

Vendor Due Diligence Questions



Security & Compliance Essentials

Data Security

1. What security certifications do you maintain? (SOC 2 Type II, ISO 27001, etc.)
2. Where is our data stored and who has access?
3. How do you handle data breaches? (Notification timeline? Insurance?)

Compliance & Privacy

5. What privacy laws do you comply with? (GDPR, CCPA, HIPAA, etc.)
6. Can you provide your Data Processing Agreement (DPA)?
7. What's your data retention and deletion policy after contract ends?

Operational & Risk

8. What's your uptime guarantee (SLA)?
9. What's your disaster recovery and backup process?
10. Do you have cyber liability insurance?

Contracting Red Flags

- Vendor refuses to answer security questions or provide certifications
- Vague answers about data location, access, or breach response
- No SLA, uptime guarantee, or liability limits defined
- Unwilling to sign a DPA or BAA when required
- No documented data export or deletion process at contract end
- Dismissive about compliance requirements for your industry

Key Takeaway

Get answers in writing. Don't rely on sales conversations. Have legal review their standard terms before signing.

Questions? Ready to evaluate your vendor agreements?

This is educational, not legal advice. For guidance on your specific situation, let's talk.

