

SCHEDULE 2

Data Pro Statement

Along with the Data Processing Addendum (DPA) and its Schedules, this Data Pro Statement forms part of the DPA for the Services as provided by the company that has drawn up this Data Pro Statement for Licensees located in the EEA, UK and Switzerland.

GENERAL INFORMATION

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

ConnectWise B.V.
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 the ConnectWise B.V. Data Protection Officer at the aforementioned address or through email via: privacy@connectwise.com.

2. The Data Pro Statement shall enter into force on 29th of June 2026. ConnectWise B.V. 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, we shall notify Licensee of the revised versions through our regular channels.

3. This Data Pro Statement applies to ConnectWise Platform and the following Services provided therein by data processor:

- ConnectWise Data Protection
- ConnectWise SaaS Security

4. Description of the Services:

4.1.

ConnectWise Data Protection 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>

4.2

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 Services are designed and built to process the types of data as described in Annex I of the DPA. When the 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. Licensee needs to determine whether or not to use the Services to process such data.

6. Privacy by design/privacy by default.

Licensee, as the data controller, remains ultimately responsible for privacy by design and default. Data processor supports Licensee in this responsibility with the technical and organizational measures for its services as described in Annex II of the DPA.

7. Standard Clauses for Data Processing

Data processor does not use the NLDigital Standard Clauses for Data Processing. Data processor instead provides the ConnectWise DPA into which this Data Pro Statement is wholly integrated.

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

Data Processor processes Licensee Personal Data partially outside the EU/EEA. Data processor has ensured in the following way that the Licensee 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; or
- 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, ConnectWise B.V. 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(s).

9. Data processor use of subprocessors:

All current Subprocessors of ConnectWise B.V., as the data processor, are listed in Annex III of the DPA.

10. Data processor support of Licensees:

Data processor shall support Licensee in the following way when they receive requests from data subjects: As described in the DPA section 3.1.

11. Data processor support for Data Protection Impact Assessments (DPIA)

Data processor shall support Licensee with Data Protection Impact Assessments (DPIA) in the manner as described in the DPA section 6.3.

12. Data processor support of data deletion:

Once the Agreement with a Licensee has been terminated data processor shall delete Licensee Personal Data it processes such that the Licensee Personal Data shall no longer be able to be used and shall be rendered inaccessible as further described in the DPA section 8.0.

13. Return of personal data:

Once the Agreement with a Licensee has been terminated, if desired by a Licensee, data processor can return Licensee Personal Data it processes, as further described in the DPA section 8.

SECURITY POLICY

14. Implemented security measures

Data processor has implemented the security measures to protect its services as described in Annex II.

15. Information Security Management System

Data processor conforms to the principles of an integrated Information Security & Privacy Management System (ISPMS) based on the following standards:

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

16. Labels and certificates

Data processor has obtained the following labels and certificates:

- Data Pro Verified
- ISO 27001:2022
- ISO 27701:2019
- Cloud Security Alliance Trusted Cloud Provider –
- STAR Level 2

17. Data Breach Protocol

In the event something does go wrong, data processor shall follow its Incident Management and Notification protocol as described in the DPA section 7.