Feel free to use as is or amend to suit your firm

The Sovereign Audit Checklist

Since you've now publicly committed to this, here is the structure for the **Sovereign Audit**. This is designed to be a "trap" for SaaS vendors—when a lawyer sends this to their Adobe or Westlaw rep, the vague answers they get back will prove your point for you.

---

1. Data Ingestion & Model Training

- **[ ]** Does the vendor utilize "Service Improvement" or "Safety Monitoring" as a legal basis to allow human reviewers or automated systems to access raw prompt data?
- **[ ]** Are inputs (client data) used in any capacity—even de-identified—to fine-tune weights or train subsequent model iterations?
- **[ ]** Can the vendor provide a technical guarantee that data is **ephemeral** and not cached on intermediate "Safety Layers" outside the primary database?

2. Sub-Processor Transparency

- **[ ]** Does the SaaS provider utilize a "Model API" (e.g., OpenAI, Anthropic, Google) to process requests?
- **[ ]** If yes, does the sub-processor's "Zero Retention" policy actually apply to the *SaaS vendor's* specific tier, or only to enterprise direct-buyers?
- **[ ]** Is the data encrypted in transit *and* at rest with **Client-Held Keys (BYOK)**, or does the vendor hold the master key?

3. The "Heppner" Expectation Test

- **[ ]** Does the vendor reserve the right to disclose data to "Regulatory or Governmental Authorities" without a warrant, based on their own internal TOS violations?
- **[ ]** Does the platform's technical architecture allow for a "Physical Air-Gap" or is it a multi-tenant cloud environment where data co-mingles on the same server?