DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") forms part of the agreement for the Spoofhound service (the "Service") between:

- Company trading as GoCloudConsulting, a sole trader established in the United Kingdom (the "Processor", "Spoofhound", "we"); and
- the customer that has accepted the Spoofhound Terms of Service (the "Controller", "Customer", "you").

It applies where Spoofhound processes personal data on the Customer's behalf and reflects the requirements of Article 28 of the UK GDPR. Where the Customer is established in the EU/EEA, references to the UK GDPR include the EU GDPR as applicable.

1. Roles and scope

For personal data contained in DMARC aggregate reports, DMARC failure (forensic) reports, TLS reports and related DNS and email authentication data processed for the Customer's verified domains, the Customer is the controller and Spoofhound is the processor. For account data of the Customer's own users (names, sign-in identifiers, contact addresses, audit records), Spoofhound processes as necessary to provide, secure and bill for the Service.

2. Details of processing

Subject matter and purpose

Receipt, parsing, storage, aggregation and presentation of email authentication reports (DMARC, TLS-RPT) for the Customer's domains; monitoring of related DNS records (SPF, DKIM, DMARC, BIMI, MTA-STS); alerting; and, where the Customer enables it, AI-assisted analysis of that data.

Categories of personal data

- Email metadata contained in reports: sending server IP addresses, sending and receiving domains, authentication results, message counts.
- DMARC failure (forensic) reports, which may contain message headers including individual email addresses and subject lines.
- Customer user account data: name, email address, sign-in identifiers, authenticator registrations, audit log entries.

Categories of data subjects

Individuals who send email purporting to be from, or to, the Customer's domains; the Customer's own users of the Service.

Duration

The term of the Customer's subscription, plus the retention periods in clause 8.

3. Processor obligations

Spoofhound shall:

- process the personal data only on the Customer's documented instructions, which are: the configuration the Customer applies in the Service and the functions the Customer invokes, unless

required otherwise by law (in which case Spoofhound will inform the Customer unless the law prohibits it);

- ensure persons authorised to process the data are bound by confidentiality obligations;
- implement the technical and organisational measures described in Annex B;
- respect the conditions in clauses 5 and 6 for engaging sub-processors;
- taking into account the nature of the processing, assist the Customer by appropriate technical and organisational measures in responding to data subject rights requests;
- assist the Customer in ensuring compliance with its obligations regarding security, breach notification, and data protection impact assessments, taking into account the nature of the processing and the information available to Spoofhound;
- at the Customer's choice, delete or return the personal data at the end of the provision of the Service, in accordance with clause 8; and
- make available the information necessary to demonstrate compliance with this DPA and allow for and contribute to audits as set out in clause 9.

4. Security

Spoofhound implements the measures in Annex B, including encryption in transit and at rest, tenant isolation enforced at the query layer, role-based access, audited administrative access, and tested backups. Spoofhound shall notify the Customer without undue delay after becoming aware of a personal data breach affecting the Customer's personal data, providing the information reasonably required for the Customer's own notification obligations.

5. Sub-processors

The Customer gives general written authorisation to the sub-processors listed in Annex C, which is also published at spoofhound.ai/legal/subprocessors. Spoofhound shall inform the Customer of intended additions or replacements at least 30 days in advance by notice in the Service or by email, giving the Customer the opportunity to object. Spoofhound imposes data protection obligations on each sub-processor equivalent to those in this DPA and remains liable for their performance.

6. AI processing (optional features)

AI analysis runs only where the Customer enables it, per domain. Where the Customer selects the managed AI option, Anthropic acts as a sub-processor. Where the Customer configures its own AI provider ("bring your own AI"), that provider processes data under the Customer's own agreement with it and is not a Spoofhound sub-processor; Spoofhound transmits data only to the provider the Customer configured. DNS record contents are excluded from data sent to the help assistant.

7. International transfers

Customer data is stored in the region of the Customer's chosen instance (Annex A). Personal data is transferred outside the UK/EEA only: (a) for Customers on the US instance, where processing occurs on US infrastructure; (b) to sub-processors listed in Annex C in the locations there stated; in each case under a lawful transfer mechanism (UK IDTA or Addendum to the EU Standard Contractual Clauses, or an applicable adequacy regulation).

8. Retention and deletion

The Service enforces the following retention automatically: full report detail (raw DMARC records and failure reports) 90 days; aggregate history 13 months; raw report emails 395 days; reports for unclaimed

domains at most 60 days. On termination, or on the Customer's request via the Service's deletion function, the Customer's tenant data is deleted; backup copies expire on the backup retention cycle (no more than 12 weekly and 13 monthly copies).

9. Audit

Spoofhound will make available on request documentation reasonably necessary to demonstrate compliance with this DPA. Where that is insufficient, the Customer may conduct, at its cost and on reasonable notice no more than once in any 12-month period, an audit limited in scope to Spoofhound's compliance with this DPA, conducted so as not to compromise the security or confidentiality of other customers' data.

10. General

This DPA prevails over the Terms of Service to the extent of any conflict concerning the processing of personal data. Liability under this DPA is subject to the limitations in the Terms of Service. This DPA is governed by the law governing the Terms of Service.

Annex A — Processing locations

- EU instance (eu1): Cloudflare EU jurisdiction; outbound email from AWS eu-west-2 (London).
- US instance (us1): Cloudflare US jurisdiction; outbound email from AWS us-east-1 (N. Virginia).
- Rest-of-world, KSA and UAE instances (row1, ksa1, uae1): isolated instances on Cloudflare's network without a contractual data jurisdiction; outbound email from AWS eu-west-2.

Annex B — Technical and organisational measures

- Encryption in transit (TLS) for all connections; encryption at rest on all storage.
- Tenant isolation: each customer's data is scoped to its tenant at the database query layer, enforced by build-time checks; instances share no data with each other.
- Access control: role-based access (viewer, analyser, admin); optional customer single sign-on with roles derived from the customer's directory at each sign-in; multi-factor authentication; administrative surfaces behind an additional access layer.
- Credential handling: customer-supplied secrets stored encrypted (AES-256-GCM); private keys generated and held by the Service are never disclosed.
- Auditing: administrative and security-relevant actions are recorded in per-tenant audit logs; staff support actions require a recorded reason and notify the customer's administrators.
- Availability: weekly verified backups retained 12 weeks in-region, monthly off-platform copies retained approximately 13 months with write-only credentials; automatic enforcement of the retention schedule in clause 8.
- Monitoring: continuous checks of the platform services the Service depends on, with alerting on failure.

Annex C — Sub-processors

- Cloudflare, Inc. (US/global) — application hosting, database and report storage, network security. Data location per Annex A.
- Amazon Web Services (AWS) — outbound email delivery (SES) and backup copy storage; regions eu-west-2 and us-east-1.
- ipinfo.io — IP address enrichment (sending server IP addresses only).

- Anthropic (US) — AI analysis, only for customers who enable the managed AI option.

Document status: draft v0.1, 2026-09-05. Produced for internal review; requires review by a qualified solicitor before issue.