AI Vendor Checklist

25 questions to ask before any real customer information goes in.

Vendor: _____

Product and plan: _____

Date asked: _____

Get the important answers in writing. Under PIPEDA you remain responsible for personal information you hand to a service provider. These are buyer questions, not a list of legal requirements for every business.

Data and privacy

- ☐ 1. Who is the legal provider, and who do we contact for support and privacy questions?
- ☐ 2. What exact business function is in scope, and what is out of scope?
- ☐ 3. What personal or sensitive information will the system process?
- ☐ 4. Which AI models and subcontractors (subprocessors) are involved, and can you name them in writing?
- ☐ 5. Where are transcripts, recordings and logs stored and processed?
- ☐ 6. Do you use our content or our customers' content to train or improve your models? Can that be switched off in the contract?
- ☐ 7. How long are inputs and outputs kept, and can we set the retention period?
- ☐ 8. Can we export and delete our records, and what happens to backups?
- ☐ 9. What do you do if you receive a legal request for our data or have a breach, and how fast do you tell us?

Security and permissions

- [ ] 10. Who can access the admin portal, and is multi-factor authentication available?
- [ ] 11. What access does the system need to our other software? Can write access be turned off?
- [ ] 12. Which actions need a person's approval before they happen?
- [ ] 13. Is every action logged with who or what did it, when, and the result?
- [ ] 14. How do you defend against prompt injection, such as an email or web page containing instructions?
- [ ] 15. How do we stop the system immediately if something goes wrong?

Performance

- [ ] 16. What happens if the AI service, the phone line or our CRM goes down?
- [ ] 17. Which languages, accents and features have you actually tested?
- [ ] 18. Can it show where an answer came from and say when it does not know?
- [ ] 19. How are wrong answers corrected, and by whom?

Cost

- [ ] 20. How are minutes, messages, usage, phone numbers and overages billed?
- [ ] 21. What is the full one-time cost: setup, integration, migration, training?
- [ ] 22. Who maintains the prompts, policies, knowledge base and integrations, and is that included?

Exit

- [ ] 23. What is the cancellation term, what export format do we get, and can we keep our phone number?
- [ ] 24. Can we pilot first with test data or properly de-identified data?
- [ ] 25. If you shut down or are acquired, what happens to our data and our setup?

Based on the Office of the Privacy Commissioner of Canada's guidance on assessing third-party service providers (September 2026) and Canadian Centre for Cyber Security guidance. General information, not legal advice. Reviewed 2026-11-23. More: vortio.com/resources/ai-toolkit/pilot-guide