

Questionnaire de due diligence fournisseur

25 questions à envoyer à tout fournisseur d'IA juridique avant de lui confier des données clients. PDF, français et anglais.

Fournisseur : _____ Date : _____ Revu par : _____

Stockage des données

1. Dans quel pays et quel centre de données nos documents, requêtes, résultats et sauvegardes sont-ils stockés ?

2. Pouvons-nous fixer contractuellement le stockage en Suisse ?

Où tourne l'IA / sous-traitants

3. Dans quels pays les modèles d'IA traitent-ils nos requêtes, y compris en cas de repli ou de pic de charge ?

4. Merci de fournir la liste complète des sous-traitants avec leur localisation et la procédure de notification des changements.

Exposition au Cloud Act

5. Votre société ou un sous-traitant de la chaîne de traitement est-il une société américaine ou la filiale d'une telle société ?

6. Comment répondriez-vous à une demande d'une autorité étrangère portant sur nos données, et nous en informeriez-vous ?

Clauses d'auxiliaire art. 321 CP

7. Acceptez-vous contractuellement le statut d'auxiliaire au sens de l'art. 321 CP et le répercutez-vous sur vos sous-traitants ?

8. Qui, chez vous ou chez vos sous-traitants, peut accéder à nos contenus en clair ?

Contrat de sous-traitance nLPD / RGPD

9. Merci de nous transmettre votre DPA. Mentionne-t-il la nLPD suisse en plus du RGPD ?

10. Quel mécanisme de transfert couvre un éventuel traitement hors de Suisse/EEE ?

Pas d'entraînement sur les données

11. Est-il contractuellement exclu que nos données entraînent ou affinent un modèle, y compris ceux des fournisseurs de modèles ?

12. Que conservent les fournisseurs de modèles (surveillance des abus, journaux), et combien de temps ?

ISO 27001 / SOC 2

13. Merci de nous transmettre votre certificat ISO 27001 en vigueur et son périmètre, ou votre rapport SOC 2 Type II.

14. Quand a eu lieu votre dernier test d'intrusion indépendant ?

Questions générales et contractuelles

15. Quelle entité juridique contracte avec nous, sous quel droit et quel for ?

16. Pouvons-nous mener un pilote uniquement avec des données non confidentielles ?

17. Combien de temps les documents, requêtes et résultats sont-ils conservés, et pouvons-nous fixer la durée ?

18. Comment les demandes de suppression sont-elles traitées, y compris pour les sauvegardes et les journaux des fournisseurs de modèles ?

19. Quel est votre délai et votre procédure de notification des incidents ?

20. Nos contenus font-ils l'objet d'un contrôle humain (qualité, surveillance des abus) ? Par qui et où ?

21. Pouvons-nous limiter les modèles ou fonctions utilisés (p. ex. recherche web, connecteurs externes) ?

22. Offrez-vous des droits d'audit ou des évaluations indépendantes aux clients ?

23. Quel est votre plafond de responsabilité pour les incidents de données et les erreurs d'actions générées par l'IA ?

24. Comment nous informez-vous des changements de sous-traitants, d'hébergement ou de modèles ?

25. Comment remplissez-vous vos obligations de fournisseur au titre de l'AI Act européen ?

À titre informatif uniquement, ne constitue pas un avis juridique. Les résultats reflètent les déclarations publiques des fournisseurs à la date de vérification et nos règles de notation. Vérifiez vous-même les contrats avant d'utiliser un outil avec des données clients. À titre informatif uniquement, ne constitue pas un avis juridique. Les notes reflètent les déclarations publiques des fournisseurs à la date de vérification. SecretSafe est un projet indépendant ; aucun service juridique n'est offert via ce site. Aucun fournisseur ne paie pour figurer ou pour sa note.