Data Protection Policy

dnswatchdog.io

1. Purpose

This policy describes how DNS Watchdog handles personal data and customer data in compliance with the General Data Protection Regulation (GDPR) and other applicable data protection legislation. It covers the lawful basis for processing, data minimisation, retention, and data subject rights.

2. Scope

This policy applies to all personal data processed by DNS Watchdog, whether collected directly from users or derived through platform operations. It covers data processed by the application, stored in AWS services, and held by third-party processors.

3. Data Controller

DNS Watchdog acts as the data controller for personal data collected through the platform. For DNS record data and provider credentials supplied by customers, DNS Watchdog acts as a data processor on behalf of the customer (data controller).

For questions about this policy or to exercise your data protection rights, please contact our Data Protection Officer (DPO) at dpo@dnswatchdog.io, or by post at: DNS Watchdog Ltd., Data Protection Officer, 167-169 Great Portland Street, 5th Floor, London W1W 5PF, United Kingdom.

4. Personal Data Processed

4.1 Data Collected Directly

Data Category	Data Elements	Source	Purpose
Account identity	User ID, email address, full name	Clerk authentication	Account management, authentication, communication
Organisation context	Organisation ID, organisation slug, user role	Clerk JWT claims	Multi-tenant access control, role-based authorisation

Data Category	Data Elements	Source	Purpose
Subscription data	Subscription ID, plan tier, usage limits	Stripe via Clerk JWT	Service entitlement, billing
User preferences	Display settings, notification preferences	User input	Personalisation
User notes	Free-text notes on DNS records	User input	Record annotation

4.2 Data Derived Through Processing

Data Category	Data Elements	Source	Purpose
DNS records	Domain names, record types, record values, IP addresses	Customer DNS providers (Route53, Cloudflare, CSC, Azure DNS, Google Cloud DNS)	Security analysis, change detection
SSL/TLS certificates	Certificate issuer, expiry, SANs, chain details	Public certificate endpoints	Certificate monitoring
Port scan results	Open ports, detected services	Network scanning	Security risk assessment
Website screenshots	Page captures, AI analysis summaries	HTTP requests to customer domains	Visual monitoring, risk assessment
IP intelligence	Geolocation, ASN, hosting provider	IP resolution and enrichment	Context for security analysis
Audit trail	User actions, timestamps, change details	Application events	Accountability, compliance

5. Lawful Basis for Processing

Processing Activity	Lawful Basis	Justification
Account creation and authentication	Contract performance (Art. 6(1)(b))	Necessary to provide the service the customer has subscribed to.
DNS record synchronisation and analysis	Contract performance (Art. 6(1)(b))	Core service functionality requested by the customer.
Security scanning (ports, certificates, HTTP)	Legitimate interest (Art. 6(1)(f))	Necessary for the security monitoring service; balanced against minimal privacy impact as scanning targets customer-owned infrastructure.
Screenshot capture and AI analysis	Contract performance (Art. 6(1)(b))	Feature of the subscribed service for visual monitoring.
Billing and subscription management	Contract performance (Art. 6(1)(b))	Necessary to manage the commercial relationship.
Error monitoring and logging	Legitimate interest (Art. 6(1)(f))	Necessary to maintain service reliability and investigate issues. Logs are minimised and access-controlled.
Audit trail	Legitimate interest (Art. 6(1)(f))	Necessary for security accountability and customer compliance requirements.

6. Data Minimisation

DNS Watchdog collects and processes only the data necessary for the stated purposes:

- Authentication data is sourced from Clerk JWT claims; the platform does not store

passwords or manage authentication credentials directly.

- DNS provider credentials are stored in SSM Parameter Store and accessed only when performing provider operations; they are never logged or included in error reports.
- Structured logging includes user IDs and email addresses for request tracing but excludes request bodies, provider credentials, and other sensitive payloads.
- Sentry error reports are filtered to exclude rate limit errors, expected validation failures, and other non-actionable events.

7. Data Retention

Data Type	Retention Period	Mechanism
DNS records (active)	Retained while the provider connection is active	Deleted when provider is removed or record is archived
Archived DNS records	Up to 3 years (available for restoration)	Stored in the `archive` DynamoDB table; can be restored or permanently deleted by the customer
Screenshots	365 days	S3 lifecycle policy: STANDARD → STANDARD_IA (30 days) → GLACIER (90 days) → Deleted (365 days)
Changelog / audit trail	Up to 3 years	Retained for compliance and audit purposes
Scan history	Up to 2 years	Retained for trend analysis and audit
Provider API request logs	Up to 1 year	Retained for debugging and audit; logs are filtered to exclude provider credentials, API tokens, and other sensitive authentication material

Data Type	Retention Period	Mechanism
Application logs	Per CloudWatch retention policy	Configurable per log group
Error reports (Sentry)	Per Sentry retention settings	Managed by Sentry's data retention configuration
User preferences	Retained while account is active	Deleted upon account closure
Subscription/billing data	Retained per legal requirements	Managed through Stripe; local cache in DynamoDB with TTL

8. Data Security

8.1 Encryption at Rest

- **DynamoDB**: AWS-managed encryption enabled by default on all tables.
- **S3**: Server-side encryption with AES-256 (SSE-S3) enabled on the screenshots bucket with bucket key optimisation.
- **SSM Parameter Store**: SecureString parameters encrypted with AWS KMS.
- **CloudFormation parameters**: Sensitive values (encryption keys, Sentry DSN) use `NoEcho` to prevent exposure in stack outputs or logs.

8.2 Encryption in Transit

- All API communication enforced over TLS 1.2 minimum via API Gateway security policy.
- Frontend-to-API communication over HTTPS with strict CORS policy restricting origins to the application domain.
- Internal AWS service communication uses AWS SDK default TLS configuration.
- CloudFront distributions enforce HTTPS for screenshot delivery.

8.3 Tenant Isolation

Customer data is isolated at multiple levels:

- Application-level isolation via `scope_id` partition keys.
- Infrastructure-level isolation via IAM session tags on temporary STS credentials.

- Storage-level isolation via S3 object prefix conditions and SSM parameter path restrictions.

9. Data Subject Rights

DNS Watchdog supports the following data subject rights under GDPR:

Right	How It Is Fulfilled
Right of access (Art. 15)	Customers can view all their data through the application dashboard. Additional requests can be made to the support team.
Right to rectification (Art. 16)	Account details are managed through Clerk. DNS data is synced from authoritative providers and can be corrected at source.
Right to erasure (Art. 17)	Customers can delete providers, zones, and records through the application. Account deletion requests are processed through the support team.
Right to restriction (Art. 18)	Customers can disconnect providers to stop data processing while retaining existing data.
Right to data portability (Art. 20)	DNS data and other customer data can be exported through the application dashboard in standard formats such as JSON or CSV.
Right to object (Art. 21)	Customers can contact the support team to object to specific processing activities.

10. Third-Party Processors

Processor	Data Processed	Purpose	Location
AWS (Amazon Web Services)	All platform data	Cloud infrastructure hosting	EU (eu-west-2, London)
Clerk	User identity, authentication data	Identity and authentication provider	US (with EU data processing)

Processor	Data Processed	Purpose	Location
Sentry	Error traces, request metadata	Error monitoring and alerting	US/EU
Stripe	Subscription and billing data	Payment processing	US (with EU data processing)
Vercel	Frontend application code (no customer data at rest)	Frontend hosting and CDN	Global edge network

Data processing agreements are in place with all third-party processors.

11. International Transfers

Where personal data is transferred outside the EEA (e.g., to US-based processors), transfers are protected by:

- Standard Contractual Clauses (SCCs) incorporated into processor agreements.
- EU-US Data Privacy Framework certification where applicable.
- Supplementary technical measures including encryption in transit and at rest.

12. Data Breach Notification

In the event of a personal data breach, DNS Watchdog will:

- Assess the breach through the incident response team, led by the Data Protection Officer, in accordance with the Incident Response Policy.
- Notify the relevant supervisory authority within 72 hours of becoming aware of the breach, where required.
- Notify affected data subjects without undue delay where the breach is likely to result in a high risk to their rights and freedoms.
- Document all breaches in the incident register regardless of notification requirements.

13. Data Protection Impact Assessments

DNS Watchdog conducts Data Protection Impact Assessments (DPIAs) for processing activities that are likely to result in a high risk to the rights and freedoms of individuals.

This includes, but is not limited to, security scanning of customer infrastructure, website screenshot capture with AI-assisted analysis, and any new processing activities involving personal data at scale. DPIAs are reviewed when there are significant changes to the relevant processing activity.

14. Data Protection by Design and Default

DNS Watchdog implements data protection by design and by default (Art. 25 GDPR) throughout the platform. This includes:

- Multi-tenant isolation at the application, infrastructure, and storage levels to ensure customer data is segregated by default.
- Encryption at rest and in transit for all personal data.
- Data minimisation in logging and error reporting, excluding sensitive payloads and credentials.
- Privacy-preserving defaults, such as non-essential cookies being disabled until the user provides consent.
- Regular review of new features and processing activities for data protection implications before deployment.

15. Records of Processing Activities

DNS Watchdog maintains records of processing activities (ROPA) in accordance with Art. 30 GDPR. These records document the purposes of processing, categories of data subjects and personal data, recipients, international transfers, retention periods, and technical and organisational security measures. The ROPA is reviewed and updated when processing activities change and is available to the supervisory authority upon request.

16. Data Classification

Personal data processed by DNS Watchdog is classified in accordance with the Data Classification Policy. Data classification levels determine the security controls, access restrictions, and handling procedures applied to each category of data.

17. Staff Training

All personnel with access to personal data are required to complete data protection training as part of their onboarding, covering this policy, the Data Classification Policy,

and platform-specific data handling procedures. Training is refreshed annually or when significant changes are made to data processing activities or applicable legislation.

18. Review

This policy is reviewed annually or when there are significant changes to data processing activities, applicable legislation, or the platform architecture.