# Data Processing Agreement

dnswatchdog.io

This Data Processing Agreement ('DPA') forms part of the agreement between DNS Watchdog Ltd. ('Processor', 'we', 'us', or 'our') and the customer ('Controller', 'you', or 'your') for the provision of DNS Watchdog services (the 'Services'). This DPA sets out the terms under which the Processor processes personal data on behalf of the Controller in accordance with the General Data Protection Regulation (EU) 2016/679 ('GDPR') and the UK General Data Protection Regulation ('UK GDPR').

For more information about how we handle personal data, please see our Privacy Policy and Data Protection Policy.

## 1. Definitions

In this DPA, the following terms have the meanings set out below. Terms not defined here have the meanings given to them in the GDPR or the main service agreement.

- **Controller**: The customer who determines the purposes and means of processing personal data and on whose behalf the Processor processes personal data under this DPA.
- **Processor**: DNS Watchdog Ltd., which processes personal data on behalf of the Controller in connection with the Services.
- **Data Subject**: An identified or identifiable natural person whose personal data is processed under this DPA.
- **Personal Data**: Any information relating to a Data Subject that is processed by the Processor on behalf of the Controller in connection with the Services.
- **Sub-processor**: A third party engaged by the Processor to process Personal Data on behalf of the Controller.
- **Processing**: Any operation or set of operations performed on Personal Data, including collection, recording, organisation, storage, adaptation, retrieval, consultation, use, disclosure, erasure, or destruction.
- **Data Protection Laws**: The GDPR, the UK GDPR, and any other applicable data protection legislation.
- **Supervisory Authority**: An independent public authority responsible for monitoring the application of Data Protection Laws.

## 2. Scope and Roles

### 2.1 Roles of the Parties

The Controller determines the purposes and means of processing Personal Data. The Processor processes Personal Data solely on behalf of the Controller and in accordance with the Controller's documented instructions, as described in this DPA and the main service agreement. This allocation of roles is in accordance with GDPR Article 28.

### 2.2 Scope of Processing

This DPA applies to all Personal Data that the Processor processes on behalf of the Controller in connection with the provision of the Services.

## 3. Details of Processing

### 3.1 Subject Matter

The processing relates to the provision of the DNS Watchdog platform, a DNS security service that helps organisations monitor, govern, and secure their DNS portfolio.

### 3.2 Duration

Processing begins when the Controller starts using the Services and continues for the duration of the service agreement. Upon termination, processing ceases in accordance with Section 10 of this DPA.

### 3.3 Nature and Purpose of Processing

The Processor processes Personal Data for the following purposes in connection with delivering the Services:

- Authenticating and managing user accounts
- Synchronising and analysing DNS records from the Controller's DNS providers
- Performing security scans (port scanning, certificate monitoring, HTTP checks)
- Capturing and analysing website screenshots
- Generating audit trails and change logs
- Processing billing and subscription data
- Monitoring application errors and performance
- Providing customer support

### 3.4 Categories of Personal Data

The following categories of Personal Data may be processed under this DPA:

| Category | Examples |
| --- | --- |
| Account information | Names, email addresses, usernames, user IDs |

| Category | Examples |
|---|---|
| Organisation data | Organisation names, organisation IDs, user roles |
| DNS record data | Domain names, record types, record values, IP addresses |
| SSL/TLS certificate data | Certificate issuers, expiry dates, subject alternative names |
| Network scan data | Open ports, detected services |
| Website monitoring data | Page screenshots, AI analysis summaries |
| IP intelligence data | Geolocation, ASN, hosting provider information |
| Usage and log data | IP addresses, browser information, timestamps, actions performed |
| Billing information | Subscription IDs, plan details (payment card data is processed directly by Stripe and is not accessed or stored by the Processor) |
| Audit trail data | User actions, timestamps, change details |

### 3.5 Categories of Data Subjects

The following categories of Data Subjects may have their Personal Data processed under this DPA:

- **Customers**: Individuals who create an account and use the Services.
- **End users**: Individuals within the Controller's organisation who are granted access to the Services.
- **Website visitors**: Individuals whose information may appear in DNS records, certificate data, or website monitoring data processed through the Services.

## 4. Obligations of the Processor

### 4.1 Documented Instructions

The Processor shall process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country, unless required to do so by applicable law. If such a legal requirement applies, the Processor

shall inform the Controller of that legal requirement before processing, unless the law prohibits such notification on important grounds of public interest.

### 4.2 Confidentiality

The Processor shall ensure that all persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Access to Personal Data is restricted to personnel who require it to perform their duties in connection with the Services.

### 4.3 Security Measures

The Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:

- Encryption of Personal Data at rest (AES-256 for stored data, AWS KMS for sensitive parameters) and in transit (TLS 1.2 minimum)
- Tenant isolation through application-level scope controls, IAM session tags, and storage-level access restrictions
- Access controls and authentication for all systems processing Personal Data
- Regular testing and assessment of the effectiveness of security measures
- Incident detection and response capabilities

For further details on our security measures, please refer to our Data Protection Policy.

### 4.4 Sub-processor Management

The Processor shall not engage another processor (Sub-processor) without prior general written authorisation from the Controller. The Controller provides general authorisation for the Sub-processors listed in Section 6 of this DPA.

Where the Processor engages a new Sub-processor, the Processor shall:

- Inform the Controller of any intended changes concerning the addition or replacement of Sub-processors, giving the Controller the opportunity to object to such changes
- Impose the same data protection obligations as set out in this DPA on the Sub-processor by way of a contract
- Remain fully liable to the Controller for the performance of the Sub-processor's obligations

### 4.5 Data Subject Rights

The Processor shall assist the Controller, by appropriate technical and organisational measures and taking into account the nature of the processing, in fulfilling the Controller's obligation to respond to requests from Data Subjects exercising their rights under Data Protection Laws, including:

- Right of access (Article 15)
- Right to rectification (Article 16)
- Right to erasure (Article 17)
- Right to restriction of processing (Article 18)
- Right to data portability (Article 20)
- Right to object (Article 21)

### 4.6 Breach Notification

The Processor shall notify the Controller without undue delay, and in any event within forty-eight (48) hours, after becoming aware of a personal data breach affecting Personal Data processed under this DPA. The notification shall include:

- A description of the nature of the breach, including the categories and approximate number of Data Subjects and Personal Data records affected
- The name and contact details of the Processor's data protection officer or other contact point
- A description of the likely consequences of the breach
- A description of the measures taken or proposed to address the breach, including measures to mitigate its possible adverse effects

The Processor shall cooperate with the Controller and take reasonable steps to assist in the investigation, mitigation, and remediation of the breach.

### 4.7 Data Protection Impact Assessments

The Processor shall assist the Controller, taking into account the nature of processing and the information available to the Processor, with any data protection impact assessments and prior consultations with Supervisory Authorities that the Controller is required to carry out under Articles 35 and 36 of the GDPR.

### 4.8 Deletion and Return of Data

Upon termination of the service agreement, the Processor shall, at the Controller's choice:

- Delete all Personal Data processed on behalf of the Controller and delete existing copies, unless applicable law requires storage of the Personal Data; or
- Return all Personal Data to the Controller in a commonly used, machine-readable format and delete existing copies.

The Controller may request deletion or return of data at any time during the term of the agreement by contacting the Processor at the details provided in Section 12.

### 4.9 Audit Rights

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

Audits shall be conducted with reasonable prior notice, during normal business hours, and in a manner that does not unreasonably disrupt the Processor's operations. The Controller shall bear the costs of any audit unless the audit reveals material non-compliance by the Processor.

## 5. Obligations of the Controller

The Controller shall:

- Provide documented instructions for the processing of Personal Data in accordance with Data Protection Laws
- Ensure that there is a lawful basis for the processing of Personal Data instructed under this DPA
- Notify the Processor promptly of any changes to applicable data protection requirements that may affect the Processor's obligations
- Be responsible for responding to Data Subject requests, with assistance from the Processor as described in Section 4.5

## 6. Approved Sub-processors

The Controller provides general authorisation for the Processor to engage the following Sub-processors. This list is consistent with the Processor's Vendor Management Policy.

| Sub-processor | Processing Purpose | Data Processed | Location |
|---|---|---|---|
| AWS (Amazon Web Services) | Cloud infrastructure hosting — compute, storage, networking, and database services for the platform | All platform data including customer data, DNS records, screenshots, and audit trails | EU (eu-west-2, London) |
| Clerk | Customer authentication and identity management | Customer identity data (email addresses, names, organisation membership, session tokens) | US (with EU data processing) |
| Stripe | Payment processing and subscription billing | Subscription and billing data (Stripe manages payment card details directly; the Processor does not store card numbers) | US (with EU data processing) |
| Sentry | Application error monitoring and performance tracking | Application error traces and request metadata (may include user IDs and email addresses in error context) | US/EU |
| Vercel | Frontend application hosting and content delivery | Application build artefacts and static assets (no customer Personal Data stored at rest) | Global edge network |

The Processor shall notify the Controller before adding or replacing any Sub-processor, providing the Controller with the opportunity to object. If the Controller objects on reasonable grounds relating to data protection, the parties shall discuss the objection in good faith. If no resolution can be reached, the Controller may terminate the affected Services.

## 7. International Data Transfers

Where Personal Data is transferred outside the European Economic Area ('EEA') or the United Kingdom — for example, to Sub-processors located in the United States — the Processor shall ensure that appropriate safeguards are in place, including:

- Standard Contractual Clauses ('SCCs') approved by the European Commission, incorporated into agreements with Sub-processors
- EU-US Data Privacy Framework certification, where applicable
- Supplementary technical measures, including encryption in transit and at rest

The Processor shall inform the Controller of any changes to the transfer mechanisms relied upon.

## 8. Liability

Each party's liability under this DPA is subject to the limitations and exclusions of liability set out in the main service agreement. Nothing in this DPA limits either party's liability for breaches of Data Protection Laws to the extent that such limitation is not permitted by applicable law.

## 9. Term and Termination

This DPA takes effect when the Controller begins using the Services and remains in force for the duration of the service agreement. The obligations of the Processor regarding the processing of Personal Data shall continue for as long as the Processor retains Personal Data processed on behalf of the Controller.

Upon termination, the provisions of Section 4.8 (Deletion and Return of Data) shall apply.

## 10. Changes to This DPA

We may update this DPA from time to time to reflect changes in our processing activities, Sub-processors, or applicable law. The 'Last Updated' date at the top of this page indicates when this DPA was last revised. We will notify the Controller of material changes at least thirty (30) days in advance. If the Controller objects to a material change, the Controller may terminate the affected Services by providing written notice within thirty (30) days of receiving notification of the change.

## 11. Governing Law

This DPA is governed by the laws of England and Wales. Any disputes arising under this DPA shall be subject to the exclusive jurisdiction of the courts of England and Wales, without prejudice to the rights of Data Subjects under Data Protection Laws to bring proceedings in their Member State of habitual residence.

## 12. Contact Us

If you have questions about this Data Processing Agreement or wish to exercise any rights under it, please contact us:

- **Email:** privacy@dnswatchdog.io
- **Data Protection Officer:** dpo@dnswatchdog.io
- **Website:** https://dnswatchdog.io