NETHOLD LIMITED

Privacy Policy

Version: 1.0
Effective Date: 13/04/2026
Last Reviewed: 13/04/2026
Controller: NETHOLD LIMITED
Registered Office: 26 Russell Road, Southport. PR97RB
Companies House No.: 17153341
Contact: privacy@nethold.co.uk

1. Introduction

NETHOLD LIMITED ("NETHOLD", "we", "us", or "our") is committed to protecting and respecting your privacy. This Privacy Policy explains how we collect, use, store, and share personal data when you interact with our services, website (nethold.co.uk), or communicate with us.

We act as the Data Controller for the personal data we collect and process. This policy has been prepared in accordance with the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("DPA 2018").

Please read this policy carefully. If you have any questions, you can contact us at any time using the details in Section 14.

2. Who We Are

NETHOLD LIMITED is a UK-registered company providing managed domain leasing and web security services, primarily to sole traders and micro-businesses. We operate under a tiered service model (Core, Plus, and Pro) delivered through Cloudflare-based infrastructure.

As the Data Controller, we determine the purposes and means of processing your personal data. Where we engage third-party service providers who process data on our behalf, those parties act as Data Processors and are bound by appropriate contractual obligations (see Section 8).

3. Personal Data We Collect

We may collect and process the following categories of personal data:

3.1 Identity & Contact Information

- Full name
- Business name (if applicable)
- Email address
- Telephone number
- Postal address

3.2 Financial Information

- Bank account details (for GoCardless Direct Debit authorisation only — see note below)
- Billing address
- Invoice and payment history

Note: NETHOLD does not store full bank account details on its own systems. These are provided directly to GoCardless, our payment processor. GoCardless is a regulated payment institution authorised by the Financial Conduct Authority.

3.3 Technical & Usage Data

- Domain names registered or managed under your account
- IP addresses and DNS configuration data
- Security event logs generated through Cloudflare
- Website usage data (e.g. pages visited, browser type) if analytics are enabled

3.4 Communications Data

- The content of emails, messages, and meeting records relating to your account or enquiries
- Electronic signature records and signed agreements (via PandaDoc)
- Meeting scheduling data (via Calendly)

3.5 Data We Do Not Collect

We do not knowingly collect special category data (such as health, ethnicity, or political opinions) or personal data from children under the age of 16. Our services are intended for business use by adults.

4. How We Collect Personal Data

We collect personal data through the following means:

- Directly from you — when you enquire about our services, sign up as a client, complete a contract, or communicate with us
- Automatically — through our website and infrastructure (e.g. Cloudflare security logs, Hostinger server logs)
- From third parties — for example, when you schedule a meeting via Calendly or sign documents via PandaDoc

5. Legal Bases for Processing

Under the UK GDPR, we are required to have a valid legal basis for each type of processing activity. We rely on the following bases:

5.1 Performance of a Contract (Article 6(1)(b))

The majority of our processing is necessary to deliver the services you have contracted with us for. This includes managing your domain, applying security configurations, processing payments, and communicating about your account.

5.2 Legal Obligation (Article 6(1)(c))

We are required by law to retain certain financial records. For example, HMRC requires us to keep accounting records for a minimum of six years. We also process data as required to comply with any other applicable UK law.

5.3 Legitimate Interests (Article 6(1)(f))

We may process personal data where it is necessary for our legitimate business interests, provided those interests are not overridden by your rights. These interests include:

- Maintaining the security and integrity of our systems and network
- Preventing fraud and unauthorised access
- Improving our services
- Maintaining business records and correspondence

We carry out a Legitimate Interests Assessment (LIA) before relying on this basis and will provide a copy upon request.

5.4 Consent (Article 6(1)(a))

Where we send marketing communications or use non-essential cookies, we will seek your prior consent. You have the right to withdraw consent at any time without affecting the lawfulness of processing carried out before withdrawal.

Note: Consent is not our primary basis for processing. We do not use consent as a workaround for processing that should be justified by another basis.

6. How We Use Your Personal Data

We use your personal data for the following purposes:

- Providing and managing your domain leasing and web security services
- Processing and recording payments via GoCardless
- Issuing invoices and maintaining financial accounts
- Communicating with you by email, video call, or other channels
- Entering into and executing client agreements
- Monitoring for and responding to security incidents
- Complying with our legal and regulatory obligations
- Improving our services and internal processes

7. Sharing Your Personal Data

We do not sell, rent, or trade your personal data to third parties for marketing purposes.

We share personal data only in the following circumstances:

7.1 With Data Processors

We share data with third-party service providers who process it on our behalf. These are detailed fully in Section 8. All processors are required to process data only on our documented instructions and to maintain appropriate security standards.

7.2 With GoCardless (Payment Processor)

Where you pay by Direct Debit, your bank account details are provided directly to GoCardless Limited, a regulated payment institution. GoCardless is itself a Data Controller for the purposes of processing payment mandates and is subject to its own privacy policy.

7.3 Legal Disclosure

We may disclose personal data where required or permitted by law, including to HMRC, law enforcement agencies, or courts of competent jurisdiction.

7.4 Business Transfers

In the event of a business sale, merger, or restructuring, personal data may be transferred as part of that transaction. We will notify affected individuals where required by law.

8. Third-Party Data Processors

The table below lists all third-party services we use that may process personal data on our behalf. Where services are hosted outside the UK or European Economic Area (EEA), we describe the safeguards in place — see also Section 9.

8.1 Financial & Banking

Service	Category	Data Processed	Location	Safeguard
FreeAgent	Accounting	Client names, invoices, payment records, financial transactions	UK/EEA	UK GDPR compliant; Data Processing Agreement in place
Mettle (NatWest)	Business Banking	Business payment data, beneficiary details, account activity	UK	FCA-regulated UK bank; UK GDPR compliant

8.2 Communication & Scheduling

Service	Category	Data Processed	Location	Safeguard
Zoho Mail	Email Platform	Email addresses, message content, attachments	UK/EEA (EU servers)	Standard Contractual Clauses (SCCs); GDPR-compliant infrastructure
Zoom	Video Conferencing	Names, email addresses, meeting content, recordings (if enabled)	US / Global	SCCs for international transfers; ISO 27001 certified
Calendly	Meeting Scheduling	Names, email addresses, availability data, meeting details	US	SCCs in place; Privacy Shield successor framework
Resend	Email Delivery	Recipient email addresses, email content, delivery logs	US	Data Processing Agreement; SCCs for UK-to-US transfers

8.3 Operations & Infrastructure

Service	Category	Data Processed	Location	Safeguard
Hostinger	Website Hosting	Website visitor IP addresses, server logs	EU (Lithuania)	EU-based hosting; GDPR-compliant; DPA in place
Cloudflare	CDN & Web Security	IP addresses, DNS queries, traffic data, security event logs	US / Global	SCCs; Privacy Shield successor; ISO 27001; DPA in place
PandaDoc	Electronic Signatures	Names, email addresses, signed agreement content, audit trails	US	SOC 2 Type II; SCCs for UK-to-US transfers; DPA in place

8.4 Security

Service	Category	Data Processed	Location	Safeguard
Bitwarden	Credential Management	Encrypted credential vaults (employee use only — no client data stored)	US	Open-source; end-to-end encrypted; SCCs in place; SOC 2 Type II
Norton	Device Security	Local device telemetry and threat data (employee devices only)	US	Device-level processing; no client personal data transmitted; DPA in place

Note on Bitwarden and Norton: These tools are used exclusively on NETHOLD employee and operator devices for internal security purposes. They do not process client personal data and are included here for full transparency.

9. International Data Transfers

Some of our third-party processors operate servers located outside the United Kingdom and the European Economic Area — primarily in the United States. The UK GDPR restricts transfers of personal data to countries outside the UK unless adequate safeguards are in place.

For transfers to the United States and other third countries, we rely on the following safeguards where applicable:

9.1 Standard Contractual Clauses (SCCs)

The UK Information Commissioner's Office (ICO) has approved the use of Standard Contractual Clauses (SCCs) — also known as the International Data Transfer Agreement (IDTA) in the UK context — as a valid transfer mechanism. Where our processors are based in the US, we ensure that UK IDTA-compatible agreements or approved SCCs are in place.

9.2 Adequacy Decisions

Where the UK Government has issued an adequacy decision for a particular country (e.g. the EEA and certain other territories), personal data may flow to that country without additional safeguards.

9.3 Processor-Level Safeguards

In addition to contractual mechanisms, we select processors that demonstrate robust security practices — for example ISO 27001 certification, SOC 2 Type II audit reports, and end-to-end encryption. Specific safeguards are noted in the processor table in Section 8.

You may request a copy of the relevant transfer mechanism documents by contacting us using the details in Section 14.

10. Data Retention

We retain personal data only for as long as necessary to fulfil the purposes for which it was collected, or as required by applicable law. The following retention periods apply:

Category	Retention Period	Reason / Legal Basis
Financial & accounting records	6 years from end of relevant tax year	Legal obligation — HMRC / Companies Act 2006
Client contracts and signed agreements	6 years from contract end date	Legal obligation / Limitation Act 1980 (contractual claims)
Active client data (domains, DNS, security config)	Duration of the service relationship + 6 months	Contract performance; reasonable period for account closure queries
Email communications and correspondence	3 years from last contact	Legitimate interests — resolving disputes, service history
Security and infrastructure logs (Cloudflare, Hostinger)	Up to 12 months	Legitimate interests — security incident investigation
Prospective client enquiry data	12 months from last contact if no contract formed	Legitimate interests — follow-up and quoting
Marketing consent records	3 years from consent or until withdrawn	Legal compliance — evidence of consent under UK GDPR

At the end of the applicable retention period, we will securely delete or anonymise personal data. Where data is held by third-party processors, we will ensure it is deleted in accordance with our processor agreements.

11. Your Rights as a Data Subject

Under the UK GDPR and DPA 2018, you have the following rights in relation to your personal data. These rights are not absolute and may be subject to certain exceptions, but we will always respond to your request within one calendar month (or notify you if an extension is required).

Your Right	What It Means
Right of Access	You may request a copy of the personal data we hold about you. We will provide this free of charge in a commonly used electronic format.
Right to Rectification	You have the right to ask us to correct inaccurate or incomplete personal data. We will act on reasonable rectification requests promptly.
Right to Erasure	You may ask us to delete your personal data where there is no longer a lawful basis for us to retain it. This right does not apply where processing is required by law (e.g. statutory financial records).
Right to Restriction	You can request that we restrict the processing of your data in certain circumstances — for example, while the accuracy of data is being contested.
Right to Portability	Where processing is based on consent or contract and carried out by automated means, you may request that we provide your data in a structured, machine-readable format, or transfer it directly to another controller where technically feasible.
Right to Object	You have the right to object to processing based on legitimate interests or for direct marketing. Where you object to direct marketing, we will stop processing immediately with no exceptions.
Rights re Automated Decisions	We do not currently carry out fully automated decision-making or profiling that produces legal or similarly significant effects on individuals. If this changes, we will update this policy and provide the necessary safeguards.
Right to Withdraw Consent	Where processing is based on consent, you may withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing prior to withdrawal.

To exercise any of your rights, please contact us using the details in Section 14. We may need to verify your identity before processing your request.

12. Data Security

We take the security of personal data seriously and have implemented technical and organisational measures proportionate to the risks involved. Our security arrangements include:

- All domain and DNS infrastructure is managed through Cloudflare, with DNSSEC enabled as standard across all service tiers

- OWASP-based Web Application Firewall (WAF) rules applied at the Pro service tier
- SSL/TLS encryption enforced on all client-facing services
- Credentials and access keys are managed exclusively through Bitwarden, a zero-knowledge, end-to-end encrypted credential manager
- Operator devices are protected by Norton security software
- Client agreements and contracts are executed through PandaDoc, which maintains a full audit trail
- Access to financial data is restricted to authorised personnel only

In the event of a personal data breach that is likely to result in a risk to your rights and freedoms, we will notify the ICO within 72 hours of becoming aware of the breach, in accordance with Article 33 UK GDPR. Where the breach is likely to result in a high risk to you, we will also notify you directly without undue delay.

13. Cookies and Tracking Technologies

Our website (nethold.co.uk) may use cookies and similar technologies. We use only the minimum cookies necessary for the site to function correctly. We do not currently use advertising or tracking cookies.

Where our website is delivered via Cloudflare, Cloudflare may set technical cookies to support performance and security functions (such as bot management). These are strictly necessary and do not require prior consent under the UK Privacy and Electronic Communications Regulations (PECR).

If we introduce any non-essential cookies (e.g. analytics), we will update this section and implement an appropriate consent mechanism before those cookies are placed.

14. Contact Us & How to Complain

14.1 Data Controller Contact

NETHOLD LIMITED
26 Russell Road, Southport. PR97RB
Email: privacy@nethold.co.uk
Website: https://nethold.co.uk

14.2 Complaints

If you are unhappy with how we have handled your personal data, you have the right to lodge a complaint with the UK supervisory authority:

> Information Commissioner's Office (ICO)
> Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
> Telephone: 0303 123 1113
> Website: https://www.ico.org.uk

We would, however, appreciate the opportunity to address your concerns before you approach the ICO. Please contact us in the first instance and we will endeavour to resolve any issue promptly.

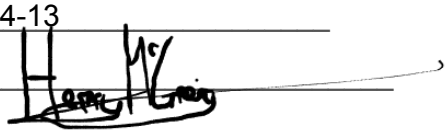
15. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our services, legal requirements, or best practice. When we make material changes, we will notify existing clients by email and update the "Last Reviewed" date at the top of this document. The most current version will always be available at https://nethold.co.uk/privacy.

Your continued use of our services following notification of changes will constitute acceptance of the revised policy.

Approved by: Henry McGreig
Director, NETHOLD LIMITED

Date: 2026-04-13

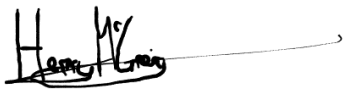
Signature: 

NETHOLD LIMITED | Privacy Policy v1.0 | UK GDPR & DPA 2018

CERTIFICATE *of* SIGNATURE

REF. NUMBER
R48MH-ZLVJE-NBZGH-6MR9G

DOCUMENT COMPLETED BY ALL PARTIES ON
13 APR 2026 22:54:20 UTC

SIGNER	TIMESTAMP	SIGNATURE
EMAIL **HENRY@NETHOLD.CO.UK**	SENT **13 APR 2026 22:54:19** SIGNED **13 APR 2026 22:54:20**	 IP ADDRESS **77.99.137.14** LOCATION **SOUTHPORT, UNITED KINGDOM**