Corduroy Intelligence — Security & Privacy Summary

Last updated: 2025-12-12

Our Commitment

Corduroy treats all customer data as confidential by default. Our Master Service Agreement contractually prohibits using client data for model training or any third-party purpose — data is accessed solely for service delivery. Upon engagement termination, all client data is deleted within 60 days (MSA §§ 5.1–5.4).

Infrastructure & Hosting

Provider	Role	Certifications	Encryption	Trust Page
Hetzner	Compute infrastructure	ISO 27001:2022	TLS in transit; corduroy-managed at rest	hetzner.com/security
Vercel	Application hosting & edge delivery	SOC 2 Type 2, ISO 27001:2022, PCI DSS v4.0	AES-256 at rest, TLS 1.3 in transit	security.vercel.com
Supabase	Database, auth & storage	SOC 2 Type 2	AES-256 at rest, TLS in transit	supabase.com/security

> **Note on encryption at rest:** Persistent customer data (database contents, files, credentials) resides in Supabase and Vercel, both of which enforce AES-256 encryption at rest. Hetzner provides compute infrastructure where data is encrypted in transit and can be encrypted at rest via corduroy-managed disk encryption where appropriate.

Tenant Isolation & Architecture

- **Per-customer project environments** — dedicated database, application instances and isolated network and API endpoints per engagement
- **Cloudless or Self-hosted options available** — Platform can be deployed on bare metal servers in Hetzner datacenters or within customer owned/controlled infrastructure for customers requiring full infrastructure isolation.
- **Managed Supabase** — per-project database isolation with Row Level Security (RLS) enforced at the database layer
- **Network controls** — Hetzner Cloud Firewalls, private networking, and IP allowlisting restrict access to production infrastructure. Cloudflare for WAF, DDoS, and bot protection.

Data Residency & Compliance

- **Hetzner** — data centers in Germany, Finland, and the US; Corduroy deployments use the most appropriate region based on customer location by default.

- **Vercel & Supabase** — region-selectable deployments (EU or US) per customer requirement
- **GDPR** — data processing agreements available from all three providers
- **CCPA/CPRA** — supported by Vercel and Supabase

Data Handling Practices

- Client data used solely for service delivery — never for training or third-party benefit
- Data retained only during active engagement; deleted within 60 days of termination
- All API keys, credentials, and secrets encrypted at rest and in transit
- DDoS protection across all tiers: Hetzner automatic mitigation, Vercel edge protection, Supabase edge protection and Cloudflare

---

For any security or compliance oriented requests, contact **security@corduroyintelligence.com**.

Vendor trust centers: Hetzner · Vercel · Supabase