Top 20 Data Privacy Questions & Answers

---

1. “How do you prevent unauthorized access to our data?”

Answer:
All requests require a **hashed API key** unique to each partner tenant. Only authenticated requests are processed, ensuring no unauthorized access.

---

2. “Can other companies see our data?”

Answer:
No. Each company receives a **dedicated tenant_id** with fully isolated configuration, FAQs, RAG documents, and interaction logs. There is **zero cross-tenant data sharing**.

---

3. “How is admin access protected?”

Answer:
The **admin dashboard** uses **TOTP-based two-factor authentication**, providing strong protection against unauthorized access.

---

4. “Can the AI answer questions about other companies?”

Answer:
No. Tenants are configured with an **allowed ticker list**. Queries about unapproved tickers are automatically rejected.

---

5. “How can we control what the AI says on sensitive topics?”

Answer:
You can define **authoritative answers** via the **custom FAQ system**, ensuring that sensitive queries always return pre-approved responses.

---

6. “What if someone tries to trigger an easter egg or off-script response?”

Answer:
Easter egg triggers are fully configurable, so you can route queries to **pre-approved canned responses** only. Unapproved triggers are ignored.

---

7. “Which documents are used to generate AI responses?”

Answer:
You **control document ingestion**. Only the documents you index are available for retrieval in the RAG system. No outside content is accessed.

---

8. “Could documents from other companies leak into our AI responses?”

Answer:
No. Documents are **chunked, embedded, and stored per tenant**, preventing cross-contamination between tenants.

---

9. “How can we verify the source of each answer?”

Answer:
All AI responses include **source attribution** with citations to the originating document, ensuring transparency and auditability.

---

10. “Are all interactions logged?”

Answer:
Yes. Every query and response is logged in the **partner_interactions table** with timestamps, maintaining a **complete audit trail**.

---

11. “Can we review past conversations?”

Answer:
Yes. **Full conversation history** is available, so your team can audit all investor/shareholder interactions at any time.

---

12. “Do we have visibility into usage?”

Answer:
Yes. The **admin analytics dashboard** provides real-time metrics on usage patterns, query types, response quality, and trends.

---

13. “How do you ensure financial data is accurate?”

Answer:
Core financial data comes from **authoritative sources** only, like **SEC EDGAR filings and regulated market data providers**. No AI hallucinations are used for critical data.

---

14. “Can the AI make up financial information?”

Answer:
No. Responses are **grounded in retrieved RAG documents** and official data APIs. There is **no generation of unverified numbers**.

---

15. “Is there a risk of abuse or scraping?”

Answer:
We implement **rate limiting** at **30 requests per minute per tenant** and monitor usage for anomalies to prevent scraping or abuse.

---

16. “Can we monitor usage for suspicious activity?”

Answer:
Yes. Each tenant is monitored individually, and anomalies are flagged in real-time to prevent misuse.

---

17. “Can the AI be customized to match our brand?”

Answer:
Absolutely. Tenants can configure **custom branding**, including company name, contact info, and response tone.

---

18. “Can we control how the AI talks?”

Answer:
Yes. You can adjust **response tone**, level of detail, and even enforce a **controlled vocabulary** via the FAQ system to stay consistent with company-approved terminology.

---

19. “Who decides what queries are allowed?”

Answer:
You do. **Content guardrails** let each tenant define allowed tickers, pre-approved responses, and restricted topics. Anything outside this scope is rejected.

---

20. “How is all this compliant and auditable?”

Answer:
Everything—queries, responses, sources, and usage—is logged and attributed. The **dashboard provides real-time analytics**, and all data is **isolated per tenant**, giving you a complete **audit trail for regulatory and internal compliance**.