# CONNECTWISE DATA PROCESSING ADDENDUM (DPA)

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"). This DPA shall be effective as of the date accepted. The terms of this DPA replace any previously applicable data processing terms as of the date of execution.

**RECITALS**

a) ConnectWise and Client have entered into an Agreement together with one or more connected statements of work, 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 "**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**

In this DPA, the following terms shall have the following meanings:

"**controller**", "**processor**", "**data subject**", "**personal data**", "**processing**" (and "**process**") "**special categories of personal data**" and shall have the meanings given in European Data Protection Law.

"**Controller Model Clauses**" means the European Commission's model clauses for the transfer of Personal Data from EU Controllers to a non-EU or EEA Controllers, the approved version of which in force at present is that set out in the European Commission's Decision 2004/915/EC of 27 December 2004, available at: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en and as may be amended or replaced by the European Commission from time to time.

"**European Data Protection Law**" shall mean the applicable European data protection legislation, including, but not limited to: (a) EU Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (also known as the General Data Protection Regulation) (the "**GDPR**"), and (b) any and all applicable national data legislation made under or pursuant to the GDPR; in each case, as may be amended from time to time.

"**End-Clients**" means business end-clients and/or end-customers to whom the Client provides managed services using the support of the Offerings, where applicable.

"**Processor Model Clauses**" the European Commission's model clauses for the transfer of Personal Data from EU Controllers to non-EU or EEA Processors, the approved version of which in force at present is that set out in the European Commission's Decision 2010/87/EU of 5 February 2010, which are available at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outsideeu/model-contracts-transfer-personal-data-third-countries_en;

"**Security Incident**" means a breach of security leading to any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Client Personal Data.

**2) Relationship of the parties**

a. Client (as a controller, and where applicable, a processor acting on behalf of its End-Clients) appoints ConnectWise as its processor to process the personal data that is the subject of the Agreement and as more particularly described in Annex A (the "**Client Data**") for the purposes of and in connection with delivering to Client the Offerings described in the Agreement (the "**Permitted Purpose**"). Except where otherwise required by applicable law, ConnectWise shall process the Client Data (i) in accordance with Client's documented instructions (which instructions are set out in the Agreement, this DPA and Client), (ii) for the purposes of providing the Offering as further described in Annex A.

b. ConnectWise will also process certain personal data (such as names, contact details e.g. email addresses and correspondence and details about use of the Offerings) of Client's employees, contractors, agents and other representatives ("**CRM Data**") in connection with ConnectWise's Offerings, including for example for: (i) correspondence between ConnectWise and Client; (ii) invoicing, billing and other business inquiries related to the Agreement or any Offerings; (iii) information on ConnectWise's performance of the Offerings (including metadata and IP addresses in relation to use of the Offerings); and (iv) general management of the Agreement, the Offerings and the relationship between the parties including marketing. The Parties acknowledge that ConnectWise shall be an independent controller of the CRM Data. Client agrees to provide such employees and other representatives, within a reasonable time but at the latest within one month of this DPA, with notice of ConnectWise's processing of the CRM Data and to refer them to ConnectWise's Privacy Policy www.*connectwise.com/privacy* or information about such processing.

c. Each Party agrees to comply with the obligations that apply to it under European Data Protection Law with regards to its processing of the Client Data and the CRM Data.

**3) International transfers**

Client acknowledges and agrees that ConnectWise may transfer and process Client Data anywhere in the world where ConnectWise, its affiliates or its subprocessors maintain data processing operations. Where European Data Protection Law applies to Client Data ("**European Data**"), ConnectWise shall not process or transfer European Data outside of the European Economic Area ("**EEA**"), the United Kingdom ("**UK**") or Switzerland unless it has taken such measures as are necessary to ensure the transfer is in compliance with European Data Protection Law. Where ConnectWise transfers to a receipting in a country that the European Commission or any applicable UK authority has not decided provides adequate protection for European Data, such measures may include (without limitation) transferring European Data out of the EEA, UK or Switzerland on the basis of (i) appropriate Model Clauses; (ii) on the basis of ConnectWise having implemented Binding Corporate Rules approved by competent EU or UK data protection authorities and/or (iii) any mechanism approved by the European Commission or other relevant data protection authority.

Where required under European Data Protection Law to transfer Client Data to ConnectWise, Client and ConnectWise will be deemed to have entered into the Processor Model Clauses with Client as the 'data exporter", ConnectWise as the "data importer", Appendix 1 and Appendix 2 to the Processor Model Clauses shall be deemed completed with Annex A and Annex B of this DPA, and with the Additional Terms in the Model Clauses set out in Annex C of this DPA. The date of the Processor Model Clauses shall be the date of the DPA. It is not the intention of either party, nor the effect of this DPA, to contradict or restrict any of the provisions set out in the Processor Model Clauses. Accordingly, if and to the extent the Processor Model Clauses conflict with any provision of this DPA, the Processor Model Clauses shall prevail to the extent of such conflict.

Where ConnectWise is onward transferring Client Data outside the EEA or UK under Model Clauses, Client authorises ConnectWise to enter into the Controller Model Clauses for the benefit of Client or its End-Clients.

Where Client is transferring European CRM Data to ConnectWise outside of the EEA, UK or Switzerland and to a country that the European Commission or any applicable UK authority has not decide provides adequate protection for European CRM data, Client and ConnectWise will be deemed to have entered into the Controller Model Clauses as follows: the Client is the "data exporter", ConnectWise is the "data importer", in Clause II of the Controller Model Clauses, option h(iii) (the data processing principles set forth in Annex A) will be deemed to have been selected, the provisions in Section 2(b) of this DPA will be deemed to be set out in Annex B, the optional illustrative commercial clauses will be deemed to have been deleted, and if there is any conflict between this DPA and the Controller Model Clauses, the Controller Model Clauses will prevail.

**4) Transfers after Brexit**

In the event that European Union law ceases to apply to the UK then:

a. to the extent that the Client Data is subject to the GDPR by virtue of European Union law, ConnectWise shall not transfer the Client Data to (nor permit the Data to be processed in or from) the UK unless it takes such measures as are necessary to ensure the transfer is in compliance with European Data Protection Law; and

b. ConnectWise shall not transfer the Data to (nor permit the Data to be processed in or from) a country outside of the UK unless it complies with the requirements of UK Data Protection Law.

**5) Confidentiality of processing**

ConnectWise shall ensure that any person it authorizes to process the Client Data (an "**Authorized Person**") shall protect the Client Data in accordance with ConnectWise's confidentiality obligations under the Agreement.

**6) Security**

ConnectWise shall implement technical and organisational measures as set out in Annex B to protect the Client Data from Security Incidents.

**7) Subcontracting**

Client consents to ConnectWise engaging third party subprocessors to process the Client Data for the Permitted Purpose provided that: (i) ConnectWise maintains an up-to-date list of its subprocessors which can be found at 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 European Data Protection Law; 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 European Data Protection Law.

**8) Cooperation and data subjects' rights**

ConnectWise shall provide reasonable and timely assistance to Client (at Client's expense) to enable Client and/or an End-Client to respond to: (i) any request from a data subject to exercise any of its rights under European Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, regulator or other third party in connection with the processing of the Client Data. In the event that any such valid request, correspondence, enquiry or complaint is made directly to ConnectWise, ConnectWise shall inform Client providing full details of the same in a timely fashion.

**9) Data protection impact assessment**

If ConnectWise believes or becomes aware that its processing of the Client Data is likely to result in a high risk to the data protection rights and freedoms of data subjects, it shall inform Client and provide reasonable cooperation to Client (at Client's expense) in connection with any data protection impact assessment that may be required under European Data Protection Law.

**10) Security incidents**

If it becomes aware of a confirmed Security Incident, ConnectWise shall inform Client without undue delay and shall provide reasonable information and cooperation to Client so that Client (and/or End-Client) can fulfil any data breach reporting obligations it may have under (and in accordance with the timescales required by) European Data Protection Law. ConnectWise shall further take such reasonable necessary measures and actions to remedy or mitigate the effects of the Security Incident and shall keep Client (and/or End-Client) up to date of all material developments in connection with the Security Incident.

**11) Deletion or return of Client Data**

Upon termination or expiry of the Agreement, ConnectWise shall (at Client's election) destroy or return to Client all

Client Data in its possession or control provided that Client agrees to pay any reasonable costs associated with retrieval where retrieval by Client is otherwise possible. This requirement shall not apply to the extent that ConnectWise is required by applicable law to retain some or all of the Client Data, or to Client Data it has archived on back-up systems, which ConnectWise shall securely isolate and protect from any further processing until deletion is possible except to the extent required by such law.

**12) Audit**

Client acknowledges that ConnectWise is regularly audited against SOC-2 standards by independent third-party auditors. Upon request, ConnectWise shall supply a summary copy of its audit report(s) to Client, which reports shall be subject to the confidentiality provisions of the Agreement.

**13) Miscellaneous**

a. Headings in this DPA are for convenience of reference only and will not constitute a part of or otherwise affect the meaning or interpretation of this DPA.

b. Annexes to this DPA will be deemed to be an integral part of this DPA to the same extent as if they had been set forth verbatim herein.

c. To the extent there is any conflict or inconsistency between this DPA and any other terms of the Agreement, or contracts between the parties relating to its subject matter, the terms of this DPA shall prevail.

d. The provisions of this DPA are severable. If any phrase, DPA or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability will affect only such phrase, DPA or provision, and the rest of this DPA will remain in full force and effect.

e. The provisions of this DPA will endure to the benefit of and will be binding upon the Parties and their respective successors and assigns.

f. This DPA shall be governed by and construed in all respects in accordance with the governing law and jurisdiction as prescribed in the Agreement.

## Annex A

This Annex A forms part of the DPA and describes the Client Data that ConnectWise will process on behalf of Client and/or End Client

**Data exporter**
The data exporter is (please specify briefly your activities relevant to the transfer):
Data Exporter is (i) the legal entity that has executed the DPA and, (ii) all Affiliates (as defined in the Agreement) of Client or the End-Client established within the European Economic Area (EEA), United Kingdom (UK) and Switzerland that have purchased the ConnectWise Offering.

**Data importer**
The data importer is (please specify briefly activities relevant to the transfer):
ConnectWise provides a SaaS-based managed services platform that managed services providers use to efficiently backup, monitor, troubleshoot, and maintain desktops, servers (physical and virtual), mobile devices and other endpoints to Clients and End-Clients.

**Type(s) of Personal Data processed:**
Depending on the Offering chosen by the Client, ConnectWise will process on behalf of Client the following personal data:

- First Name
- Last Name
- 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.

**Special Categories of Personal Data (if applicable):**
Client and/or End Client may submit special categories of data to the ConnectWise Offering, the extent of which is determined and controlled by the data exporter in its sole discretion, and which is for the sake of clarity Client Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

**Categories of Data Subjects:**
ConnectWise will process on behalf of Client and/or End Client personal data of the following categories data subjects:

- consultants, contractors, agents and/or employees of Client;
- consultants, contractors, agents and/or employees End-Client(s); and/or
- third parties with which the End-Client conducts business.

**Purposes of Processing:**
As a processor, ConnectWise shall process the above Client Data only for the purposes of processing to provide

the applicable Offerings in accordance with the Agreement; and the terms of the Agreement and the parties acknowledge that this DPA shall constitute the Client's complete and final documented instructions to ConnectWise for these purposes.

**Annex B**
**DATA SECURITY GUIDE**

This Data Security Guide describes the measures ConnectWise takes to protect Client Data. This Data Security Guide forms a part of any legal agreement into which this Data Security Guide is explicitly incorporated by reference (the "DPA") and is subject to the terms of the DPA. Capitalized terms not otherwise denoted in this Data Security Guide will have the meaning given to them in other parts of the DPA.

## 1. SECURITY PROGRAM

While providing the Offering, ConnectWise will maintain a written information security program of policies, procedures, and controls governing the processing, storage, transmission and security of Client Data (the "Security Program"). The Security Program includes industry-standard practices designed to protect Client Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. ConnectWise regularly tests, assesses and evaluates the effectiveness of the Security Program and may periodically review and update the Security Program to address new and evolving security technologies, changes to industry standard practices and changing security threats.
Although no such update will materially reduce the commitments, protections or overall level of service provided to Client as described herein.

## 2. TECHNICAL AND ADMINISTRATIVE SECURITY MEASURES

TECHNICAL SECURITY MEASURES

**a) Access Administration.** Access to the Offering by ConnectWise employees and contractors is protected by authentication and authorization mechanisms. User authentication is required to gain access to production and subproduction instances. Access privileges are based on job requirements and are revoked upon termination of employment or consulting relationships. Production infrastructure includes appropriate user account and password controls (e.g. the required use of VPN connections. complex passwords with expiration dates) and is accessible for administration.

**b) Service Access Control.** The Offering provides user and role-based access controls. Client is responsible for configuring such access controls within its instance.

**c) Logging and Monitoring**. The production infrastructure log activities are centrally collected and are secured in an effort to prevent tampering and are monitored for anomalies by a trained Security learn.

**d) Firewall Systems.** Industry-standard firewalls are installed and managed to protect ConnectWise systems by residing on the network to inspect all ingress connections routed to the ConnectWise environment.

**e) Vulnerability Management.** ConnectWise conducts periodic independent security risk evaluations to detect critical information assets, assess threats to such assets and determine potential vulnerabilities and provide for remediation. When software vulnerabilities are revealed and addressed by a vendor patch, ConnectWise will obtain the patch from the applicable vendor and apply it within an appropriate timeframe in accordance with ConnectWise's current vulnerability management and security patch management standard operating procedures and only after such patch is tested and determined to be safe for installation in all production systems.

**f) Antivirus** ConnectWise updates antivirus, anti-malware and anti-spyware software on regular intervals and centrally logs events for effectiveness of such software.

**g) Change Control** ConnectWise ensures that changes to platform, applications and production infrastructure are evaluated to minimize risk and are implemented following ConnectWise's standard operating procedure.

**h) Data Separation** Client Data shall be maintained within a logical single-tenant architecture on multi-tenant cloud infrastructure that is logically and physically separate from ConnectWise's corporate infrastructure.

ADMINISTRATIVE SECURITY MEASURES

**a) Security Awareness and Training** ConnectWise maintains a security awareness program that includes appropriate training of ConnectWise personnel on the Security Program. Training is conducted at time of hire and periodically throughout employment at ConnectWise.

**b) Vendor Risk Management** ConnectWise maintains a vendor risk management program that assesses all vendors that access, store, process or transmit Client Data for appropriate security controls and business

## 3. CERTIFICATIONS AND AUDITS

**a)** ConnectWise shall establish and maintain sufficient controls to meet the objectives stated in SOC 2 Type 2 (or equivalent standards) (collectively. the “Standards”) for the information security management system supporting the Offering. At least once per calendar year, ConnectWise shall obtain an assessment against such Standards by an independent third-party auditor.

## 4. AUDITS AND CORRECTIVE ACTIONS

**a) Audits.** Upon Client's request ConnectWise shall grant Client access to the ConnectWise documentation where Client may access industry-recognized documentation evidencing the Security Program ("Audit”). Such documentation will include a copy of ConnectWise's certification or audit reports performed by an independent third-party of ConnectWise's information security management system supporting the Offering against the Standards.

**b) Corrective Actions.** ConnectWise and Client may schedule a mutually convenient time to discuss the Audit. If a material deficiency is discovered between ConnectWise commitments in this Data Security Guide and the information gathered during an Audit then ConnectWise shall take at its own cost the necessary corrective actions. This sets forth Client's exclusive rights and remedies (and ConnectWise sole liability) with respect to any material deficiencies noted during an Audit and the results derived therefrom are Confidential Information of ConnectWise.

## 5. MONITORING AND INCIDENT MANAGEMENT

**a) Incident Monitoring and Management** ConnectWise will monitor, analyze and respond to security incidents in a timely manner in accordance with ConnectWise's standard operating procedure. ConnectWise security group will escalate and engage response teams as may be necessary to address anincident,

**b) Breach Notification** Unless notification is delayed by the actions or demands of a law enforcement agency. ConnectWise will report to Client any accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to Client Data (a “Security Incident”) without undue delay following determination by ConnectWise that a Security Incident has occurred.

**c) Report** The initial report will be made to Client security or privacy contact(s) (or if no such contact(s) are designated, to the primary contact designated by Client). As information is collected or otherwise becomes available to ConnectWise and unless prohibited by applicable law ConnectWise shall provide without undue delay any further information regarding the nature and consequences of the Security Incident to allow Client to notify relevant parties including affected Data Subjects, government agencies and data protection authorities in accordance with applicable data protection law. The report will include the name and contact information of the ConnectWise contact from whom additional information may be obtained ConnectWise shall inform Client of the measures that it will adopt to mitigate the cause of the Security Incident and to prevent future Security Incidents.

**d) Client Obligations** Client will cooperate with ConnectWise in maintaining accurate contact information in the customer support portal and by providing any information that is reasonably requested to resolve any security incident, including any Security Incidents, identify its root cause(s) and prevent a recurrence. Client is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects and for providing such notice.

## 6. COOKIES

When providing the Offering, ConnectWise uses cookies to (i) track session state, (ii) route a browser request to a specific node when multiple nodes are assigned, and (iii) recognize a user upon returning to the Offering. Client shall be responsible for providing notice to, and collecting any necessary consents from, its authorized users of the Offering for ConnectWise's use of cookies.

## 7. PENETRATION TESTS BY A THIRD-PARTY

ConnectWise contracts with third-party vendors to perform an annual penetration test on the ConnectWise application family to identity risks and remediation that help increase security.

## 8. SHARING THE SECURITY RESPONSIBILITY

**a) PRODUCT CAPABILITIES** The Offering has the capabilities to, (i) authenticate users before access, (ii) encrypt passwords, (iii) allow users to manage passwords, and (iv) prevent access by users with an inactive account Client manages each user's access to and use of the Offering by assigning to each use a credential and user type that controls the level of access to the Offering. Client shall be responsible for implementing encryption and access control functionalities available within the Offering, for protecting all Client Data containing sensitive data, including credit card numbers, social security numbers and other government issues identification numbers, financial and health information, Personal Data, and any Personal Data deemed sensitive or special categories of personal data under European Data Protection Law. Client is solely responsible for its decision not to encrypt such data and

ConnectWise will have no liability to the extent that damages would have been mitigated by Client's use of such encryption measures. Client is responsible for protecting the confidentiality of each user's login and password and managing each users access to the Offering.

**b) CLIENT COOPERATION** Client shall promptly apply any application upgrade that ConnectWise determines is necessary to maintain the security performance or availability of the Offering.

**c) LIMITATIONS** Notwithstanding anything to the contrary in this Data Security Guide or other parts of the DPA. ConnectWise's obligations extend only to those systems, networks, network devices, facilities, and components over which ConnectWise exercises control. This Data Security Guide does not apply to, (i) information shared with ConnectWise that is not data stored in its systems using the Offering, (ii) data in Client's VPN or a third-party network, (iii) any data processed by Clients or its users in violation of the DPA or this Data Security Guide, or (iv) Integrated Products. For the purposes of this Data Security Guide, "Integrated Products" shall mean ConnectWise -provided integrations to third-party products or any other third-party products that are used by Client in connection with the Offering. Client agrees that its use of such Integrated Products will be, (i) in compliance with all applicable laws, including but not limited to European Data Protection Law, and (ii) in accordance with as contractual agreement with the provider of such Integrated Products. Any Personal Data populated from the Integrated Products to the Offering must be collected, used, disclosed and, if applicable, internationally transferred in accordance with Client's privacy policy, which will adhere to European Data Protection Law. For clarity, as between ConnectWise and Client, Client assumes all liability tor any breaches of confidentiality that occur outside of the Offering.

**Annex C**
**ADDITIONAL CLAUSES**

The parties agree that the audits described in Clause 5(f), Clause 11 and Clause 12(2) of the Processor Standard Contractual Clauses shall be carried out in accordance with the Section 12 of the Data Processing Addendum.

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

The parties agree that Data Exporter's consent for sub-processing as set forth in Section 3 of the Data Processing Addendum shall be deemed consent for the purposes of these Processor Standard Contractual Clauses.

| **CLIENT** | | | | | |
|---|---|---|---|---|---|
| Company Name | | | | | |
| Phone | | Fax | | | |
| Street Address | | | | | |
| City | | State | | Zip | |
| Website | | | | Country | |
| Technical Staff Count | | Sales Staff Count | | | |
| **CONTACT INFORMATION** | | | | | |
| Primary Business Contact | | Title | | | |
| Phone | ` | Email | | | |
| Primary Technical Contact | | Title | | | |
| Phone | | Email | | | |
| **BILLING INFORMATION** | | | | | |
| Business Structure (Please Circle One) | Sole Owner | Partnership | | Corporation | |
| Billing Contact | | Title | | | |
| Phone | | Email | | | |
| Billing Currency (Please Circle One) | U.S. Dollar | Euro | | Pound Sterling | |

This Agreement is a binding contract between ConnectWise and Client and is effective as of the latest date of signature appearing below.

| | |
|---|---|
| Client | ConnectWise |
| Authorized Signature | Authorized Signature |
| Printed Name | Printed Name |
| Title | Title |
| Date | Date |

Please list ConnectWise Account Manager

Please fill out this Signature page electronically by clicking on each field, or print out and fax to 888-739-6203