

Data Processing Agreement

Angstep Ltd — NetMon Platform
Version 1.1, August 2026

This Data Processing Agreement (“**DPA**”) forms part of the agreement between Angstep Ltd and the Customer for use of the NetMon platform (the “**Agreement**”). It records the parties’ obligations under Article 28 of the UK GDPR where Angstep Ltd processes personal data on the Customer’s behalf.

This DPA must be completed and signed before the Customer uses the Platform to monitor any network belonging to a third party. Where the Customer monitors only its own network, and no personal data of any other organisation is processed, this DPA is not required — but signing it does no harm.

Party	Detail
Processor	Angstep Ltd, registered in England and Wales, company number 17358935. Registered office: Applegarth, Groes Lwyd, Abergele, Conwy, LL22 7SU. ICO registration ZC183626.
Controller	The Customer, as identified in the signature block at the end of this DPA.
Effective date	The date of the Customer’s signature below, or the date the Customer first uses the Platform to process third-party personal data, whichever is earlier.
Governing law	England and Wales

1. Definitions

Terms not defined here have the meaning given in the UK GDPR.

Term	Meaning
Client Data	Personal data relating to the Customer’s own clients and their network users, processed through the Platform on the Customer’s instructions.
Data Protection Laws	The UK GDPR, the Data Protection Act 2018, and the Privacy and Electronic Communications Regulations 2003, each as amended.
Platform	The NetMon network monitoring, vulnerability scanning and remote access service operated by Angstep Ltd.
Agent	The software component installed on a monitored network which discovers devices and reports to the Platform.
Sub-processor	A third party engaged by Angstep Ltd to process Client Data. The current list is at Annex C.

2. Roles of the Parties

2.1 In respect of **Client Data**, the Customer is the controller and Angstep Ltd is the processor. The Customer determines which networks are monitored, which devices are scanned, and for what purpose.

2.2 In respect of the Customer’s **own account data** — the names and email addresses of the Customer’s own users, billing details, and product usage statistics — Angstep Ltd is the controller. That processing is described in the Angstep Privacy Policy and is not governed by this DPA.

2.3 The Customer confirms it has a lawful basis for processing Client Data through the Platform, and has provided any notices and obtained any consents required of it as controller.

3. Scope and Instructions

3.1 Angstep Ltd will process Client Data only on the Customer's documented instructions. The Agreement, this DPA, and the Customer's use of the Platform together constitute those instructions.

3.2 Angstep Ltd will not process Client Data for its own purposes, will not sell it, and will not use it to build or improve products or datasets.

3.3 If Angstep Ltd believes an instruction infringes Data Protection Laws it will inform the Customer without undue delay, and may suspend the relevant processing until the instruction is amended or confirmed.

3.4 Where Angstep Ltd is required by law to process Client Data otherwise than on instruction, it will inform the Customer before doing so unless prohibited from doing so by that law.

4. Confidentiality and Security

4.1 Angstep Ltd will ensure that personnel authorised to process Client Data are bound by confidentiality obligations.

4.2 Angstep Ltd will implement and maintain the technical and organisational measures set out in **Annex B**, appropriate to the risk under Article 32 UK GDPR.

4.3 Angstep Ltd may update those measures provided the change does not materially reduce the level of protection.

5. Sub-processors

5.1 The Customer gives general authorisation for Angstep Ltd to engage the sub-processors listed in **Annex C**.

5.2 Angstep Ltd will give the Customer at least **30 days' notice** by email before adding or replacing a sub-processor. The Customer may object on reasonable data-protection grounds within that period. If the parties cannot resolve the objection, the Customer may terminate the affected part of the Agreement without penalty, with a pro-rata refund of prepaid fees.

5.3 Angstep Ltd will impose data protection obligations on each sub-processor no less protective than those in this DPA, and remains fully liable to the Customer for each sub-processor's performance.

6. Data Subject Rights

6.1 The Platform allows the Customer to access, correct, export and delete Client Data directly, so the Customer can respond to most data subject requests without assistance.

6.2 Where the Customer cannot do so through the Platform, Angstep Ltd will provide reasonable assistance, taking into account the nature of the processing.

6.3 If a data subject contacts Angstep Ltd directly about Client Data, Angstep Ltd will not respond substantively but will refer them to the Customer and inform the Customer promptly.

7. Personal Data Breach

7.1 Angstep Ltd will notify the Customer **without undue delay and in any event within 48 hours** of becoming aware of a personal data breach affecting Client Data.

7.2 The notification will describe the nature of the breach, the categories and approximate number of data subjects and records affected, the likely consequences, the measures taken or proposed, and a contact point for further information. Where the full picture is not immediately available, information will be provided in phases without undue further delay.

7.3 Angstep Ltd will assist the Customer in meeting its own obligations under Articles 33 and 34 UK GDPR.

7.4 Unsuccessful attempts that do not compromise Client Data — failed logins, port scans, blocked intrusion attempts — are not personal data breaches and are not notifiable under this clause.

8. Data Protection Impact Assessments

Taking into account the nature of processing and the information available to it, Angstep Ltd will provide reasonable assistance with any data protection impact assessment or prior consultation with the ICO that the Customer is required to carry out in relation to the Platform.

9. Deletion and Return

9.1 The Customer may export or delete Client Data through the Platform at any time during the term.

9.2 On termination, Angstep Ltd will delete or anonymise all Client Data **within 30 days**, except where retention is required by law. The 30-day window exists to allow the Customer to export data after closing the account.

9.3 Angstep Ltd will certify deletion in writing on request.

9.4 Backups containing Client Data are securely isolated from further processing and are deleted in accordance with the ordinary backup rotation, within 90 days.

10. Demonstrating Compliance

10.1 Angstep Ltd will make available the information reasonably necessary to demonstrate compliance with this DPA.

10.2 The Customer may audit compliance no more than **once per calendar year**, on 30 days' written notice, unless there are reasonable grounds to suspect non-compliance or an audit is required by a supervisory authority. Audits must be conducted during business hours, must not unreasonably disrupt operations, and are subject to confidentiality.

10.3 Angstep Ltd may satisfy an audit request by providing written responses to reasonable questions, or documentation of its security measures, where this reasonably addresses the Customer's concerns.

11. International Transfers

11.1 Client Data is stored and processed within the **European Union** (Falkenstein, Germany). The EU benefits from UK adequacy regulations, so no additional transfer mechanism is required.

11.2 The limited transfers to sub-processors outside the UK and EEA identified in Annex C are covered by Standard Contractual Clauses as modified by the UK International Data Transfer Addendum.

11.3 Angstep Ltd will not transfer Client Data to any other country without an appropriate transfer mechanism under Chapter V UK GDPR.

12. Liability and Term

12.1 Liability under this DPA is subject to the limitations and exclusions in the Agreement, save that nothing limits either party's liability to a data subject under Data Protection Laws.

12.2 This DPA takes effect on the effective date above and continues for as long as Angstep Ltd processes Client Data.

12.3 Where this DPA conflicts with the Agreement, this DPA prevails in respect of the processing of Client Data.

12.4 Angstep Ltd may update this DPA to reflect changes in law or in the Platform, on 30 days' notice. If a change materially reduces the Customer's protections, the Customer may terminate without penalty.

Annex A — Details of Processing

Subject matter and duration

Provision of the NetMon network monitoring, vulnerability scanning and remote access service. Processing continues for the term of the Agreement, plus up to 30 days thereafter (clause 9.2).

Nature and purpose of processing

- Automated discovery of devices on networks the Customer chooses to monitor;
- Continuous availability monitoring, latency and packet-loss measurement;
- Vulnerability scanning against public CVE and CISA KEV data;
- Detection of devices not present in the established network baseline;
- Brokering remote desktop and shell sessions to devices, where the Customer's plan includes remote access;
- **Executing diagnostic scripts on devices at the Customer's instruction**, and returning their output. Scripts are written and reviewed by Angstep Ltd and supplied as part of the Platform — the Customer selects from a fixed library and cannot author, upload or modify scripts;
- Storage and display of the above to authorised users of the Customer's organisation.

Types of personal data

The data collected is primarily technical and about devices rather than people. It becomes personal data where a device is associated with an identifiable individual — for example a named personal laptop, or a home worker's network.

Category	Detail
Device identifiers	IP address, MAC address, hostname
Device characteristics	Device type, vendor, model, operating system, firmware version
Network exposure	Open ports, running services, detected vulnerabilities
Availability data	Online/offline status, latency, packet loss, first and last seen timestamps
Remote access metadata	Which device a session was opened to, by which of the Customer's users, and when
Script output	Whatever the selected script returns. Depending on the script this may include usernames, account names, process owners, logged-in users, event log entries and file paths. Output is stored so that the Customer can review what was run and what it returned.
Script execution record	Which script was run, on which device, by which of the Customer's users, when, with what parameters, and the exact version and checksum of the script that executed

Angstep Ltd does not record, view or log the content of remote access sessions. The Platform brokers the connection only.

No special category data under Article 9 UK GDPR, and no criminal offence data under Article 10, is intentionally processed. The Customer must not use the Platform to process such data.

Categories of data subjects

- Employees, contractors and other users of the Customer's clients' networks;
- Any individual whose device connects to a monitored network, including visitors and guests;
- The Customer's own personnel who use the Platform.

Annex B — Technical and Organisational Measures

B1. Access control and tenant isolation

- Authentication via Google OAuth 2.0; Angstep Ltd never receives or stores user passwords;
- Role-based access within each organisation (org admin, viewer);

- **Per-organisation isolation of remote access:** each customer organisation has its own MeshCentral device group and its own scoped account, restricted to that group alone. No shared administrative credential is used for customer access;
- Server-side enforcement of organisation scoping on all data endpoints, so a request cannot return another organisation's data;
- SSH key-only access to infrastructure servers; password authentication disabled.

B2. Encryption

- All data in transit protected by TLS 1.2 or higher;
- Database accessible only over a private internal network, not from the public internet;
- Credentials and API keys held as environment variables, never in source control.

B3. Logging and monitoring

- Security events logged with IP address, including authentication failures, cross-tenant access attempts and rate-limit breaches;
- Rate limiting on authentication and account-creation endpoints;
- Application logs retained and reviewable for incident investigation.

B4. Resilience and availability

- Managed database with automated backup;
- Automatic service restart on failure;
- Infrastructure provider maintaining redundant power, network and cooling.

B5. Development and change management

- Source control with reviewable history;
- Static analysis and dependency scanning;
- Non-root container execution;
- Staged deployment with the ability to roll back.

B6. Script execution controls

- **Curated library only.** Scripts are authored and reviewed by Angstep Ltd. Customers cannot write, upload or modify scripts, so the executable surface is a fixed set of reviewed code rather than arbitrary customer input;
- **Read-only scripts only** in the current release — the library performs diagnostics and does not modify the target system;
- Parameters are **declared, typed and validated** against an allowlist or pattern, server-side and again on the agent, and are passed to the script as environment variables rather than being built into a command line. Command injection through a parameter is therefore not possible;
- Each script's content is **checksummed**, and the agent refuses to execute a script whose content does not match the checksum recorded by the Platform;
- Execution requires an organisation administrator on a Pro or MSP plan; ordinary users cannot run scripts;
- Rate limits cap how many scripts an organisation may run, and a global control allows Angstep Ltd to suspend all script execution immediately;
- Scripts run under a time limit and their output is capped; a script exceeding either is terminated;
- The agent does not pass its own credentials into the script environment;
- Every execution and every refusal is recorded (see Annex A), and the record is retained for the Customer's own audit purposes.

B7. Data minimisation

- Only data necessary to deliver monitoring is collected;
- Remote session content is never captured;
- Payment card data never touches Angstep systems (handled by Stripe);
- Defined retention periods, with deletion on termination (clause 9).

Annex C — Authorised Sub-processors

Current as at the version date of this DPA. Changes are notified under clause 5.2.

Sub-processor	Purpose	Location	Transfer basis
Hetzner Online GmbH	Infrastructure hosting: application, database and remote access server	Falkenstein, Germany (EU)	EU — adequacy; no mechanism required
Railway (Railtown Inc.)	Deployment and runtime platform; infrastructure hosted on Hetzner	EU (Germany)	EU — adequacy
Google LLC	OAuth authentication only. Receives the user's email address; receives no Client Data.	USA	SCCs / UK IDTA
Mailjet (Sinch)	Transactional and operational email delivery, including alerts about the Customer's monitored devices	France (EU)	EU — adequacy
Stripe, Inc.	Payment and subscription processing. Receives the Customer's billing details only; receives no Client Data.	USA	SCCs / UK IDTA

HubSpot, Inc. is not a sub-processor under this DPA. Angstep Ltd uses HubSpot as its own customer relationship system for the Customer's account and contact details, acting as controller for that purpose under its Privacy Policy. **No Client Data is sent to HubSpot.**

Signatures

By signing below, the parties agree to be bound by this DPA. The Customer confirms it is authorised to enter into this DPA on behalf of the legal entity named.

For Angstep Ltd (Processor)	For the Customer (Controller)
Signature: _____	Signature: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____
Angstep Ltd Company number 17358935 Applegarth, Groes Lwyd, Abergele, Conwy, LL22 7SU supportteam@angstep.co.uk	Company name: _____ Company number: _____ Registered address: _____ _____ Data protection contact email: _____

Return one signed copy to **supportteam@angstep.co.uk**. Angstep Ltd will return a countersigned copy for your records.