Reguweb — Data Processing Agreement

Effective July 28, 2026

1. Purpose

This Data Processing Agreement (“DPA”) governs the processing of personal data by Reguweb (“Processor”) on behalf of the customer (“Controller”) under the Reguweb Terms of Service. It forms an integral part of the parties’ agreement and takes precedence over conflicting terms regarding data processing.

2. Definitions

Capitalised terms not otherwise defined have the meaning given to them in the EU General Data Protection Regulation (Regulation (EU) 2016/679, the “GDPR”). “Personal Data” means any information relating to an identified or identifiable natural person.

3. Subject matter and duration

The Processor processes Personal Data on the Controller’s behalf for the duration of the underlying service subscription. Categories of data, categories of data subjects, and the nature of processing are described in Annex A.

4. Processor obligations

1. Process Personal Data only on documented instructions from the Controller, including with regard to transfers to third countries, unless required by Union or Member State law to which the Processor is subject.
2. Ensure persons authorised to process the Personal Data are bound by an obligation of confidentiality.

3. Implement appropriate technical and organisational measures as described in Annex B.
4. Provide reasonable assistance to the Controller in responding to data subject requests, conducting Data Protection Impact Assessments, and complying with Articles 32–36 GDPR.
5. At the Controller's choice, delete or return all Personal Data after the end of the provision of services, unless storage is required by applicable law.

5. Sub-processors

The Controller authorises the Processor to engage sub-processors listed at **https://app.reguweb.com/sub-processors**. The Processor will give the Controller at least thirty (30) days' advance notice of any intended addition or replacement of a sub-processor and will impose data protection obligations on the sub-processor no less protective than those in this DPA.

6. International transfers

Where Personal Data is transferred outside the European Economic Area to a country not deemed adequate by the European Commission, the parties will rely on the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914.

7. Security incidents

The Processor will notify the Controller without undue delay after becoming aware of a Personal Data breach, and in any event within seventy-two (72) hours. Notification will include the nature of the breach, the categories and approximate number of data subjects affected, likely consequences, and mitigation measures.

8. Audits

The Processor will make available to the Controller all information necessary to demonstrate compliance with this DPA. Where the Controller requires further verification, the Processor will accept audits — at the Controller's expense and no more than once per twelve (12) months — conducted under reasonable confidentiality terms.

9. Liability

Each party's liability under this DPA is subject to the limitations of liability set out in the underlying Terms of Service.

Annex A — Processing details

- **Categories of data subjects:** Controller's end users, employees, contractors, and authorised representatives.
- **Categories of Personal Data:** name, business email, hashed password, billing identifiers, scan target URLs, activity-log entries, support correspondence.
- **Nature and purpose of processing:** providing accessibility and compliance scanning, billing, customer support, and security monitoring.
- **Retention:** Personal Data is retained for the duration of the customer relationship plus the windows described in the Reguweb retention policy (activity_log 365 days, email_logs 90 days, scan_results 1 year, compliance_history 2 years).

Annex B — Technical and organisational measures

- TLS 1.2+ on every customer-facing endpoint; HSTS enforced.
- Encryption at rest (AES-256) on application database, scan-result blobs, and ticket attachments.

- Role-based access controls with MFA-required production access and audit logging.
- Sentry integration with request-id correlation for every reported exception.
- HMAC-SHA256 signed outbound webhooks with 300-second timestamp tolerance to prevent replay.
- Composer audit and dependency review for high-severity CVEs within seven (7) days.

Questions about this DPA? Contact no-reply@reguweb.com.