

データ処理契約（DPA） — テンプレート

本書は未署名のテンプレートです。締結には第12条の連絡先までご連絡のうえ、署名済みの正式版をご依頼ください。

1. 契約当事者

本DPAは、AuditToDesk（提供事業者：株式会社サグブレイン「処理者」）と、AuditToDeskサービスを利用する貴社（「管理者」）との間の、個人データの取り扱いに関する条件を定めるものです。

2. 処理対象データ

管理者が AuditToDesk に登録または送信した、(i) ユーザーアカウント情報（メールアドレス・氏名）、(ii) スキャン対象URL、(iii) スキャン結果に含まれる公開ウェブサイトコンテンツ、(iv) 課金・利用ログ。

3. 処理目的

サイト診断レポートの生成、制作会社のご紹介、アカウント運用、不正利用検知、法令上の保持義務、および本サービスの提供に必要な範囲。

4. 処理期間

管理者がアカウントを保持している期間。アカウント削除後、PRD §17 に定める保持ポリシー（最大90日のバックアップ保持）に従い消去します。

5. 副処理者

現行の副処理者：Amazon Web Services（インフラ・ホスティング）、Google Gemini API（AI診断）、Google PageSpeed Insights API（性能診断）、Stripe（決済）、SendGrid または AWS SES（メール配信）。副処理者の追加は事前にメールで通知します。

6. セキュリティ対策

TLS 1.2 以上による通信、保存時の AES-256 暗号化、PostgreSQL の Row-Level Security による多層の隔離、bcrypt（コスト12）によるパスワードハッシュ化、JWT による短期アクセストークン、SOC 2 準拠の AWS インフラ。

7. データ侵害通知

個人データに関する侵害を認識した場合、72時間以内に管理者へメール通知します。通知には、侵害の性質、影響を受ける可能性のあるレコード数、当社が取った対策が含まれます。

8. データ主体の権利

管理者からの要請に応じ、データ主体のアクセス・訂正・削除・移転リクエストに対し合理的な範囲で技術的に協力します。第12条の連絡先宛に書面でリクエストください。

9. 監査権

管理者は、合理的な事前通知（30日以上）の上、年1回までセキュリティアンケート方式の監査を実施できます。

10. 国際データ移転

日本国内に主要インフラを設置していますが、副処理者のサービス特性上、米国・EU 等への移転が発生する場合があります。GDPR の標準契約条項（SCC）に基づき適切な保護措置を講じます。

11. 契約終了

本サービス契約終了時、管理者の選択により、個人データを返却または30日以内に消去します。法令上の保持義務がある場合はその期間を除きます。

12. 連絡先

