Data Processing Agreement (Template)

erabot.ai · Effective: April 11, 2026 · Version: 1.0

1. Parties

This Data Processing Agreement (“DPA”) is entered into between erabot.ai, operated by Rohan Shah (“Processor”), and the Customer identified in the underlying Terms of Service (“Controller”).

2. Scope and Duration

This DPA applies to all Personal Data (as defined in GDPR Article 4) that Processor processes on behalf of Controller in connection with the erabot.ai Services. It takes effect on the Effective Date above and remains in force for the duration of the Services agreement.

3. Nature and Purpose of Processing

Processor processes Customer-submitted source code solely to generate code-cost audit reports. Raw source code is deleted immediately after the scan completes; the 30-day retention ceiling in the Privacy Policy is a worst-case upper bound on any intermediate processing artifacts. Audit metadata (findings, metrics, reports) is retained for the lifetime of the Customer account.

Processor does NOT train any machine-learning models on Customer code or scan data, and does not permit any Subprocessor to do so.

4. Subprocessors

Processor uses the following Subprocessors to deliver the Services:

- **Google Cloud (Gemini API)** — code audit AI inference, under the GCP Data Processing Addendum (US / EU)
- **Fly.io** — application hosting (Global)
- **Stripe** — billing, subscription management, payments (US / EU)
- **Resend** — transactional email delivery (US)
- **Sentry** — error tracking with PII scrubbing (US)
- **PostHog** — product analytics with opt-out (US / EU)

Processor will notify Controller of any changes to the Subprocessor list with at least 30 days' notice. Controller may object to the addition or replacement of a Subprocessor within that period.

5. Security Measures

Processor implements industry-standard technical and organizational measures including: TLS 1.2+ encryption in transit with HSTS, Fernet symmetric encryption for API keys at rest, Argon2 password hashing, JWT in HTTP-only secure cookies, pre-scan secrets redaction before any external API call, role-based access controls, structured logging with sensitive data excluded, and regular security reviews.

6. Data Subject Rights

Processor will support Controller in responding to Data Subject requests under GDPR Articles 12–23 within the statutory 30-day window. Deletion requests are backed by the `DELETE /api/account/data` endpoint, which cascades through scan history, findings, subscription-tier records, and account data. User rows are soft-deleted (placeholder email plus `deleted_at` timestamp) to preserve Stripe billing audit trails as required by financial record-keeping regulations.

7. International Transfers

Where Personal Data is transferred outside the EEA/UK, Processor relies on the European Commission's Standard Contractual Clauses (Commission Implementing Decision 2021/914/EU) as the transfer mechanism. Processor's Subprocessors maintain equivalent safeguards.

8. Contact

Data protection inquiries and DPA negotiation: privacy@erabot.ai / legal@erabot.ai