

Checklist de due diligence fournisseur IA

Treize questions à passer en revue avec tout fournisseur avant de lui confier des données confidentielles. Consignez la réponse et la date en regard de chacune.

Passez-les dans l'ordre. A, B et C portent sur le fournisseur. D porte sur la maîtrise qui vous reste. E porte sur vous.

A · STATUT JURIDIQUE ET CONTRAT

1. Le fournisseur accepte-t-il le statut de sous-traitant au sens de l'article 28 du RGPD, et signe-t-il un contrat de sous-traitance ?

Se rattache à : RGPD, article 28(3) : le traitement par un sous-traitant est régi par un contrat qui définit l'objet, la durée, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées.

Mauvaise réponse : « *Nous ne traitons pas de données personnelles.* » *Un dossier client, un ticket de support ou un fil d'emails en contient par construction.*

Réponse	Date
---------	------

2. La liste des sous-traitants ultérieurs est-elle publiée, avec information préalable et droit d'opposition avant toute modification ?

Se rattache à : RGPD, articles 28(2) et 28(3)(d) : le sous-traitant ne recrute un autre sous-traitant qu'avec autorisation, et informe le responsable du traitement de tout changement prévu afin de lui permettre de s'y opposer.

Mauvaise réponse : *Pas de liste, une liste « communiquée sur demande », ou une liste modifiable sans préavis.*

Réponse	Date
---------	------

3. Le contrat oblige-t-il le fournisseur à vous notifier une violation assez vite pour que vous teniez votre propre délai de 72 heures ?

Se rattache à : RGPD, article 33(1) : le responsable du traitement notifie l'autorité de contrôle dans les 72 heures après avoir pris connaissance de la violation. Article 33(2) : le sous-traitant notifie le responsable dans les meilleurs délais. « Dans les meilleurs délais » n'est pas un chiffre : mettez-en un au contrat.

Mauvaise réponse : « *Dans les meilleurs délais* » sans nombre d'heures, ou une notification une fois seulement que l'enquête interne du fournisseur est close.

Réponse	Date
---------	------

B · LOCALISATION ET ISOLATION

4. Où les données sont-elles stockées et, question distincte, où l'inférence est-elle exécutée ?

Se rattache à : Deux questions différentes, deux réponses différentes. Le chapitre V du RGPD porte sur le traitement, et un appel de modèle est un traitement : un stockage dans l'UE avec une inférence via une API hors UE constitue un transfert.

Mauvaise réponse : *Une seule réponse pour les deux, ou « nos serveurs sont en Europe » sans un mot sur le fournisseur du modèle.*

Réponse	Date
---------	------

5. Si des données sortent de l'UE, sur quelle base juridique, et le fournisseur ou ses sous-traitants sont-ils soumis à une législation extraterritoriale ?

Se rattache à : RGPD, chapitre V (articles 44 à 49) : décision d'adéquation, clauses contractuelles types accompagnées d'une analyse d'impact du transfert, ou dérogation. Un fournisseur soumis au CLOUD Act américain peut se voir ordonner de produire les données qu'il détient, quel que soit leur lieu de stockage.

Mauvaise réponse : « *Nous utilisons les clauses contractuelles types* » sans analyse d'impact du transfert derrière.

Réponse	Date
---------	------

6. Dans une architecture mutualisée, qu'est-ce qui sépare vos fichiers de ceux d'un autre client : un identifiant applicatif, ou une isolation d'infrastructure ?

Se rattache à : RGPD, article 32 (sécurité du traitement) et article 5(1)(f) (intégrité et confidentialité). Demandez une réponse en termes d'architecture, et demandez ce qu'atteindrait un point d'entrée mal configuré.

Mauvaise réponse : « *Chaque client a son propre espace* » sans description de ce qui fait tenir la frontière.

Réponse	Date
---------	------

C · CONFIDENTIALITÉ ET ENTRAÎNEMENT

7. Vos données servent-elles à entraîner, spécialiser ou évaluer un modèle, y compris sous forme agrégée ou anonymisée, et est-ce une clause du contrat ou une politique ?

Se rattache à : RGPD, article 5(1)(b) (limitation des finalités) et article 28(3)(a) : le sous-traitant agit uniquement sur instruction documentée. Une politique de confidentialité se modifie unilatéralement ; une clause contractuelle, non.

Mauvaise réponse : « *Nous n'entraînons pas sur les données clients* », écrit sur une page de politique plutôt que dans le contrat.

Réponse	Date
---------	------

8. Qui, chez le fournisseur, peut techniquement ouvrir vos données, sous quel contrôle, et quels journaux d'accès pouvez-vous consulter ?

Se rattache à : RGPD, article 28(3)(b) (engagement de confidentialité), article 32(4) (toute personne agissant sous l'autorité du sous-traitant ne traite que sur instruction) et article 32 (capacité à démontrer la sécurité). Support, ingénierie et sous-traitants sont trois réponses différentes.

Mauvaise réponse : « *Seul le personnel autorisé* », sans procédure nommée ni journal que vous puissiez lire.

Réponse	Date
---------	------

9. Quelle est la durée de conservation et, à la fin du contrat : suppression sous quel délai, avec quelle attestation, et qu'advient-il des sauvegardes et des journaux de prompts ?

Se rattache à : RGPD, article 5(1)(e) (limitation de la conservation) et article 28(3)(g) (effacer ou renvoyer les données au terme de la prestation). Les journaux de prompts et de réponses sont la copie que tout le monde oublie.

Mauvaise réponse : *La suppression du compte sans un mot sur les sauvegardes, ou des journaux conservés « à des fins de sécurité » sans limite.*

Réponse	Date
---------	------

D · MAÎTRISE ET RÉVERSIBILITÉ

10. Pouvez-vous récupérer toutes vos données et tous vos documents dans un format exploitable, sans l'aide du fournisseur, et sous quel délai contractuel ?

Se rattache à : Data Act (règlement (UE) 2023/2854), chapitre VI, applicable depuis le 12 septembre 2025 : changement de fournisseur de service de traitement de données, avec une durée de transition maximale et un export dans un format structuré, couramment utilisé et lisible par machine. Les frais de changement, y compris les frais de sortie des données, sont interdits à partir du 12 janvier 2027.

Mauvaise réponse : *Un export livré sous forme de PDF, ou qui passe par un ticket de support et un délai non précisé.*

Réponse	Date
---------	------

11. Le fournisseur documente-t-il les limites du système et les cas exigeant une vérification humaine, sous une forme que vous puissiez lui opposer ?

Se rattache à : Les articles 13 et 14 du règlement sur l'IA (notice d'utilisation, contrôle humain) s'imposent aux fournisseurs de systèmes à haut risque. Depuis l'AI Omnibus, ces obligations s'appliquent au 2 décembre 2027 pour les systèmes de l'annexe III. Posez la question maintenant : cette documentation prend plus de temps à produire que le contrat à signer.

Mauvaise réponse : *Des taux de précision sans jeu de test décrit, ou « le système est fiable à 99 % » sans nommer une seule classe d'erreur.*

Réponse	Date
---------	------

12. Le système peut-il être déployé sur votre propre infrastructure et, si non, pour quelle raison technique ?

Se rattache à : Aucune réglementation ne l'exige. La réponse vous dit ce qu'est réellement l'architecture, et c'est la seule question de cette liste dont la réponse supprime les questions 4, 5, 6 et 8 au lieu de les documenter.

Mauvaise réponse : *« Ce n'est pas ainsi que notre produit fonctionne », sans raison technique derrière.*

Réponse	Date
---------	------

E · VOTRE PROPRE OBLIGATION

13. Quelles obligations de transparence de l'article 50 votre contrat met-il à votre charge, et les tenez-vous ?

Se rattache à : Article 50 du règlement sur l'IA, applicable depuis le 2 août 2026. Le fournisseur doit faire en sorte que les personnes sachent qu'elles interagissent avec un système d'IA (50(1)) et marquer les contenus de synthèse dans un format lisible par machine (50(2)) ; les systèmes génératifs déjà sur le marché avant le 2 août 2026 ont jusqu'au 2 décembre 2026 pour ce marquage. En tant que déployeur, vous portez le 50(3) (reconnaissance des émotions et catégorisation biométrique) et le 50(4) (révélation des hypertrucages, et mention des textes générés par IA publiés pour informer le public sur des questions d'intérêt public sans relecture humaine).

Mauvaise réponse : *Un contrat muet, ce qui ne déplace pas pour autant les obligations du déployeur.*

Réponse	Date
---------	------