Angstep Ltd

NetMon Privacy Policy
Version 1.1 — August 2026

Field	Detail
Document status	Published
Version	1.1 — August 2026 (supersedes v1.0, July 2026)
Data controller	Angstep Ltd, registered in England and Wales, company number 17358935
Registered office	Applegarth, Groes Lwyd, Abergele, Conwy, LL22 7SU
ICO registration	ZC183626
Governing law	England and Wales
Regulator	Information Commissioner's Office (ICO), Wycliffe House, Water Lane, Wilmslow, SK9 5AF
Scope	This document applies to the NetMon product and the angstep.co.uk website

1. Who We Are

Angstep Ltd (“we”, “us”, “our”) is a company registered in England and Wales, company number 17358935, with its registered office at Applegarth, Groes Lwyd, Abergele, Conwy, LL22 7SU.

We operate NetMon, a multi-tenant network monitoring and remote access platform (“the Platform”) designed for Managed Service Providers (MSPs) and IT administrators. The Platform allows users to monitor, secure and remotely access networked devices on behalf of themselves or their clients.

We are the data controller in respect of personal data collected through the Platform and through the website at www.angstep.co.uk (“the Site”).

Contact for data protection	Detail
Email	supportteam@angstep.co.uk
Post	Applegarth, Groes Lwyd, Abergele, Conwy, LL22 7SU — marked “Data Protection”
ICO registration	ZC183626

2. Scope of This Policy

This Privacy Policy applies to:

- Personal data collected when you visit www.angstep.co.uk;
- Personal data collected when you create a NetMon account and use the Platform;
- Personal data processed through the Platform in the course of the monitoring and remote access services.

This policy does not apply to the personal data of the end-users or clients of our MSP customers. MSP customers who process client data through the Platform act as data controllers in their own right and are required to enter into a Data Processing Agreement (DPA) with us before doing so. See Section 9.

3. Personal Data We Collect

3.1 Account and Identity Data

When you create a NetMon account using Google OAuth sign-in, we receive the following from Google:

Data item	Source	Retained?
Email address	Google OAuth	Yes — stored in users table
Google display name	Google OAuth profile (first login only)	Yes — used to pre-fill organisation name
Google user ID	Google OAuth (internal reference)	Yes — stored as google_id

We do not receive or store your Google password. Authentication is handled entirely by Google.

3.2 Usage and Security Data

Data item	When collected	Purpose
IP address	On login, failed login, authentication failure, and certain API events	Security monitoring and abuse prevention
Session identifiers	On each authenticated session	Session management and authentication
Last login timestamp	On each successful login	Account security and audit
Consent records	When you accept our terms, or give or withdraw marketing consent	Evidence of what was agreed, when, from which IP address and browser

3.3 Network and Device Data

Our monitoring agent, once deployed on a customer network, collects technical data about networked devices. This data is primarily about devices rather than individuals; however, it may become personal data where a device is associated with an identifiable individual (for example, a named personal laptop on a home network).

Device data collected includes:

- IP address and MAC address of each discovered device;
- Hostname, device type, vendor, and model;
- Operating system and firmware version (where detectable);
- Open network ports and running services;
- Online/offline status, latency, and packet loss history;
- First seen and last seen timestamps;
- Gateway IP and network site assignment.

This data is associated with the customer’s organisation in the Platform and is not shared with other customers.

3.4 Script Execution Data

Where a customer’s plan includes it, an administrator may run a diagnostic script from our curated library on a device they monitor. Scripts are written and reviewed by us and supplied as part of the Platform; customers cannot author, upload or modify them. The current library is read-only — it reports on the state of a device and does not change it.

Two kinds of data result:

Data item	Detail
Execution record	Which script was run, on which device, by which user, when, with what parameters, and the exact version and checksum of the script that executed
Script output	Whatever the script returns. Depending on the script this may include usernames, account names, process owners, logged-in users, event log entries and file paths — so it may contain personal data

Output is stored so that the person who ran the script, and their colleagues, can see what it returned and demonstrate afterwards what was done. Where the device belongs to an MSP customer's client, that MSP is the controller for this data and we process it on their instructions under the Data Processing Agreement (Section 9).

3.5 Product Usage and Account Analysis

We derive statistics about how each customer organisation uses NetMon. These are calculated from data we already hold and are about the **organisation**, not about individuals:

- Number of devices and sites monitored;
- Which product features have been used (for example, whether a vulnerability scan has been run);
- Days on which the monitoring agent reported in;
- Whether the organisation has reached a limit of its current plan, or attempted to use a feature not included in it.

We use this to understand how organisations use the product and to identify customers who may benefit from a different plan. It is not used to profile individuals, and it does not produce decisions with legal or similarly significant effects. See Section 4.2.

3.6 Data We Do Not Collect

- Payment card numbers or bank account details (handled directly by Stripe — see Section 7);
- Special category data (health, biometric, racial or ethnic origin, and similar);
- The content of remote access sessions — we broker the connection; we do not record, view, or log session content;
- Data from the angstep.co.uk website beyond standard web server access logs, which do not contain identifiable personal data.

4. Legal Basis for Processing

We process personal data under the following legal bases as defined in Article 6 UK GDPR:

Processing activity	Legal basis	Detail
Creating and managing your account	Art. 6(1)(b) — Contract	Necessary to perform the contract for services you have signed up for
Providing the monitoring and remote access service	Art. 6(1)(b) — Contract	Core service delivery
Sending transactional emails (account, billing)	Art. 6(1)(b) — Contract	Necessary to manage your subscription

Processing activity	Legal basis	Detail
Sending operational alerts (device offline, unrecognised device detected)	Art. 6(1)(b) — Contract	Core service delivery — this is the monitoring service you signed up for, not marketing. Each user may switch these off in their Account settings.
Running diagnostic scripts requested by an administrator, and storing their output	Art. 6(1)(b) — Contract	A feature of the Pro and MSP plans, performed only when a customer administrator explicitly requests it. See Section 3.4
Security event logging (IP addresses, failed auth attempts)	Art. 6(1)(f) — Legitimate interests	Protecting the Platform and other users from unauthorised access, fraud, and abuse. See Section 4.1
Analysing organisation product usage for account management	Art. 6(1)(f) — Legitimate interests	Business-to-business account management: understanding which customers may benefit from a different plan. See Section 4.2
Sending marketing emails	Art. 6(1)(a) — Consent	Optional, separately obtained, and withdrawable at any time. See Section 4.3
Maintaining financial records	Art. 6(1)(c) — Legal obligation	UK law requires retention of financial records for 7 years
Responding to data subject requests	Art. 6(1)(c) — Legal obligation	UK GDPR Articles 12–23 rights obligations

4.1 Legitimate Interests Assessment — Security Logging

- **Purpose:** detecting, investigating, and preventing unauthorised access, credential stuffing, and abuse of the remote access capability.
- **Necessity:** IP address logging is the minimum data required to identify and block malicious activity. The Platform provides access to real device infrastructure; the security interest is material.
- **Balance:** the data subjects affected are users of the Platform who have a reasonable expectation that authentication attempts will be logged for security purposes. The data is not used for profiling, marketing, or shared with third parties. Individuals are not identified from IP addresses alone.
- **Conclusion:** the legitimate interest is not overridden by the interests or rights of the data subjects.

4.2 Legitimate Interests Assessment — Product Usage Analysis

- **Purpose:** understanding how customer organisations use NetMon so that we can identify accounts approaching the limits of their plan and offer an appropriate one.
- **Necessity:** the statistics are derived from data already held to deliver the service. No additional personal data is collected for this purpose, and the analysis is performed at organisation level rather than individual level.
- **Balance:** the subject matter is the behaviour of a business account, not of a person. Business customers reasonably expect a supplier to know how much of the product they are using. No individual is profiled, no automated decision with legal or similarly significant effect is made, and the output is not shared outside our own CRM.
- **Conclusion:** the legitimate interest is not overridden by the interests or rights of the data subjects. You may object to this processing at any time (Section 11).

4.3 Consent — Marketing Only

Marketing email is the only processing for which we rely on consent. That consent is:

- **Separate** — requested by its own unticked checkbox at sign-up, distinct from accepting our Terms of Service;
- **Optional** — refusing it has no effect whatsoever on your account, your service, or the price you pay;
- **Recorded** — we log what was agreed, when, from which IP address and browser, and every subsequent change;
- **Withdrawable at any time** — from the Account page in NetMon, with no need to contact us.

If you withdraw marketing consent, your contact record is **deleted from our CRM** at the next daily synchronisation. Withdrawal does not affect the lawfulness of processing carried out before it.

5. How We Use Your Personal Data

- Providing and managing your NetMon account and subscription;
- Authenticating your identity when you sign in;
- Operating the network monitoring, vulnerability scanning, and remote access features;
- Sending transactional communications (account confirmations, billing receipts);
- Sending operational alerts about your own network, such as a device going offline or an unrecognised device appearing;
- Detecting and investigating security incidents and abuse of the Platform;
- Understanding how customer organisations use the product, for account management;
- Sending marketing email, where and only where you have consented;
- Complying with our legal obligations.

We do not and will not sell personal data to any third party. We do not display advertising within the Platform. We do not make automated decisions producing legal or similarly significant effects.

6. Data Retention

Data category	Retention period	Basis
Account data (email, name, settings)	Duration of active account + 30 days after cancellation	Contract — data export window
Device monitoring data	Duration of active subscription; deletable by customer at any time	Contract — service provision
Security event logs (IP addresses)	90 days rolling	Legitimate interests — security investigation window
Script execution records and output	12 months from execution	Contract — the customer's own audit and troubleshooting record
Product usage statistics	Duration of active account + 30 days	Legitimate interests — account management
Consent records (terms and marketing)	Lifetime of account + 7 years after termination	Legal obligation — evidence of consent and of contract acceptance
Financial / billing records	7 years from date of transaction	Legal obligation — Companies Act 2006 / HMRC
Session cookies	7 days from issuance, or until logout	Contract — session authentication

Consent records are deliberately retained after account closure. If you later ask us to demonstrate what you agreed to and when, we must be able to show it — and if we deleted the record we could not.

On account cancellation we will delete or anonymise all personal data within 30 days of the closure date, except where retention is required by law or where a data subject has exercised a right requiring us to retain data.

7. Data Sharing and Third-Party Processors

We do not sell, rent, or trade personal data. We share data only with the processors listed below, who act on our instructions under Article 28 contracts:

Processor	Role	Data shared
Google LLC	OAuth authentication provider	Email address, Google display name, Google user ID
Hetzner Online GmbH	Infrastructure hosting (application, database and MeshCentral VPS) — Falkenstein, Germany	All Platform data
Railway (Railtown Inc.)	Platform-as-a-Service deployment layer — infrastructure hosted on Hetzner Falkenstein, Germany	Application logs and environment
Stripe, Inc.	Payment processing and subscription management	Billing contact details, subscription status. No card data passes through Angstep systems.
HubSpot, Inc.	Customer relationship management (EU-hosted portal)	**For all organisations:** company name, plan, device and site counts, product usage statistics, and whether a plan limit has been reached — business information, processed under legitimate interests. **Only where marketing consent has been given:** the account holder's name and email address. Where consent is refused or withdrawn, no contact record is created, and any existing record is deleted.
Mailjet (Sinch)	Transactional and operational email delivery	Recipient email address and message content (account, billing and network alert emails)

We do not share personal data with any other third parties except where required by law or legal process, in which case we will notify you where permitted to do so.

8. International Data Transfers

All primary personal data storage and processing takes place within the European Union (Hetzner, Falkenstein, Germany). The EU is deemed adequate under UK GDPR, so no additional transfer mechanism is required for that processing.

The following transfers to countries outside the UK and EU/EEA may occur:

Recipient	Country	Transfer mechanism
Google LLC (OAuth)	USA	Google Workspace Data Processing Terms including Standard Contractual Clauses, approved under the UK International Data Transfer Agreement (IDTA)
Stripe, Inc. (payments)	USA	Stripe Data Processing Agreement including SCCs / UK IDTA

Recipient	Country	Transfer mechanism
HubSpot, Inc. (CRM)	USA (data hosted in EU)	HubSpot Data Processing Agreement including SCCs / UK IDTA. Our HubSpot portal is EU-hosted, so data is stored within the EU; HubSpot, Inc. is a US company and may access it for support purposes.
Mailjet (Sinch)	EU (France)	EU processing — no transfer mechanism required

These transfers are limited to the specific data items described in Section 7. The volume transferred is the minimum necessary for the services provided.

9. MSP Customers and Data Processing Agreements

MSP-tier customers use the Platform to monitor and manage networks on behalf of their own clients. In this context:

- The MSP customer is a data controller in respect of their clients' data;
- Angstep Ltd acts as a data processor on the MSP customer's instructions;
- The end clients' network users are data subjects whose data may be processed through the Platform.

UK GDPR Article 28 requires a written Data Processing Agreement between Angstep Ltd (as processor) and each MSP customer (as controller) before any such processing begins. We provide a standard DPA to MSP customers before their account is activated, specifying the subject matter, duration, nature and purpose of processing; the type of personal data and categories of data subjects; our obligations and rights as processor; sub-processor arrangements; and security, confidentiality and breach notification obligations.

MSP customers must not use the Platform to process client data until a signed DPA is in place.

10. Cookies and Similar Technologies

10.1 The Platform (portal.angstep.co.uk)

Cookie name	Purpose	Duration
netmon_session	Authenticates your session after sign-in via Google OAuth. Without this cookie the Platform cannot function.	7 days from issuance, or until you sign out

This cookie is strictly necessary for the operation of the service. It does not track you across other websites, and we do not use it for profiling or advertising. No consent banner is required for strictly necessary cookies under the Privacy and Electronic Communications Regulations (PECR).

We do not use analytics cookies, advertising cookies, or any third-party tracking technology in the Platform.

10.2 The Marketing Site (www.angstep.co.uk)

The angstep.co.uk website does not set any cookies. No consent banner is required.

11. Your Rights Under UK GDPR

We will respond to all valid requests within one calendar month (Article 12 UK GDPR):

Right	What it means	How to exercise
Access (Art. 15)	Request a copy of the personal data we hold about you and information about how we use it.	Email supportteam@angstep.co.uk with subject line “Subject Access Request”
Rectification (Art. 16)	Ask us to correct personal data that is inaccurate or incomplete.	Email supportteam@angstep.co.uk, or update it in your account settings
Erasure (Art. 17)	Ask us to delete your personal data. Applies except where retention is required by law.	Email supportteam@angstep.co.uk with subject line “Data Deletion Request”
Portability (Art. 20)	Receive your personal data in a structured, machine-readable format.	Email supportteam@angstep.co.uk with subject line “Data Portability Request”
Restriction (Art. 18)	Ask us to restrict processing of your data in certain circumstances.	Email supportteam@angstep.co.uk
Objection (Art. 21)	Object to processing based on legitimate interests — security logging or product usage analysis (Section 4).	Email supportteam@angstep.co.uk. We will stop unless we can demonstrate compelling legitimate grounds.
Withdraw consent (Art. 7(3))	Withdraw marketing consent at any time. This is the only processing for which we rely on consent.	Turn it off yourself on the **Account** page in NetMon — no need to contact us. Takes effect at the next daily sync.

11.1 Right to Complain

You have the right to lodge a complaint with the Information Commissioner’s Office if you believe we have not handled your personal data in accordance with UK GDPR.

Contact	Detail
ICO website	ico.org.uk
ICO helpline	0303 123 1113
ICO address	Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF
Our ICO registration	ZC183626

We would ask that you contact us at supportteam@angstep.co.uk in the first instance, as many concerns can be resolved without a formal complaint.

12. Children’s Data

The Platform is intended for use by businesses and professionals. We do not knowingly collect personal data from anyone under the age of 18. If you become aware that a child has provided us with personal data, please contact supportteam@angstep.co.uk and we will take steps to delete it.

13. Security

We implement appropriate technical and organisational measures to protect personal data against unauthorised access, alteration, disclosure or destruction, in accordance with Article 32 UK GDPR. These measures include:

- All data in transit encrypted via TLS 1.2 or higher;

- Database access restricted to application-layer connections on a private internal network;
- Authentication via Google OAuth 2.0, with two-factor authentication enforced at the identity provider level;
- Per-organisation isolation of remote access: each customer organisation has its own scoped remote access account and device group, and cannot see another customer's devices;
- Non-root container execution and hardened server configuration;
- Security event logging with rate limiting on authentication endpoints;
- SSH key-only access to infrastructure servers;
- Regular code security review (static analysis and dynamic testing);
- Data stored on EU infrastructure (Hetzner, Falkenstein, Germany);
- Script execution restricted to a curated, reviewed library that customers cannot modify; parameters validated and passed as environment variables so they cannot be interpreted as commands; script content checksummed and verified before execution; every run and refusal recorded.

In the event of a personal data breach likely to result in a risk to the rights and freedoms of individuals, we will notify the ICO within 72 hours of becoming aware of it, and will notify affected data subjects without undue delay where the breach is likely to result in a high risk to their rights and freedoms (Articles 33–34 UK GDPR).

14. Changes to This Policy

We will update this Privacy Policy from time to time as the Platform evolves or as legal requirements change. When we make material changes, we will:

- Update the version number and date at the top of this document;
- Notify account holders by email at least 14 days before the change takes effect;
- Where required by law, seek fresh consent before processing data under a new basis.

Continued use of the Platform after the effective date of a policy change constitutes acceptance of the revised terms. Previous versions are available on request.

15. Contact Us

Contact	Detail
Email	supportteam@angstep.co.uk
Response time	Within 5 working days for general queries; within 1 calendar month for data subject requests (UK GDPR Article 12)
Post	Angstep Ltd, Applegarth, Groes Lwyd, Abergele, Conwy, LL22 7SU — marked "Data Protection"

Document history

Version	Date	Change
0.9	June 2026	Draft for legal review. Not published.
1.1	August 2026	Script execution added to the Platform. New Section 3.4 describing the execution record and script output; contract added as the lawful basis for it; retention period and security measures updated.

Version	Date	Change
1.0	July 2026	First published version. Controller updated to Angstep Ltd (company number 17358935); ICO registration ZC183626 added; HubSpot added as a processor; consent added as a legal basis for marketing email, with a legitimate interests assessment for product usage analysis; consent record retention and operational alert emails documented.