
Vendor due-diligence questionnaire

25 questions to send any legal AI vendor before you upload client data. PDF, English and French.

Vendor: _____ Date: _____ Reviewed by: _____

Data storage

1. In which country and data centre are our documents, prompts, outputs and backups stored?

.....
2. Can we contractually fix storage in Switzerland?

Where the AI runs / sub-processors

3. In which countries do the AI models process our prompts, including fallback or peak-load routing?

.....
4. Please provide the full sub-processor list with locations, and how we are notified of changes.

US Cloud Act exposure

5. Is your company or any sub-processor in the processing chain a US company or a subsidiary of one?

.....
6. How would you respond to a foreign government request for our data, and will you notify us?

Art. 321 SCC auxiliary terms

7. Will you contractually accept auxiliary-person (Hilfsperson) status under Art. 321 SCC and pass it to sub-processors?

.....
8. Who at your company or at sub-processors can access our content in clear text?

revFADP / GDPR processing agreement

9. Please send your DPA. Does it reference the Swiss revFADP as well as the GDPR?

10. Which transfer mechanism covers any processing outside Switzerland/EEA?

No training on customer data

11. Is it contractually excluded that our data trains or fine-tunes any model, including the model providers' models?

12. What is retained by model providers (abuse monitoring, logs), and for how long?

ISO 27001 / SOC 2

13. Please send your current ISO 27001 certificate and scope, or SOC 2 Type II report.

14. When was your last independent penetration test?

General and contractual

15. Which legal entity contracts with us, and under which law and jurisdiction?

16. Can we run a pilot with non-confidential data only?

17. How long are documents, prompts and outputs retained, and can we set retention?

18. How are deletion requests handled, including backups and model-provider logs?

19. What is your incident notification time and process?

20. Is there human review of our content for quality or abuse monitoring? By whom and where?

21. Can we restrict which models or features (e.g. web search, external connectors) are used?

22. Do you offer audit rights or independent assessments to customers?

23. What is your liability cap for data incidents and for errors in AI-generated actions?

24. How do you notify us of changes to sub-processors, hosting or models?

25. How do you meet your obligations under the EU AI Act as a provider?

reflect vendors' public statements on the date checked. SecretSafe is an independent project; no legal services are offered through this site. No vendor pays for inclusion or scores.