**DATA PROCESSING ADDENDUM**

This Data Processing Addendum ("DPA") supplements the ConnectWise Master Agreement and Addendums available at www.connectwise.com/legal, as updated from time to time between Client and ConnectWise, or other agreement between Client and ConnectWise governing Client's use of the Offerings (the "Agreement") when the GDPR applies to your use of the Offerings to process Client Data. This DPA is an agreement between you and the entity you represent ("Client", "you" or "your") and the applicable ConnectWise contracting entity under the Agreement ("ConnectWise").

RECITALS

a) ConnectWise and Client have entered into an Agreement together with one or more connected statements of work, schedules, purchase orders, contracts and/or agreements (collectively the " Agreement").

b) Pursuant to the Agreement, ConnectWise has agreed to provide certain SaaS based managed offerings as described in the Agreement to Client (the "Services" or "Offerings").

c) The Parties wish to define their respective data protection obligations relating to ConnectWise's provision of Offerings to Client in this DPA.

IN CONSIDERATION OF THE MUTUAL PROMISES BELOW AND OTHER GOOD AND VALUABLE CONSIDERATION THE SUFFICIENCY OF WHICH ARE HEREBY ACKNOWLEDGED, IT IS AGREED:

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.

"Authorized Affiliate" means any of Client'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 Client and ConnectWise, but has not signed its own Order Form with ConnectWise and is not a "Client" as defined under this DPA.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations. "Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Client" means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed Order Forms.

"Client Data" means what is defined in the Agreement as "Client Data" or "Your Data", provided that such data is electronic data and information submitted by or for Client to the Services. This DPA does not apply to Non-ConnectWise Applications as defined in the Agreement or, if not defined in the Agreement, as defined in the Master Agreement at https://www.connectwise.com/company/legal/.

"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, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Personal Data under the Agreement as amended from time to time.

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

"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), including as implemented or adopted under the laws of the United Kingdom.

"Personal Data" means any information 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 Client 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, 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, including as applicable any "service provider" as that term is defined by the CCPA.

"ConnectWise Group" means ConnectWise and its Affiliates engaged in the Processing of Personal Data.

"Standard Contractual Clauses" means Standard Contractual Clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.

"Sub-processor" means any Processor engaged by ConnectWise or a member of the ConnectWise Group.

"Supervisory Authority" means an independent public authority which is established by an EU Member State pursuant to the GDPR or, for the United Kingdom, the Information Commissioner's Office ("ICO").

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, Client is the Controller, ConnectWise is the Processor and that ConnectWise or members of the ConnectWise Group will engage Sub-processors pursuant to the requirements set forth in Section 5 "Sub-processors" below.

2.2 Client's Processing of Personal Data. Client shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of ConnectWise as Processor. For the avoidance of doubt, Client's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. Client shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Client acquired Personal Data. Client specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the CCPA.

2.3 ConnectWise's Processing of Personal Data. ConnectWise shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Client'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 Client (e.g., via email) where such instructions are consistent with the terms of the Agreement.

2.4 Details of the Processing. The subject-matter of Processing of Personal Data by ConnectWise 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 Schedule 2 (Details of the Processing) to this DPA.

3. RIGHTS OF DATA SUBJECTS

Data Subject Request. ConnectWise shall, to the extent legally permitted, promptly notify Client if ConnectWise 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, each such request being a "Data Subject Request". Taking into account the nature of the Processing, ConnectWise shall assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Client's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Client, in its use of the Services, does not have the ability to address a Data Subject Request, ConnectWise shall upon Client's request provide commercially reasonable efforts to assist Client in responding to such Data Subject Request to the extent ConnectWise is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Client shall be responsible for any costs arising from ConnectWise's provision of such assistance.

4. CONNECTWISE PERSONNEL

4.1 Confidentiality. ConnectWise 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 on their responsibilities and have executed written confidentiality agreements. ConnectWise shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

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

4.3 Limitation of Access. ConnectWise shall ensure that ConnectWise's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

5. SUB-PROCESSORS

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

5.2 List of Current Sub-processors and Notification of New Sub-processors. ConnectWise shall make available to Client the current listof Sub-processors for the Services identified in https://docs.connectwise.com/ConnectWise_Business_Knowledge/List_of_ConnectWise_Sub-Processors, which it shall update with details of any change in subprocessors and notify Client of the same at least 10 days' prior to any such change; (ii) ConnectWise imposes data protection terms on any subprocessor it appoints that require it to protect the Client Data to the standard required by Data Protection Laws and Regulations ; and (iii) ConnectWise remains liable for any breach of this DPA that is caused by an act, error or omission of its subprocessor. Client may object to ConnectWise's appointment or replacement of a subprocessor prior to its appointment or replacement, provided such objection is reasonable and founded on demonstrable grounds relating to the subprocessor's inability to comply with Data Protection Laws and Regulations.

5.3 Liability. ConnectWise shall be liable for the acts and omissions of its Sub-processors to the same extent ConnectWise 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.

6.SECURITY

6.1 Controls for the Protection of Client Data. ConnectWise shall 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, Client Data), confidentiality and integrity of Client Data, as set forth in the Technical and Organization Measures Security Documentation. ConnectWise regularly monitors compliance with these measures. ConnectWise will not materially decrease the overall security of the Services during a subscription term.

6.2 Third-Party Certifications and Audits. ConnectWise has obtained the third-party certifications and audits set forth in the Security, Privacy and Architecture Documentation. Upon Client's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, ConnectWise shall make available to Client that is not a competitor of ConnectWise (or Client's independent, third-party auditor that is not a competitor of ConnectWise) a copy of ConnectWise's then most recent third-party audits or certifications, as applicable.

6.3 Data Protection Impact Assessment. Upon Client's request, ConnectWise shall provide Client with reasonable cooperation and assistance needed to fulfil Client's obligation under the Data Protection Laws and Regulations to carry out a data protection impact assessment related to Client's use of the Services, to the extent Client does not otherwise have access to the relevant information, and to the extent such information is available to ConnectWise.

7.CLIENT DATA INCIDENT MANAGEMENT AND NOTIFICATION

ConnectWise maintains security incident management policies and procedures specified in the ConnectWise Trust site and shall notify Client without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Data, including Personal Data, transmitted, stored or otherwise Processed by ConnectWise or its Sub-processors of which ConnectWise becomes aware (a "Client Data Incident"). ConnectWise shall make reasonable efforts to identify the cause of such Client Data Incidentandtake thosesteps as ConnectWise deems necessary and reasonable in order to remediate the cause of such a Client Data Incidentto the extentthe remediation is within ConnectWise's reasonable control. The obligations herein shall not apply to incidents that are caused by Client or Client's Users.

8.DELETION OF CLIENT DATA

ConnectWise shall to the extent allowed by applicable law, delete Client Data in accordance within 60 days of the receipt of notification from the Client.

9.AUTHORIZED AFFILIATES

9.1 Contractual Relationship. The parties acknowledge and agree that, by executing the Agreement, Client 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 ConnectWise 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 Client.

9.2 Communication. The Client that is the contracting party to the Agreement shall remain responsible for coordinating all communication with ConnectWise 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 ConnectWise, 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 ConnectWise directly by itself, the parties agree that (i) solely the Client 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 Client 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 itself and 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 Client 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 ConnectWise and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its 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 ConnectWise, 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, ConnectWise's and its Affiliates' total liability for all claims from Client and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Client and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Client and/or to any Authorized Affiliate that is a contractual party to any such DPA.

11. EUROPEAN SPECIFIC PROVISIONS

11.1 GDPR. ConnectWise will Process Personal Data in accordance with the GDPR requirements directly applicable to ConnectWise's provision of its Services.

11.2 Data Protection Impact Assessment. ConnectWise shall provide reasonable assistance to Client in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to Section 6.3 of this DPA, to the extent required under the GDPR.

11.3 Transfer mechanisms for data transfers. Subject to the additional terms in Schedule 1, ConnectWise 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 and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations:

1. The Standard Contractual Clauses set forth in Schedule 3 to this DPA apply to the Services listed in https://docs.connectwise.com/ConnectWise_Business_Knowledge/List_of_ConnectWise_Sub-Processors to the Standard Contractual Clauses (the "SCC Services"), subject to the additional terms in Section 2 of Schedule 1.

12. LEGAL EFFECT

This DPA shall only become legally binding between Client and ConnectWise when the formalities steps set out in this agreement have been fully completed.

List of Schedules

Schedule 1: Transfer Mechanisms for European Data Transfers

Schedule 2: Details of the Processing

Schedule 3: Standard Contractual Clauses

SCHEDULE 1 - TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS 1.

1. ADDITIONAL TERMS FOR SCC SERVICES

1.1. Clients covered by the Standard Contractual Clauses. The Standard Contractual Clauses and the additional terms specified in this Section 2 apply to (i) Client which 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, (ii) its Authorized Affiliates. For the purpose of the Standard Contractual Clauses and this Section 2, the aforementioned entities shall be deemed "data exporters".

1.2. Instructions. This DPA and the Agreement are Client's complete and final documented instructions at the time of signature of the Agreement to ConnectWise for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the Client 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 SCC Services and (c) Processing to comply with other reasonable documented instructions provided by Client (e.g., via email) where such instructions are consistent with the terms of the Agreement.

1.3. Data Exports from the United Kingdom under the Standard Contractual Clauses. In case of any transfers of Personal Data under this DPA under the Standard Contractual Clauses from the United Kingdom, to the extent such transfers are subject to Data Protection Laws and Regulations applicable in the United Kingdom ("UK Data Protection Laws"), (i) general and specific references in the Standard Contractual Clauses to the GDPR shall hereby be deemed to have the equivalent reference in the UK Data Protection Laws; (ii) References in the Standard Contractual Clauses to "the law of the Member State in which the data exporter is established" shall hereby be deemed to mean "the law of the United Kingdom"; (iii) any other obligation in the Standard Contractual Clauses determined by the Member State in which the data exporter is established shall hereby be deemed to refer to an obligation under UK Data Protection Laws; and (iv) references in clause 17 and 18 of the Standard Contractual Clauses to the Republic of Ireland shall be deemed to refer to England and Wales.

1.4. Appointment of new Sub-processors and List of current Sub-processors. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Client acknowledges and expressly agrees that (a) ConnectWise's Affiliates may be retained as Sub-processors; and (b) ConnectWise and ConnectWise's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the SCC Services. ConnectWise shall make available to Client the current list of sub-processors in accordance with Section 5.2 of this DPA.

1.5. Notification of New Sub-processors and Objection Right for new Sub-processors. Pursuant to Clause 5(h) of the Standard Contractual Clauses, Client acknowledges and expressly agrees that ConnectWise may engage new Sub-processors as described in Sections 5.2 and 5.3 of the DPA.

1.6. Copies of Sub-processor Agreements. The parties agree that the copies of the Sub-processor agreements that must be provided by ConnectWise to Client pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by ConnectWise beforehand; and, that such copies will be provided by ConnectWise, in a manner to be determined in its discretion, only upon request by Client.

1.7. Audits and Certifications. The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications:

Upon Client's request, and subject to the confidentiality obligations set forth in the Agreement, ConnectWise shall make available to Client that is not a competitor of ConnectWise (or Client's independent, third-party auditor that is not a competitor of ConnectWise) information regarding the ConnectWise Group's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits set forth in the ConnectWise Trust Site Compliance page to the extent ConnectWise makes them generally available to its clients. Client may contact ConnectWise in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protectionof Personal Data. Client shall reimburse ConnectWise for any time expended for any such on-site audit at the ConnectWise Group's then-current professional services rates, which shall be made available to Client upon request. Before the commencement of any such on-site audit, Client and ConnectWise shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Client shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by ConnectWise. Client shall promptly notify ConnectWise with information regarding any non-compliance discovered during the course of an audit.

1.8. Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by ConnectWise to Client only upon Client's request.

1.9. Conflict. In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Schedule 3, the Standard Contractual Clauses shall prevail.

SCHEDULE 2 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing
ConnectWise will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Client in its use of the Services.

Duration of Processing
Subject to Section 8 of the DPA, ConnectWise will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects
Client may submit Personal Data to the Services, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Client (who are natural persons)
- Employees or contact persons of Client's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Client (who are natural persons)
- Client's Users authorized by Client to use the Services

Type of Personal Data

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

- First and last name
- Contact information (company, email, phone, physical business address)
- Position
- Employer
- Mailing Address
- Business Phone
- Mobile Phone
- Computer Name
- Computer IP address
- Computer MAC address
- Computer access password
- ID data
- Professional life data
- Connection data
- Localisation data

Computer name, IP address, and Mac address are collected via the ConnectWise Offering installed and run on partner customer end-points.

In addition, ConnectWise may process, under the terms of the Agreement, personal data which the End-Client elects to host with or upload to the Client in connection with the Client's provision of services to its End-Client.

SCHEDULE 3

**STANDARD CONTRACTUAL CLAUSES**

Controller to Processor

**SECTION I**

***Clause 1***

**Purpose and scope**

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

(b) The Parties:

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

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

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

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

***Clause 2***

**Effect and invariability of the Clauses**

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

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

***Clause 3***

**Third-party beneficiaries**

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

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

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

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

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

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

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

***Clause 4***

**Interpretation**

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

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

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

***Clause 5***

**Hierarchy**

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

***Clause 6***

**Description of the transfer(s)**

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

***Clause 7 – INTENTIONALLY OMITTED.***

**SECTION II – OBLIGATIONS OF THE PARTIES**

***Clause 8***

**Data protection safeguards**

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

**8.1 Instructions**

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

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

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

**8.3 Transparency**

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

**8.4 Accuracy**

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

**8.5 Duration of processing and erasure or return of data**

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

**8.6 Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach,

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

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

**8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

**8.8 Onward transfers**

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

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

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

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

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

**8.9 Documentation and compliance**

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

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

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

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

***Clause 9***

**Use of sub-processors**

(a) 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 ten (10) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

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

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

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

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

***Clause 10***

**Data subject rights**

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

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

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

***Clause 11***

**Redress**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

***Clause 12***
**Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

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

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

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

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

***Clause 13***

**Supervision**

(a) [Where the data exporter is 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**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based

on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([4]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

***Clause 15***

**Obligations of the data importer in case of access by public authorities**

**15.1 Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

**SECTION IV – FINAL PROVISIONS**

***Clause 16***

**Non-compliance with the Clauses and termination**

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

***Clause 17***

**Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Republic of Ireland.

***Clause 18***

**Choice of forum and jurisdiction**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of 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.

**APPENDIX**

**ANNEX I**

**A. LIST OF PARTIES**

**Data exporter(s):** [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: _____The Client named in the Schedule or Order Form._____

Address: _Client's address as specified in the Schedule or Order Form.

Contact person's name, position and contact details: Client's primary contact in the Schedule or Order Form.

Activities relevant to the data transferred under these Clauses:

The provision of software and related services by ConnectWise to the Client.

Role (controller/processor): Controller

2. …

**Data importer(s):**

Name: ConnectWise, LLC

Address: 4110 George Road, Suite 200, Tampa, Florida 33634

Contact person's name, position and contact details: privacy@connectwise.com

Activities relevant to the data transferred under these Clauses:

The provision of software and related services by ConnectWise to the Client. Role (controller/processor): processor

2. …

**B. DESCRIPTION OF TRANSFER**

*Categories of data subjects whose personal data is transferred*

*Client's employees and contractors*

*Categories of personal data transferred*

- *First and last name*
- *Contact information (company, email, phone, physical business address)*
- *Position*
- *Employer*
- *Mailing Address*
- *Business Phone*
- *Mobile Phone*
- *Computer Name*
- *Computer IP address*
- *Computer MAC address*
- *Computer access password*
- *ID data*
- *Professional life data*
- *Connection data*
- *Localisation data*

*Computer name, IP address, and Mac address are collected via the ConnectWise Offering installed and run on partner customer end-points.*

*In addition, ConnectWise may process, under the terms of the Agreement, personal data which the End-Client elects to host with or upload to the Client in connection with the Client's provision of services to its End-Client. 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 frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

*Continuous*

*Nature of the processing*

*ConnectWise will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Client in its use of the Services.Purpose(s) of the data transfer and further processing*

*ConnectWise will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Client in its use of the Services.The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

*ConnectWise will retain Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Client in its use of the Services.For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

*ConnectWise will transfers to (sub-) processors as necessary to perform the Services pursuant to the Agreement, as further specified in the Documentation, and as further instructed by Client in its use of the Services*

**C. COMPETENT SUPERVISORY AUTHORITY**

*Identify the competent supervisory authority/ies in accordance with Clause 13*

*The supervisory authority will be as set forth in Clause 13.*

**ANNEX II**

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

***Measures of pseudonymization and encryption of personal data.***

*ConnectWise maintains Customer Data in an encrypted format at rest using Advanced Encryption Standard and in transit using TLS.*

***Measures for ensuring ongoing confidentiality, integrity, and availability and resilience of processing systems and services.***

*ConnectWise's customer agreements contain strict confidentiality obligations. Additionally, ConnectWise requires every downstream Sub processor to sign confidentiality provisions that are substantially similar to those contained in ConnectWise's customer agreements. The infrastructure for the ConnectWise Offerings spans multiple cloud environments utilizing fault-independent availability zones in geographic regions physically separated from one another, supported by various tools and processes to maintain high availability of services.*

***Measures for ensuring the ability to restore availability and access to Personal Data in a timely manner in the event of a physical or technical incident.***

*ConnectWise performs regular data backups of Customer Data, which is hosted in AWS and various cloud data centers. Backups are retained redundantly across multiple availability zones and encrypted in transit and at rest using Advanced Encryption Standard (AES-256).*

***Processes for regular testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of processing.***

*ConnectWise maintains a risk-based assessment security program. The framework for ConnectWise's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Offerings and confidentiality, integrity, and availability of Customer Data. ConnectWise's security program is intended to be appropriate to the nature of the Offerings and the size and complexity of ConnectWise's business operations. ConnectWise has a separate and dedicated security team that manages ConnectWise's security program. This team facilitates and supports independent audits and assessments performed by third-parties to provide independent feedback on the operating effectiveness of the information security program.*

***Measures for user identification and authorization.***

*ConnectWise personnel are required to use unique user access credentials and passwords for authorization. ConnectWise follows the principles of least privilege through role-based and time-based access models when provisioning system access. ConnectWise personnel are authorized to access Customer Data based on their job function, role and responsibilities, and such access requires approval prior to access provisioning. Access is promptly removed upon role change or termination.*

***Measures for the protection of data during transmission.***

*End Customer Data is encrypted when in transit between Customer and the corresponding ConnectWise Offering using TLS.*

***Measures for the protection of data during storage.***

*Customer Data is stored encrypted using the Advanced Encryption Standard.*

***Measures for ensuring physical security of locations at which personal data are processed.***

*ConnectWise headquarters and office spaces have a physical security program that manages visitors, building entrances, CCTVs (closed circuit televisions), and overall office security. All employees, contractors, and visitors are required to wear identification badges.*

*The Offerings operate on Amazon Web Offerings ("AWS") and other cloud providers listed on the ConnectWise sub-processor list and are protected by the security and environmental controls of respective cloud provider.*

***Measures for ensuring events logging.***

*ConnectWise monitors access to applications, tools, and resources that process or store Customer Data, including cloud services. Monitoring of security logs is centralized by the security team. Log activities are investigated when necessary and escalated appropriately.*

***Measures for ensuring systems configuration, including default configuration.***

*ConnectWise applies Secure Software Development Lifecycle (Secure SDLC) standards to perform numerous security-related activities for the Offerings across different phases of the product creation lifecycle from requirements gathering and product design all the way through product deployment. These activities include, but are not limited to, the performance of (a) internal security reviews before new Offerings are deployed; (b) annual penetration testing by independent third parties; and (c) threat models for new Offerings to detect any potential security threats and vulnerabilities.*

*ConnectWise adheres to a change management process to administer changes to the production environment for the Offerings, including changes to its underlying software, applications, and systems.*

***Measures for internal IT and IT security governance and management.***

*ConnectWise maintains a risk-based assessment security program. The framework for ConnectWise's security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the Offerings and confidentiality, integrity, and availability of Customer Data. ConnectWise's security program is intended to be appropriate to the nature of the Offerings and the size and complexity of ConnectWise's business operations. ConnectWise has a separate and dedicated Information Security team that manages ConnectWise's security program. This team facilitates and supports independent audits and assessments performed by third parties. ConnectWise's security framework is based on the ISO 27001 Information Security Management System and includes programs covering: Policies and Procedures, Asset Management, Access Management, Cryptography, Physical Security, Operations Security, Communications Security, Business Continuity Security, People Security, Product Security, Cloud and Network Infrastructure Security, Security Compliance, Third-Party Security, Vulnerability Management, and Security Monitoring and Incident Response. Security is managed at the highest levels of the company, with the Chief Information Security Officer meeting with executive management regularly to discuss issues and coordinate company-wide security initiatives. Information security policies and standards are reviewed and approved by management at least annually and are made available to all ConnectWise employees for their reference.*

***Measures for certifications/assurance of processes and products.***

*ConnectWise conducts various third-party audits to attest to various frameworks including SOC 2 Type 2, and annual application penetration testing.*

***Measures for ensuring data minimization.***

*ConnectWise Customers unilaterally determine what Customer Data they store and consume within the ConnectWise Offerings and how the Offerings are configured. As such, ConnectWise operates on a shared responsibility model. ConnectWise provides tools within the Offerings that gives Customers control over exactly what data enters the platform and enables Customers with the ability to block data at the Source level. Additionally, ConnectWise has built in self-service functionality to the Offerings that allow Customers to delete and suppress Customer Data on demand.*

***Measures for ensuring data quality.***

*ConnectWise has a multi-fold approach for ensuring data quality. These measures include: (i) unit testing to ensure the quality of logic used to make API calls, and (ii) volume testing to ensure the code is able to scale. ConnectWise applies these measures across the board, both to ensure the quality of any Usage Data that ConnectWise collects and to ensure that the ConnectWise Platform is operating in accordance with the documentation.*

*Each ConnectWise Partner chooses what Customer Data they route through the ConnectWise Offerings and how the Offerings are configured. As such, ConnectWise operates on a shared*

*responsibility model. ConnectWise ensures that data quality is maintained from the time a Customer sends Customer Data into the Offerings and while maintained within the Offerings*

***Measures for ensuring limited data retention.***

*ConnectWise Customers unilaterally determine what Customer Data they route through the ConnectWise Offerings and how the Offerings are configured. As such, ConnectWise operates on a shared responsibility model. If a Partner is unable to delete Customer Data via the functionality within the Offering, then ConnectWise deletes Customer Data upon the Customer's written request, within the timeframe specified in the Data Protection Addendum and in accordance with Applicable Data Protection Law.*

***Measures for ensuring accountability.***

*ConnectWise has adopted measures for ensuring accountability, such as implementing data protection policies across the business, maintaining documentation of processing activities, recording and reporting Security Incidents involving Personal Data. Additionally, ConnectWise conducts regular third-party audits to ensure compliance with our privacy and security standards.*

***Measures for allowing data portability and ensuring erasure.***

*ConnectWise's Partners have direct relationships with their end customers and are responsible for responding to requests from their end customers who wish to exercise their rights under Applicable Data Protection Laws. If ConnectWise receives a request from a Data Subject in relation to their Customer Data, ConnectWise will advise the Data Subject to submit their request to the Partner, and the Partner will be responsible for responding to any such request.*

**ANNEX III**

**LIST OF SUB-PROCESSORS**

https://docs.connectwise.com/ConnectWise_Business_Knowledge/List_of_ConnectWise_Sub-Processors

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

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

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.