Asure's reasonable control. The obligations identified here do not apply to incidents that are caused by Customer or Customer's Users.

8. RETURN AND DELETION OF CUSTOMER DATA

Upon termination of the Agreement, Asure may delete Customer Personal Data to the extent allowed by applicable law, in accordance with Asure's record retention procedures and timeframes. Asure and Customer may enter into negotiations on the return of Customer Data in accordance with the procedures and timeframes specified in the Agreement.

9. AUTHORIZED AFFILIATES

9.1 Contractual Relationship. The parties acknowledge and agree that, by executing the Agreement, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between Asure and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 9 and Section 10. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, 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 and Content by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer.

9.2 Communication. The Customer that is the contracting party to the Agreement shall remain responsible for coordinating all communication with Asure under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

9.3 Rights of Authorized Affiliates. Where an Authorized Affiliate becomes a party to the DPA with Asure, 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, subject to the following:

9.3.1 Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against Asure directly by itself, the parties agree that (i) solely the Customer 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 that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate



individually but in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section 9.3.2, below).

- 9.3.2** The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on Asure and its Sub-processors by combining, to the extent reasonable possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

10. LIMITATION OF 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 Asure, 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.

For the avoidance of doubt, Asure's and its Affiliates' total liability for all claims from the 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, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any DPA.

Also for the avoidance of doubt, each reference to the DPA in this DPA means this DPA including its Attachments and Appendices.

11. European Specific Provisions.

- 11.1 GDPR.** With effect from 25 May 2018, Asure will Process Personal Data in accordance with the GDPR requirements directly applicable to Asure's provision of its Services. Asure will make available all information reasonably necessary to demonstrate compliance with its contractual obligations hereunder.
- 11.2 Cooperation with Customer.** With effect from 25 May 2018, upon Customer's request, Asure shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under the GDPR including assisting in carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Asure. Asure shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 11.2 of this DPA, to the extent required under the GDPR. Asure will assist the Controller in ensuring compliance with its obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing the information available to the processor and make available to the Customer all information necessary to demonstrate compliance with the obligations set forth in Article 28 of the GDPR. Asure will allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer.



- 11.3 Data Protection Impact Assessment.** With effect from 25 May 2018, upon Customer’s request, Asure shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer’s obligation under the GDPR to carry out a data protection impact assessment related to Customer’s use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to Asure. Asure shall provide reasonable assistance to Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 11.2 of this DPA, to the extent required under the GDPR.
- 11.4 Transfer mechanisms for data transfers.** Asure makes available the transfer mechanisms listed below which shall apply, in the order of precedence as set out in Section 11.4, to any transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws, to the extent those transfers are subject to such Data Protection Laws:
- 11.4.1** The Standard Contractual Clauses set forth in Attachment 1 to this DPA apply to the Services. To the extent the European Commission subsequently amends the Model Processor Contract at a date later than Effective Date of the Agreement, the amended terms supersede and replace any Model Processor Contract executed between Asure and Customer.
- 11.5 Order of precedence.** If the Services are covered by more than one transfer mechanism, the transfer of Personal Data will be subject to a single transfer mechanism in accordance with the following order of precedence: (1) Asure’s EU-U.S. and Swiss-U.S. Privacy Shield Framework self-certifications if applicable, and (2) the Standard Contractual Clauses.
- 12. PARTIES TO THIS DPA**
- 12.1 Representation & Warranty.** Customer hereby represents that it is duly authorized to enter into this DPA in the name and on behalf of its Affiliates.
- 12.2 How This DPA Applies.** The Section “HOW THIS DPA APPLIES” specifies which Asure entity is party to this DPA. Notwithstanding the signatures below of any other Asure entity, those other Asure entities are not a party to this DPA or the Standard Contractual Clauses.
- 12.3 Legal Effect.** This DPA will only become legally binding between Customer and Asure when the formalities steps set out in the Section “EXECUTING THIS DPA” above have been fully completed.
- 12.4 Other terms unchanged.** All terms of the Agreement not amended by this DPA remain unchanged.

[Signature page to follow]



**CUSTOMER,
acting in its own name and on its own behalf,
and in the name and on behalf of its Affiliates**

ASURE SOFTWARE UK LIMITED

Signature: _____

Customer Legal Name: _____

Print Name: _____

Title: _____

Date: _____

DocuSigned by:
Joe Karbowski
3A959A2AF47A45B...
Signature: _____
Print Name: Joe Karbowski
Title: CTO
Date: Sep-16-2019

ASURE SOFTWARE, INC.

DocuSigned by:
Joe Karbowski
3A959A2AF47A45B...
Signature: _____
Print Name: Joe Karbowski
Title: CTO
Date: Sep-16-2019

OCCUPEYE LIMITED

DocuSigned by:
Joe Karbowski
3A959A2AF47A45B...
Signature: _____
Print Name: Joe Karbowski
Title: CTO
Date: Sep-16-2019

[Remainder of page intentionally left blank]



ATTACHMENT 1

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: *[see page 9 of the DPA]*

Address:

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

..... (the data exporter)

And

Name of the data importing organisation: Asure Software, Inc.

Address: 3700 N. Capital of Texas Hwy, Suite 350, Austin, TX 78746 Tel.: 888-323-8835 fax:
5124372365 e-mail: infosecteam@asuresoftware.com

Other information needed to identify the organisation: Not applicable

(the data importer)

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

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



Clause 1

Definitions

For the purposes of the Clauses:

- (a) *'personal data'*, *'special categories of data'*, *'process/processing'*, *'controller'*, *'processor'*, *'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹;
- (b) *'the data exporter'* means the controller who transfers the personal data;
- (c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

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

¹ Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.



Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing SaaS Platform will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing SaaS Platform which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer²

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

² Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.



- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing SaaS Platform by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

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

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

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



case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

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

Clause 8

Cooperation with supervisory authorities

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

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

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

Clause 11

Subprocessing

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

³ This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.



the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

- 3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
- 4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing SaaS Platform

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

On behalf of the data exporter: [see page 9 of the DPA]

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature
(stamp of organisation)

On behalf of the data importer: Asure Software, Inc.

Name

Position:

Address: 3700 N. Capital of Texas Highway, Suite 350, Austin, TX 78746

Other information necessary in order for the contract to be binding (if any):

Signature
(stamp of organisation)



APPENDIX 1

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is the non-Asure entity party to the amendment to which these Standard Contractual Clauses are attached.

Data exporter is a commercial enterprise established within the EEA or Switzerland that has executed a services agreement with data importer, as provider of SaaS Platform, and/or all of such enterprise's affiliates established within the EEA or Switzerland that have purchased SaaS Platform on the basis of an order form pursuant to said services agreement.

Data importer

The data importer is **Asure Software, Inc.** which is a third party SaaS Platform services provider that provides a platform to data exporter for resource management and other data processing running Asure proprietary software.

Data Subjects

Data subjects include the data exporter's customer's representatives and end users including, employees, representatives, consultants, contractors or agents who are authorized to use the contracted for services on behalf of data exporter.

Categories of data

The electronic personal data (e.g., email) transferred by data exporter to data importer through use of the contracted services to the extent necessary to perform the contracted for services. Data exporter may submit Personal Data to the SaaS Platform, the extent of which is determined and controlled by the data exporter in its sole discretion.

Special categories of data (if appropriate)

The data exporter and data importer will mutually agree in writing if there are special categories of data.

Processing operations

The personal data transferred will be subject to the following basic processing activities in furtherance of providing the contracted for services:

a. Duration and Object of Data Processing. The duration of data processing shall be for the term designated under the agreement between data exporter and the Asure entity which is party to the Addendum to which these Standard Contractual Clauses are annexed ("Agreement"). The objective of the data processing is the performance of Asure SaaS Platform services.

b. Scope and Purpose of Data Processing. The scope and purpose of processing personal data is described in the Amendment. The data importer operates a SaaS Platform, and processing may take place in any jurisdiction where data importer or its sub-processors operate those facilities.

c. Customer Data Access. For the term designated under the Addendum, data importer will, at its election, and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide data exporter with the ability to correct, delete, or block Customer Data, or (2) make such corrections, deletions, or blockages on its behalf.

d. Data Exporter's Instructions. For Asure's SaaS Platform services, data importer will only act upon data exporter's instructions.

e. Customer Data Deletion or Return. Upon expiration or termination of data exporter's use of Asure's SaaS Platform services, it may extract Customer Data and data importer will delete Customer Data, each in accordance with the Agreement.



Subcontractors

The data importer may hire other companies to provide limited services on data importer’s behalf, such as providing customer support. Any such subcontractors will be permitted to obtain customer data only to deliver the services the data importer has retained them to provide, and they are prohibited from using customer data for any other purpose.

DATA EXPORTER [*see page 9 of the DPA*]

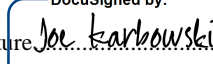
Name:.....

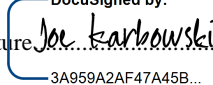
Authorised Signature.....

DATA IMPORTER **Asure Software, Inc.**

Joe Karbowski

Name: DocuSigned by:

Authorised Signature 


3A959A2AF47A45B...



APPENDIX 2

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the SaaS Platform, as described in the Asure Information Security Policy.

1. Personnel.

Data importer’s personnel will not process Customer Personal Data without authorization. Data importer personnel are obligated to maintain the confidentiality of any Customer Personal Data and this obligation continues even after their engagement ends.

2. Data Privacy Contact.

The data privacy officer of the data importer can be reached at the following address:

Asure Software
Attn: Privacy Officer
3700 N. Capital of Texas Hwy., Suite 350, Austin, TX 78746
infosecteam@asuresoftware.com

3. Technical and Organization Measures.

General Practices. The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Customer Data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as described in the Asure Information Security Policy.

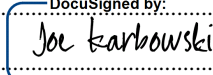
DATA EXPORTER [*see page 9 of the DPA*]

Name:.....

Authorised Signature.....

DATA IMPORTER **Asure Software, Inc.**

Name: **Joe Karbowski**
DocuSigned by:

Authorised Signature: 
3A959A2AF47A45B...



ATTACHMENT 2

Asure Information Security Policy

1. Introduction

- This Asure Information Security Policy is a part of the Data Processing Addendum and is incorporated by reference. It sets out additional commitments of Asure for Customer Data. Capitalized terms not otherwise defined here retain the same meaning set forth in the Limited Use License Agreement or the Data Processing Addendum, as applicable.

2. Data Confidentiality

- Asure (“**Data Processor**”) shall maintain administrative, physical and technical controls designed to protect the security, confidentiality and integrity of Client’s (“**Data Controller**”) Customer Data.

3. Access

- Data Processor will not knowingly authorize its personnel to have access to any records or data of Data Controller if the person has been convicted of a crime involving fraud or dishonesty. Data Processor shall, to the extent permitted by law, conduct a check of public records in all of the employee’s states/ country of residence and employment to verify the above.

4. Compliance

- Data Processor agrees to provide evidence upon request of compliance of any system or component used to process, store, or transmit Customer Data that is operated by Data Processor as part of its service. Similarly, Data Processor will be prepared to provide available evidence of compliance of any third party it has sub-contracted as part of the service offering. As evidence of compliance, Data Processor will provide, upon request, a current attestation of compliance. Data Processor shall take reasonable steps to periodically review and maintain its policies, standards, and procedures. An internal committee with representation from various parts of the organization will oversee our information technology security policies, standards, and procedures.

5. Network Security

- Data Processor agrees to maintain commercially reasonable network security that, at a minimum, includes:
 - Firewalls to protect the perimeter network;
 - Intrusion detection/prevention tools;
 - Periodic third party penetration testing;
 - Network security that at minimum conforms to an industry recognized standardAnti-spoofing filters enabled on routers;
 - Network, application and server authentication passwords meet minimum complexity guidelines and regularly changed, adhering to acceptable industry standards.
 - Initial user passwords changed during first logon, and policy prohibiting the sharing of user IDs and passwords.



- **Virtual Private Networks (“VPN”).** When remote connectivity to the data exporter network is required for processing of Customer Data, Data Processor uses VPN servers for the remote access.

6. Data Security

- Data Processor agrees to conform to the following measures:
 - a. Data Transmission.** Data Processor agrees that any transmission or exchange of system application data with Data Controller will occur through secure protocols, e.g. HTTPS, FTPS, SFTP, or equivalent means.
 - b. Data Storage and Backup.** Customer Data in production is not encrypted at rest. With respect to back up, Data Processor agrees to maintain (for the applicable contractual period) Data Controller’s Customer Data for backup and recovery processes in encrypted form, using no less than 128-bit key.
 - c. Testing Data.** Data Processor shall implement data protection and obfuscation during application testing or other processes outside of the production environment to sufficiently prevent identification of the actual individual or corporate customer to whom the original data refers, or preparing and executing a data protection plan.

7. System Acquisition, Development and Maintenance

- a. Security Requirements.** Data Processor has adopted security requirements for the purchase or development of information systems, including for application services delivered through public networks.
- b. Development Requirements.** Data Processor has policies for secure development, system engineering and support. Data Processor conducts appropriate tests for system security as part of regression testing processes.

8. Supplier Relationships

- a. Policies.** Data Processor has information security policies or procedures for its use of suppliers.
- b. Management.** Data Processor performs periodic reviews of key suppliers and manages service delivery commitments through contracts with its suppliers.

9. Data Breach

- Data Processor agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of personally identifiable information or other event requiring notification.

10. Safekeeping and Security

- Data Processor will be responsible for safekeeping all keys, access codes and similar security codes and identifiers issued to Data Processor’s employees, agents, contractors, or subcontractors. Data Processor shall ensure that access codes and passwords conforms to an industry recognized standard.



- a. **Access Policy.** An access control policy is established, documented, and reviewed based on business and information security requirements.
- b. **Access Recordkeeping.** Data Processor maintains a record of security privileges of its personnel that have access to personal data, networks and network services.
- c. **Access Authorization.**
 - i. Data Processor has user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to Data Processor's and/or its clients' systems and networks at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role.
 - ii. Data Processor maintains and updates a record of personnel authorized to access systems that contain personal data.
 - iii. Data Processor maintains strict policies against any shared "generic" user identification access.
 - iv. Data Processor maintains a password policy requiring accounts to be locked out after a defined maximum number of login attempts
- d. **Integrity and Confidentiality.**
 - i. Data Processor instructs its personnel to automatically lock screens and/or disable administrative sessions when leaving premises that are controlled by Data Processor or when computers are otherwise left unattended.
 - ii. Data Processor computers and trusted devices automatically lock after a defined period of inactivity.
 - iii. Data Processor stores passwords in a secured and restricted way that makes them unintelligible while they are in force.
- e. **Authentication.**
 - i. Data Processor uses industry standard practices to identify and authenticate users who attempt to access information systems. Where authentication mechanisms are based on passwords, Data Processor requires that the passwords be renewed regularly, based on acceptable industry standards.
 - ii. Where authentication mechanisms are based on passwords, Data Processor requires the password to conform to strong password control parameters including length, character complexity, and non-repeatability.
 - iii. Data Processor monitors repeated attempts to gain access to the information system using an invalid password.
 - iv. Data Processor maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.



11. Operations Security

- Data Processor will maintain policies describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data.

12. Physical Access to Facilities

- a. Data Processor limits access to facilities where systems that process personal data are located to authorized individuals.
- b. Access is controlled through key card and/or appropriate sign-in procedures for facilities with systems processing personal data. Personnel must be registered and are required to carry appropriate identification badges.
- c. A security alarm system or other appropriate security measures shall be in place to provide alerts of security intrusions after normal working hours.

13. Monitoring and Auditing

- Data Processor will regularly monitor and audit the effectiveness of its information security practices. Servers shall be scanned regularly to ensure they meet the current security standards.

14. Disaster Recovery

- To minimize potential losses and to permit resumption of processing, Data Processor shall maintain contingency plans consistent with the impact of any system failures on the business. These plans include a suitable backup and disaster recovery plan that is maintained, properly documented, periodically tested and appropriate for the system covered.