Data Processing Agreement (DPA) — Template

This is an unsigned template. To execute a binding DPA, contact support@audittodesk.com for a counter-signed copy.

1. Parties

This DPA governs the processing of personal data between AuditToDesk (operated by Sagbrain Global Pte. Ltd., the "Processor") and the customer using the AuditToDesk service (the "Controller").

2. Data in scope

Data the Controller registers or submits to AuditToDesk, including (i) user account information (email, name), (ii) scanned URLs, (iii) public website content surfaced by scans, and (iv) billing and usage logs.

3. Processing purpose

Generating site-diagnosis reports, agency matching, account operations, fraud detection, statutory retention, and any activity necessary to deliver the service.

4. Processing duration

For as long as the Controller maintains an account. After deletion, data is erased per the retention policy in PRD §17 (backups retained up to 90 days).

5. Sub-processors

Current sub-processors: Amazon Web Services (hosting), Google Gemini API (AI diagnosis), Google PageSpeed Insights API (performance), Stripe (payments), Sentry (error monitoring), SendGrid or AWS SES (email). New sub-processors will be notified by email ≥30 days in advance.

6. Security measures

TLS 1.2+ in transit, AES-256 at rest, dual-layer multi-tenant isolation via PostgreSQL Row-Level Security, bcrypt (cost 12) password hashing, short-lived JWT access tokens, Sentry error monitoring, SOC 2-compliant AWS infrastructure.

7. Personal-data breach notification

We will notify the Controller by email within 72 hours of becoming aware of any breach of personal data, including the nature of the breach, an estimate of affected records, and the steps we have taken.

8. Data-subject rights

On the Controller's reasonable request we will provide technical assistance for data-subject access, rectification, erasure, and portability requests. Send written requests to privacy@audittodesk.com.

9. Audit rights

Controllers may conduct a security-questionnaire-based audit once per year with ≥30 days' notice. OEM-tier customers may additionally conduct an on-site audit.

10. International data transfers

Primary infrastructure is hosted in Japan, but sub-processors may process data in the US or EU. Cross-border transfers are protected by GDPR-compliant Standard Contractual Clauses (SCCs).

11. Termination

On service-agreement termination, personal data will be returned or erased within 30 days at the Controller's choice, subject to statutory retention obligations.

12. Contact

DPA-related inquiries: privacy@audittodesk.com / Sagbrain Global Pte. Ltd. (Singapore).