

Data Processing Agreement

RevCore Pro LLC

Version 1.0 | Effective April 06, 2026

security@revcorepro.com | revcorepro.com/security

This Data Processing Agreement (“DPA”) forms part of the Terms of Service between RevCore Pro LLC (“Processor”) and the Customer (“Controller”) and governs the processing of personal data by RevCore Pro LLC on behalf of the Customer in connection with the RevCore Pro platform.

By signing below, both parties agree to the terms of this DPA. This DPA supplements and is incorporated into the RevCore Pro Terms of Service available at revcorepro.com/terms.

1. Definitions

Personal Data means any information relating to an identified or identifiable natural person as defined under applicable data protection laws, including the GDPR and applicable U.S. state privacy laws.

Processing means any operation performed on Personal Data, including collection, storage, use, disclosure, or deletion.

Controller means the Customer, who determines the purposes and means of Processing Personal Data.

Processor means RevCore Pro LLC, which Processes Personal Data on behalf of the Controller.

Sub-processor means any third party engaged by the Processor to Process Personal Data on behalf of the Controller.

Services means the RevCore Pro platform and related services provided under the Terms of Service.

2. Scope and Nature of Processing

The Processor will Process Personal Data only as necessary to provide the Services and only in accordance with the Controller's documented instructions, including those set out in this DPA and the Terms of Service.

The subject matter, duration, nature, and purpose of the Processing, as well as the types of Personal Data and categories of Data Subjects, are as follows:

- **Subject matter:** Operation of the RevCore Pro field service management platform
- **Duration:** For the term of the Services agreement and as required by applicable law thereafter
- **Nature:** Storage, retrieval, display, transmission, deletion, and backup of Personal Data
- **Purpose:** Providing CRM, quoting, scheduling, invoicing, payment, and related features to the Controller
- **Data types:** Contact information (name, email, phone, address), business information, communications, location data from time entries, financial reference data
- **Data subjects:** Controller's customers, employees, and contractors whose data is entered into the platform

3. Controller Instructions

The Processor will Process Personal Data only on documented instructions from the Controller. The Controller's use of the Services constitutes its instructions to Process Personal Data as described in this DPA.

If the Processor is required by applicable law to Process Personal Data in a manner inconsistent with the Controller's instructions, the Processor will notify the Controller before such Processing unless prohibited by law.

The Controller warrants that it has the authority to provide Personal Data to the Processor and that it has obtained all necessary consents and provided all required notices to Data Subjects.

4. Processor Obligations

a. Confidentiality

The Processor will ensure that personnel authorized to Process Personal Data are subject to appropriate confidentiality obligations.

b. Security

The Processor will implement and maintain appropriate technical and organizational measures to protect Personal Data against unauthorized access, disclosure, alteration, or destruction, taking into account the risks presented by the Processing. Current security measures include:

- All data in transit encrypted via TLS over HTTPS

- Cookie-based authentication with automatic session refresh
- Role-based access control with organization-level data isolation
- Row-level security enforced at the database layer
- bcrypt password hashing at cost factor 12
- Distributed rate limiting on authentication endpoints
- Webhook signature verification for all inbound third-party events
- Dual audit logging for organization-level and platform admin actions
- Daily automated backups with 7-snapshot retention per organization

A full description of current security controls is maintained at revcorepro.com/security.

c. Data Subject Rights

The Processor will provide reasonable assistance to the Controller in responding to Data Subject requests to exercise rights under applicable data protection law. The Controller is responsible for determining how to respond to such requests.

d. Data Breach Notification

In the event of a confirmed Personal Data breach, the Processor will notify the Controller without undue delay and in any event within 72 hours of becoming aware of the breach. The notification will include: (i) a description of the nature of the breach; (ii) the categories and approximate number of Data Subjects affected; (iii) the categories and approximate volume of Personal Data records affected; (iv) likely consequences of the breach; and (v) measures taken or proposed to address the breach.

e. Data Protection Impact Assessments

The Processor will provide reasonable assistance to the Controller in conducting data protection impact assessments and prior consultations with supervisory authorities, where required by applicable law.

5. Sub-processors

The Controller authorizes the Processor to engage the following Sub-processors to assist in providing the Services. The Processor will impose data protection obligations on Sub-processors equivalent to those in this DPA.

Service	Category	Data Received
Supabase	Database, Auth, Storage	All application data, user sessions, uploaded files, backup exports
Stripe	Payment processing	Customer IDs, subscription IDs, invoice amounts, payment metadata. No raw card data.
Resend	Transactional email	Recipient email addresses, names, email bodies (may contain PII), delivery events

Upstash Redis	Rate limiting	IP addresses, authenticated user IDs, rate-limit counters
OpenAI	AI generation	User-authored slide generation prompts. No structured PII by default.
Google APIs	Calendar integration	Calendar event titles, timestamps, attendees. OAuth tokens stored in database.
GoHighLevel	CRM integration	Contact names, emails, phone numbers, addresses, conversation data from connected accounts
Sentry	Error monitoring	Error stack traces, server-side exception details. Session Replay with PII scrubbing.
Vercel	Hosting, CDN, Cron	HTTP traffic, server logs, environment variables, function execution metadata

The Processor will provide the Controller with at least 30 days' prior written notice before adding or materially changing a Sub-processor. Notice will be sent to the email address on file for the Controller's account and posted at revcorepro.com/subprocessors. If the Controller objects to a new Sub-processor, it may terminate the Services with written notice within 30 days of receiving the notification.

6. International Data Transfers

The Processor is based in the United States. Where the Controller is located outside the United States, or where Personal Data of individuals located outside the United States is transferred to or Processed by Sub-processors outside the Controller's jurisdiction, such transfers are subject to applicable data transfer mechanisms, including Standard Contractual Clauses where required.

The Controller acknowledges that the Sub-processors listed in Section 5 may process data in the United States and other jurisdictions. Each Sub-processor maintains its own data transfer mechanisms. Links to Sub-processor data transfer documentation are available upon request.

7. Data Retention and Deletion

The Processor will retain Personal Data for the duration of the Services agreement and as necessary to comply with legal obligations.

Upon termination of the Services, the Processor will, at the Controller's election, either delete or return all Personal Data within 90 days, unless applicable law requires retention. Organization data exports are available on request for up to 90 days following termination. After this period, Personal Data will be permanently deleted from production systems.

Backup copies may be retained for up to 90 days following deletion from production systems, after which they will be purged.

8. Audit Rights

The Processor will make available to the Controller all information reasonably necessary to demonstrate compliance with this DPA and will allow for and contribute to audits conducted by the Controller or a third-party auditor mandated by the Controller, subject to reasonable notice and confidentiality obligations.

The Controller agrees to exercise audit rights no more than once per calendar year and to give at least 30 days' advance written notice, unless a confirmed data breach requires more urgent investigation. Audit costs will be borne by the Controller unless the audit reveals a material breach by the Processor.

9. Limitation of Liability

Each party's liability under this DPA is subject to the limitations and exclusions set out in the RevCore Pro Terms of Service. Nothing in this DPA limits either party's liability for fraud, gross negligence, or willful misconduct.

10. Governing Law

This DPA is governed by the laws of the State of Delaware, United States, without regard to conflict of law provisions. Any disputes arising under this DPA will be resolved in accordance with the dispute resolution provisions of the Terms of Service.

Where the Controller is subject to GDPR, this DPA incorporates the requirements of Article 28 of the GDPR. Where the Controller is subject to applicable U.S. state privacy laws (including CCPA/CPRA), this DPA incorporates the requirements of those laws to the extent applicable.

11. General

This DPA constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior agreements, understandings, and representations relating to data processing.

If any provision of this DPA is held invalid or unenforceable, the remaining provisions will remain in full force and effect.

This DPA may be amended by the Processor with 30 days' written notice to the Controller. Continued use of the Services after the notice period constitutes acceptance of the amended DPA.

Questions regarding this DPA should be directed to: security@revcorepro.com

Signatures

By signing below, both parties agree to the terms of this Data Processing Agreement.

DATA CONTROLLER (Customer)

Signature: _____

Name: _____

Title: _____

Company: [Customer Legal Name]

Date: _____

DATA PROCESSOR (RevCore Pro)

Signature: _____

Name: _____

Title: _____

Company: RevCore Pro LLC

Date: _____

RevCore Pro LLC · security@revcorepro.com · revcorepro.com/security · revcorepro.com/subprocessors