

AI Compliance Readiness Checklist

For Contractors Using AI Answering Services

DevHouse AI | 2026

Why This Matters

Your AI answering service handles customer calls, collects personal information, and books appointments. Contractors using AI must verify their provider meets basic security and compliance standards.

1. Data Protection

- Is call data encrypted in transit (TLS 1.3)?
- Is stored data encrypted at rest (AES-256)?
- Who owns the call recordings and transcripts?
- Is data stored in US-only data centers?
- Can you export/delete your data on request?

2. Access Control

- Multi-factor authentication for admin access?
- Role-based access (who can see what)?
- Audit logs of all system access?
- Employee background checks?

3. AI Security

- Tested against prompt injection attacks?
- Input validation and sanitization?
- Output filtering for sensitive data?
- Regular third-party security audits?

4. Compliance

- GDPR compliant (if you have EU customers)?
- CCPA compliant (California customers)?
- TCPA compliant (SMS/text regulations)?
- HIPAA-aware (for medical-adjacent trades)?

5. Business Continuity

- Uptime SLA (99.9%+)?
- Backup and disaster recovery tested?
- Data retention policy documented?

- Incident response plan with notification?

Scoring

Count your checkmarks:

- 20-25 ■: Excellent — your provider takes security seriously
- 15-19 ■: Good — some gaps to address
- 10-14 ■: Fair — significant risk exposure
- Under 10 ■: Poor — consider switching providers

DevHouse AI Security Summary

What we do to protect your business:

- Zero data sharing: Your call data never trains third-party AI models
- US-only infrastructure: All data stays domestic
- Quarterly penetration testing: External security firm audits our systems
- Prompt injection hardened: Avery has been tested against adversarial inputs
- Instant data deletion: Request deletion, data is gone in 24 hours
- No subcontractor access: Only DevHouse AI employees handle your account

Next Steps

1. Score your current provider using this checklist
2. Request their security documentation
3. Book a DevHouse AI security review

Book: <https://www.devhouseai.com/book-strategy-call>

Call: (929) 407-3669

DevHouse AI LLC | hello@devhouseai.com | <https://www.devhouseai.com>