Attachment 2 – Data Pro Statement

Along with the ConnectWise Cloud Backup and SAAS Security Data Processing Addendum (DPA) and its Attachments this Data Pro Statement constitutes the DPA for the product or service(s) as provided by the company that has drawn up this Data Pro Statement for Customers located in the EU/EEA, UK and Switzerland and those countries as listed under the section Local Provisions Asia-Pacific & South Africa.

GENERAL INFORMATION

1. This Data Pro Statement was drawn up by the following data processor:

ConnectWise S-K B.V. ("ConnectWise Nederland")
James Wattstraat 100
1097 DM Amsterdam
The Netherlands

If you have any queries about this Data Pro Statement or data protection in general, please contact:

ConnectWise Nederland
c/o Data Protection Officer
James Wattstraat 100
1097 DM Amsterdam
The Netherlands
privacy@connectwise.com

2. The Data Pro Statement shall enter into force on 5th of November 2020. ConnectWise Nederland, the data processor, regularly revises its security measures described in this Data Pro Statement to ensure that it is always fully prepared and up to date regarding data protection. If this document is updated, ConnectWise shall notify you of the revised versions through its regular channels

3. This Data Pro Statement applies to the following products and services provided by data processor:

- ConnectWise Cloud Backup
- ConnectWise SAAS Security.

4. Description of the services

4.1 ConnectWise Cloud Backup

ConnectWise Cloud Backup allows customers to protect their data from ransomware and other malicious and indeliberate events which lead to data loss or data corruption.

Further product information is available here:
https://www.connectwise.com/platform/security-management/cloud-backup

4.3 ConnectWise SAAS Security

ConnectWise SAAS Security allows for seamless management of services across a customer SaaS, and even hybrid environments. Through automation customers can improve their help desk performance and strengthen security and data protection.

Further product information is available here:
https://www.connectwise.com/platform/security-management/saas-security

5. Intended use of the services

The Cloud Backup and SAAS Security services are designed and built to process the types of data as described in **Attachment 3** – Scope of Processing.

When the Cloud Backup and SAAS Security services were designed the possibility that these would be used to process special categories of personal data or data regarding criminal convictions and offences or personal numbers issued by the government was not taken into account for these services.

Customer needs to determine whether or not to use the Cloud Backup & SAAS Security services to process such data.

6. Privacy by design/privacy by default.

Customer, as the data controller, remains ultimately responsible for privacy by design and default. The data processor supports Customer in this responsibility with the technical and organizational measures for its services as described in **Attachment 4** – Technical & Organizational Security Measures.

7. Standard Clauses for Data Processing

Data processor does NOT use the NLDigital Standard Clauses for Data Processing. Data processor instead provides the ConnectWise Cloud Backup and SAAS Security Data Processing Addendum into which this Data Pro Statement is wholly integrated.

8. Processing of personal data outside of the EU/EEA.

Data Processor processes personal data partially outside the EU/EEA. Data processor has ensured in the following way that the personal data shall be protected to an appropriate standard:

- The country in which the Subprocessor is located is subject to an adequacy decision by the European Commission;
- Data processor has entered into Standard Contractual Clauses Module 3 (processor-to-processor) with the relevant Subprocessor.

As part of its commitment to the adherence to the GDPR, the UK GDPR and Swiss Data Protection Law, the Data Protection Officer of ConnectWise Nederland can, on request, provide additional detail on the additional safeguards it has put in place to complement these Standard Contractual Clauses Module 3 (processor-to-processor) with the relevant Subprocessor.

9. Data processor use of subprocessors:
All current Subprocessors are listed in **Attachment 3** – Scope of Processing section 3.

10. Data processor support of clients:
Data processor shall support Customer with requests it receives from data subjects as described in the DPA section 4.1

11. Data processor support for Data Protection Impact Assessments (DPIA)
Data processor shall support Customer with Data Protection Impact Assessments (DPIA) in the manner as described in the DPA section 4.2

12. Data processor support of data deletion:
Once the Agreement with a Customer has been terminated data processor shall delete personal data it processes such that the personal data shall no longer be able to be used and shall be rendered inaccessible as further described in the DPA section 3.

13. Return of personal data
Once the Agreement with a Customer has been terminated, if desired by a customer, data processor can return personal data it processes, as further described in the DPA section 3.

SECURITY POLICY

14. Implemented security measures

Data processor has implemented the security measures to protect its services as described in **Attachment 4** – Technical & Organization Security Measures.

15. Information Security Management System (ISMS)

Data processor conforms to the principles of the following Information Security Management System (ISMS):

- ISO 27001
- ISO 27701
- Cloud Security Alliance CAIQ V4

16. Labels and certificates

Data processor has obtained the following labels and certificates:

- Data Pro Verification
- ISO 27001:2013
- ISO 27701:2019
- Cloud Security Alliance Trusted Cloud Provider
- Cloud Security Alliance STAR

17. Data Breach Protocol

In the event something does go wrong, the data processor shall follow its Personal Data Breach Notice and Assistance protocol as described in the DPA section 4.3. If Customer is based in Australia, section 9 shall apply in addition to section 4.3.

***

Attachment 3 – Scope of Processing

1. SUBJECT-MATTER AND DURATION OF PROCESSING

ConnectWise Processes Personal Data for the subject matter specified under the Agreement and until the Agreement terminates or expires, unless otherwise agreed upon by the parties in writing. In particular, the subject matter is determined by the Services to which Customer subscribes.

2. NATURE AND PURPOSE OF PROCESSING

The nature of the Processing is cloud migration, cloud storage and cloud management. A more detailed description of the nature and purposes of the Services can be made available upon request in accordance with applicable law and the Agreement.

3. SUBCONTRACTOR'S PROCESSING OF PERSONAL DATA

In the table below is a summary of the categories of data, and storage locations for ConnectWise S-K B.V.'s current Subprocessors and their respective Processing activities.

Subprocessor	**Scope and purpose of processing**	**Categories of Personal Data**	**Processing (and storage) locations (e.g. country/state)**
ConnectWise S-K, LLC (200 W. Thomas Street, Seattle, WA98119 USA)	Provision of (technical) support	Personal data as described under Section 4 below	United States

The duration of processing is the term of the distribution and services agreement between ConnectWise S-K B.V. and ConnectWise S-K, LLC. The subject matter and nature of the processing is access to Personal Data for support services under the distribution and services agreement between ConnectWise S-K B.V. and ConnectWise S-K, LLC.

4. TYPES OF PERSONAL DATA

Categories of Personal Data to be processed under this DPA includes the following categories of data: names, e-mail addresses and other contact details, as well as any personal data that may be included in the content of e-mails. More specifically:

	Cloud Backup	SAAS Security
Administrator accounts [1]		
Username	√	
Password	√ [2]	
User accounts		
Username	√	√
Password	√ [3]	
Email address	√	√
First name	√	√
Last name	√	√
Job title	√	√
Business phone	√	√
Employee number		√
Department		√

Location		√
DNS Registrar credentials		
Username	√ [4]	
Password	√ [4]	

[1] For ConnectWise Cloud Backup & ConnectWise SAAS Security multi-factor authentication is used, no usernames or passwords are stored and access to the underlying SAAS service is granted based on an authentication token.

[2] ConnectWise recommends using a temporary administrator account for migrations which should be disabled on the completion of the migration when using the Migration feature of ConnectWise Cloud Backup.

[3] May be applied to obtain access to the source for a migration, when using the Migration feature of ConnectWise Cloud Backup, if this access cannot be obtained through the administrator account. ConnectWise in all cases recommends resetting the password on the destination environment on completion of a migration and provides automation to support this.

[4] Only applicable when using the Migration feature of ConnectWise Cloud Backup. ConnectWise recommends using a temporary administrator account for migrations which should be disabled on the completion of the migration.

5. CATEGORIES OF DATA SUBJECTS

The categories of Data Subjects are Customer employees, contractors, business partners and other individuals whose Personal Data is included in the Customer Data. If Customer is based in South Africa, juristic persons are also included.

6. THE FREQUENCY OF THE PROCESSING (E.G. WHETHER THE DATA IS PROCESSED ON A ONE-OFF OR CONTINUOUS BASIS).

The frequency of the Processing is on a continuous basis.

***

Attachment 4 – Technical & Organizational Security Measures

ConnectWise has various technical and organizational security measures in a place to secure, maintain and safeguard Personal Data. The security commitments in this DPA are the sole responsibility of ConnectWise with respect to the security of that data.

Domain	**Practices**
Organization of Information Security	**Security Ownership**. ConnectWise has appointed a data protection team responsible for coordinating, monitoring and regularly auditing all rules and procedures. **Security Roles and Responsibilities**. ConnectWise staff with access to Personal Data are subject to confidentiality obligations. **Risk Management Program**. ConnectWise performed a risk assessment before processing Personal Data through their Services and retains related documents pursuant to applicable retention requirements.
Asset Management	**Asset Inventory**. ConnectWise maintains an inventory of all media on which Personal Data is stored. Access to the inventories of such media is restricted to ConnectWise employees authorized to have such access. **Asset Handling** ConnectWise classifies Personal Data to help identify it and to allow for access to it to be appropriately restricted.

ConnectWise imposes restrictions on printing Personal Data and has procedures for disposing of printed materials that contain Customer Data.

ConnectWise staff must obtain ConnectWise authorization prior to storing Personal Data on portable devices, remotely accessing Customer Data, or processing Personal Data outside ConnectWise's facilities.

Human Resources Security

Security Training.

ConnectWise informs its staff about relevant security procedures and their respective roles. ConnectWise also informs its staff of possible consequences of breaching the security rules and procedures. ConnectWise will only use anonymous data in training.

Physical and Environmental Security

Physical Access to Facilities.

ConnectWise limits access to facilities where information systems that process Personal Data are located to identified authorized staff members.

Physical Access to Components.

Where applicable, ConnectWise maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Personal Data they contain.

Protection from Disruptions.

ConnectWise applies a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

Component Disposal.

ConnectWise uses industry standard processes to delete Personal Data when it is no longer needed.

Communications and Operations Management

Operational Policy.

ConnectWise maintains security documents describing its security measures and the relevant procedures and responsibilities of its staff who have access to Customer Data.

Data Recovery Procedures

On an ongoing basis ConnectWise maintains copies of Personal Data from which Personal Data can be recovered.

ConnectWise stores copies of Personal Data and data recovery procedures in a different container from where the processing the Personal Data is performed.

ConnectWise has procedures in place governing access to copies of Customer Data.

ConnectWise reviews its data recovery procedures at least annually.

ConnectWise logs data restoration efforts, including the person responsible, the description of the restored data and where applicable and the person responsible.

Malicious Software.

ConnectWise has anti-malware controls to help avoid malicious software, including malicious software originating from public networks, gaining unauthorized access to Customer Data.

Data Beyond Boundaries

ConnectWise encrypts, or enables Customer to encrypt, Personal Data that is transmitted over public networks.

ConnectWise restricts access to Personal Data in media leaving its facilities.

Event Logging.

ConnectWise logs the access and use of information systems containing Customer Data, registering the user ID, time, authorization granted or denied, and relevant activity of its staff members.

Access Control

Access Policy.

ConnectWise maintains a record of security privileges of staff members having access to Customer Data.

Access Authorization

ConnectWise maintains and updates a record of staff authorized to access ConnectWise systems that contain Customer Data.

ConnectWise deactivates authentication credentials that are not used for a period not exceeding six months.

ConnectWise identifies those staff members who may grant, alter or cancel authorized access to data and resources.

ConnectWise ensures that where more than one individual has access to systems containing Customer Data, the staff members have separate user identifiers and log-ins.

Least Privilege

ConnectWise staff members are only permitted to have access to Personal Data when required.

ConnectWise restricts access to Personal Data to only those staff members who require such access to perform their job function.

Integrity and Confidentiality

ConnectWise instructs ConnectWise staff to disable administrative sessions when leaving premises ConnectWise controls or when computers are otherwise left unattended.

ConnectWise stores passwords in a way that makes them unintelligible while they are in force.

Authentication

ConnectWise uses industry standard practices to identify and authenticate users who attempt to access information systems.

Where authentication mechanisms are solely based on passwords, ConnectWise requires that the passwords are renewed regularly.

Where authentication mechanisms are solely based on passwords, ConnectWise requires the password to be at least eight characters long.

ConnectWise ensures that de-activated or expired identifiers are not granted to other staff members.

ConnectWise monitors repeated attempts to gain access to the information system using an invalid password.

ConnectWise maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

ConnectWise uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

Network Design.

ConnectWise has controls to avoid staff members assuming access rights they have not been assigned to gain access to Personal Data they are not authorized to access.

Information Security Incident Management

Incident Response Process

ConnectWise maintains a record of security incidents with a description of the incident, the time period, its consequences, the name of the reporter, and to whom the incident was reported, and the procedure for recovering from an incident.

For each incident pertaining to Customer Data, notification by ConnectWise will be made without undue delay and, in any event, within 72 hours.

ConnectWise tracks disclosures of Customer Data, including what data has been disclosed, to whom, and at what time.

Service Monitoring.

ConnectWise security staff verify logs at least every six months to propose remediation efforts if necessary.

Business Continuity Management

ConnectWise maintains emergency and contingency plans for the facilities in which ConnectWise information systems that process Personal Data are located.

ConnectWise’s redundant storage and its procedures for recovering data are designed to attempt to reconstruct Personal Data in its original or last-replicated state from before the time it was lost or destroyed.

***