COADAN

Security & Data Handling

How Coadan stores, protects, and isolates your data.

Coadan handles your loan documents, financial data, and borrower information. This document covers how that data is stored, who can access it, and what we do and don't do with it. We've written it the way an asset manager would want it written: direct, specific, and honest about what's in production today versus what's on the roadmap.

Coadan is an early-stage company. We are pre-SOC 2 and transparent about that. The controls described below reflect what is actually deployed in production today. Items on the roadmap are labeled as such. We are happy to walk a security team through this document, share infrastructure compliance reports under NDA, or respond to a formal security questionnaire before any pilot.

Data residency & infrastructure

Where is my data stored?

All customer data is stored in **Supabase Cloud (Postgres)**, hosted on AWS in US regions. Document files (PDF and Excel uploads) are stored in Supabase Storage, backed by AWS S3. Supabase is **SOC 2 Type II certified** and HIPAA-eligible. Coadan does not transfer customer data to additional infrastructure or third-party data warehouses.

Is data segregated by customer?

Yes. Every customer is a separate *firm* in Coadan's schema. Every business table carries a firm_id foreign key, and Postgres row-level security (RLS) policies enforce that a user can only read or write rows belonging to their own firm. **This is enforced at the database layer, not the application layer**, so a bug in application code cannot leak data across firms. RLS is enabled on every firm-scoped table in production today.

Is data encrypted?

Yes. **In transit:** TLS 1.3 on every connection. **At rest:** AES-256 via Supabase's encrypted storage, using AWS-managed keys. Database backups are encrypted with the same standard.

How long is data retained?

Data is retained for the duration of the customer relationship. On contract termination, customer data is deleted within 30 days of the termination effective date. Before deletion, customers can request a complete export of their data (loans, documents, narratives, financials, audit trails) in machine-readable format at no charge.

Access control

Who at Coadan can see my data?

Today, Coadan is a single-founder operation. Alex Gottlieb has administrative access to all customer data for purposes of platform support and incident response. This is enforced through a dedicated administrative role at the database layer, separate from customer login. **Access is logged.** As Coadan adds engineering staff, access will be limited to the minimum required for support, with logging maintained. Customer data is never used for any purpose other than operating the platform for that customer.

How do users authenticate?

Email plus password, with passwords hashed using bcrypt via Supabase Auth. **Multi-factor authentication** is supported via the Supabase Auth platform and can be enabled on request. **Single sign-on** (Okta, Microsoft Entra ID, Google Workspace) is supported on the Supabase Auth platform and can be enabled for customers requiring it.

Can my employees have different access levels within Coadan?

All users within a firm currently have read access to all loans in the firm. Granular per-loan and per-role permissions (for example, AM team sees everything, IC members see only memos and approvals) are on the roadmap. This is not deployed today.

AI & data processing

What AI models does Coadan use, and where does my data go?

Coadan uses **Anthropic's Claude API** for document extraction and narrative generation. Document content (loan agreements, financials, etc.) is sent to Anthropic's API for processing. Per Anthropic's commercial API terms, **your data is not used to train Anthropic's models**. Anthropic's data processing addendum is available on request.

Are document uploads used to train Coadan's models?

No. Coadan does not train any model on customer data. Extraction prompts and templates are general-purpose and were developed against synthetic test loans.

Can I review what was extracted before it's saved?

Yes. Every document upload presents a review screen showing every extracted field. Users approve or edit before extraction is committed to the loan record. **Extraction is never silently overwritten**: every value is editable and any field can be corrected at any time.

Does AI ever auto-act without user review?

No. **AI drafts. Humans approve.** Quarterly narratives, covenant tests, watchlist flags: all are presented for review before they reach a stakeholder. Coadan never sends emails, draws future funding, or modifies external systems on its own behalf.

Compliance & audit

What compliance certifications do you hold?

Coadan is **pre-SOC 2**. The underlying infrastructure (Supabase, AWS, Anthropic, Cloudflare) is SOC 2 Type II certified. Coadan's own SOC 2 audit is planned; timeline will be confirmed once an auditor is engaged. Infrastructure provider compliance reports can be shared under NDA.

Is there an audit trail?

Critical events (covenant test results, balance changes, alerts) are logged today with user, timestamp, and prior value. **Comprehensive write-level audit logging across all tables is on the near-term roadmap.** Customers requiring full audit logging from day one should raise this in pilot discussions so we can scope it into their timeline.

What's your incident response posture?

Customer notification within **72 hours** of any confirmed data incident affecting that customer's data. Founder is the direct escalation contact (alex@coadan.com).

Do you handle GDPR / CCPA / consumer data?

Coadan handles commercial loan data, not consumer financial data. We do not collect PII on borrowers beyond what's in standard loan documentation (entity names, guarantor identities). Where customer-uploaded documents contain incidental personal data, we treat it under the same protection standard as the rest of the document and do not process it separately.

Operational

What's your uptime posture?

Coadan inherits the uptime SLA of Supabase (99.95% on the Pro tier) and AWS. Coadan does not yet publish an independent SLA. As Coadan signs paying customers, an SLA will be added to commercial agreements.

How do backups work?

Database is backed up nightly via Supabase, with point-in-time recovery available for the last 7 days, retained for 30 days. Document storage is backed by S3 versioning. **Restoration to a specific timestamp is available on request.**

Can I export everything?

Yes. **Full data export** (loans, documents, financials, narratives, audit trail) is available in JSON plus a folder of original document files, on 24-hour notice. No vendor lock-in.

Who answers if something breaks?

Alex Gottlieb (founder) is the direct contact for any escalation. **alex@coadan.com** for incidents. Response within 4 business hours during the working week, best-effort outside.

Need more detail?

This document summarizes current posture and roadmap. For specifics on infrastructure providers' compliance posture, data processing agreements, or to respond to a security questionnaire before a pilot, contact **alex@coadan.com**.