DATA PROCESSING ADDENDUM (DPA)

Version: 1.0

Last Updated: 25 January 2026

This Data Processing Addendum ("DPA") forms part of the Terms of Service ("Agreement") between **Cyber Security Stack LTD** ("Processor") and the entity agreeing to these terms ("Controller").

1. Definitions

- **"Data Protection Laws"** means the UK GDPR, the Data Protection Act 2018, and (where applicable) the EU GDPR.
- **"Customer Data"** means the personal data processed by the Processor on behalf of the Controller via the Endpoint Agents and Services.
- **"Personal Data," "Processing," "Controller," "Processor,"** and **"Data Subject"** shall have the meanings given to them in the Data Protection Laws.

2. Roles and Scope

- **Roles:** The parties acknowledge that for the purposes of the Services, the Customer is the **Controller** and Cyber Security Stack LTD is the **Processor**.
- **Duration:** This DPA remains in effect as long as the Processor processes Customer Data under the Agreement.
- **Nature of Processing:** The Processor provides endpoint security, threat detection, and incident response. Processing includes the collection of system telemetry, logs, and metadata from covered devices.

3. Processor Obligations

The Processor agrees to:

- **Instructions:** Process Customer Data only on the documented instructions of the Controller, including with regard to transfers of personal data to a third country.
- **Confidentiality:** Ensure that persons authorised to process the personal data have committed themselves to confidentiality.

- **Security:** Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including encryption and access controls.
- **Subprocessors:** The Controller provides a general authorisation for the Processor to engage subprocessors (e.g., cloud hosting providers). The Processor shall remain liable for the performance of the subprocessor's obligations.
- **Data Subject Rights:** Assist the Controller, insofar as this is possible, in fulfilling the Controller's obligation to respond to requests from Data Subjects exercising their rights.
- **Personal Data Breach:** Notify the Controller without undue delay after becoming aware of a personal data breach.

4. International Transfers

The Processor shall ensure that any transfer of Customer Data outside the UK or EEA is conducted in accordance with Data Protection Laws (e.g., using **Standard Contractual Clauses** or the **UK International Data Transfer Agreement**).

5. Audit Rights

The Processor shall make available to the Controller all information necessary to demonstrate compliance with Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

6. Return or Deletion of Data

Upon termination of the Services, the Processor shall, at the choice of the Controller, delete or return all Customer Data, unless applicable law requires storage of the personal data.