

Vendor Risk Assessment — Groq

Vendor Risk Assessment: Groq Inc.

Vendor Name: Groq Inc.

Service Provided: AI-driven financial transaction categorization.

Assessment Date: April 13, 2026

Status: Approved (with mitigations)

1. Data Processing Context

- **Data Category Shared: Restricted** (Sanitized transaction strings only).
- **Sensitive Data Stripping:** Before transfer, Orbiq's local sanitization layer removes **Names, Account Numbers, and Exact Locations**.
- **Data Transferred:** Merchant category keywords, rounded transaction amounts, and transaction types.

2. Technical Safeguards & Certifications

- **Security Certification:** Groq maintains **SOC 2 Type II** compliance (verified for 2024 and 2025 reporting periods), ensuring high standards for security, availability, and confidentiality.
- **Infrastructure:** Services are hosted on **GroqCloud** within the United States.
- **Encryption:** All data in transit to Groq is protected via **TLS 1.2+**.

3. Contractual & Regulatory Controls

- **Data Processing Addendum (DPA):** FINARO CAPITAL SERVICES INC. (operator of Orbiq) has executed Groq's DPA, which incorporates **Standard Contractual Clauses (SCCs)** to govern the cross-border transfer of data from Canada to the US.
- **Zero Data Retention (ZDR):** Orbiq has explicitly enabled **ZDR mode** in the Groq Cloud Console. This ensures that prompts and outputs are processed in RAM and are **not persisted** for system reliability or abuse monitoring.
- **PIPEDA Accountability:** Under PIPEDA Section 4.1.3, FINARO CAPITAL SERVICES INC. (as data controller for Orbiq) remains accountable for the protection of data sent to Groq. This VRA serves as evidence of that oversight.

4. Residual Risk & Mitigations

Risk Factor	Assessment	Orbiq Mitigation
US CLOUD Act	US authorities may legally compel access to data on US soil.	Prompt Sanitization: The data sent is de-identified, making it useless to authorities without the local Orbiq database.
Data Residency	Data leaves Canada for processing in the US.	Disclosure & Consent: Users are notified of US processing during onboarding and in the Privacy Policy.
Model Leakage	Risk of prompts being used for global model training.	ZDR Policy: Groq's contractual ZDR policy explicitly forbids training on API inference data.

5. Continuous Oversight Plan

- **Annual Review:** The Privacy Officer will review Groq's latest SOC 2 report annually.
- **ZDR Verification:** Quarterly check of the Groq Console to ensure the ZDR toggle remains active.
- **Audit Trail:** Maintain logs in Axiom of every API call made to Groq for usage and anomaly tracking.