AI Vendor Due Diligence Checklist

Thirteen questions to work through with any vendor before handing it confidential data. Record the answer and the date next to each one.

> Work through them in order. A, B and C are about the vendor. D is about how much control you keep. E is about you.

A · LEGAL STATUS AND CONTRACT

1. Does the vendor accept processor status under Article 28 of the GDPR, and will it sign a data processing agreement?

Hooks to: GDPR Article 28(3): processing by a processor is governed by a contract setting out the subject matter, duration, nature and purpose of the processing, the type of personal data and the categories of data subjects.

Bad answer: *"We don't process personal data." A client file, a support ticket or an email thread contains it by construction.*

Answer	Date

2. Is the list of sub-processors published, with prior notice and a right to object before any change?

Hooks to: GDPR Articles 28(2) and 28(3)(d): a processor engages another processor only with authorisation, and must inform the controller of intended changes so that the controller can object.

Bad answer: *No list, a list "available on request", or a list that can change without notice.*

Answer	Date

3. Does the contract require the vendor to notify you of a breach fast enough for you to meet your own 72-hour deadline?

Hooks to: GDPR Article 33(1): the controller notifies the supervisory authority within 72 hours of becoming aware. Article 33(2): the processor notifies the controller without undue delay. "Without undue delay" is not a number, so put one in the contract.

Bad answer: *"Without undue delay" with no hours attached, or notification only once the vendor's own investigation is closed.*

Answer	Date

B · LOCATION AND ISOLATION

4. Where is the data stored and, as a separate question, where is inference executed?

Hooks to: Two different questions with two different answers. Chapter V of the GDPR bears on the processing, and a model call is processing: EU storage with inference through a non-EU API is a transfer.

Bad answer: *One answer covering both, or "our servers are in Europe" with not a word about the model provider.*

Answer	Date

5. If data leaves the EU, on what legal basis, and are the vendor or its sub-processors subject to extraterritorial legislation?

Hooks to: GDPR Chapter V (Articles 44 to 49): adequacy decision, standard contractual clauses backed by a transfer impact assessment, or a derogation. A vendor subject to the US CLOUD Act can be ordered to produce the data it holds, wherever that data is stored.

Bad answer: *"We use the standard contractual clauses" with no transfer impact assessment behind them.*

Answer	Date

6. In a shared-tenancy architecture, what separates your files from another customer's: an application-level identifier, or infrastructure isolation?

Hooks to: GDPR Article 32 (security of processing) and Article 5(1)(f) (integrity and confidentiality). Ask for the answer in architectural terms, and ask what a misconfigured endpoint would reach.

Bad answer: *"Every customer has their own tenant" with no description of what holds the boundary in place.*

Answer	Date

C · CONFIDENTIALITY AND TRAINING

7. Is your data used to train, fine-tune or evaluate a model, including in aggregated or anonymised form, and is that a contract clause or a policy?

Hooks to: GDPR Article 5(1)(b) (purpose limitation) and Article 28(3)(a): a processor acts only on documented instructions. A privacy policy can be changed unilaterally; a contract clause cannot.

Bad answer: *"We don't train on customer data", written on a policy page rather than in the contract.*

Answer	Date

8. Who at the vendor can technically open your data, under what control, and which access logs can you consult?

Hooks to: GDPR Article 28(3)(b) (confidentiality commitments), Article 32(4) (anyone acting under the processor's authority processes only on instruction) and Article 32 (being able to demonstrate security). Support, engineering and sub-processors are three different answers.

Bad answer: *"Only authorised staff", with no named procedure and no log you can read.*

Answer	Date

9. What is the retention period and, at the end of the contract: deletion within what timeframe, with what attestation, and what becomes of backups and of prompt logs?

Hooks to: GDPR Article 5(1)(e) (storage limitation) and Article 28(3)(g) (delete or return the data at the end of the provision of services). Prompt and completion logs are the copy everyone forgets.

Bad answer: *Account deletion with not a word about backups, or logs kept "for security purposes" with no limit.*

Answer	Date

D · CONTROL AND REVERSIBILITY

10. Can you retrieve all your data and documents in a usable format, without the vendor's help, and within what contractual timeframe?

Hooks to: Data Act (Regulation (EU) 2023/2854), Chapter VI, applicable since 12 September 2025: switching between data processing services, with a maximum transition period and an export in a structured, commonly used, machine-readable format. Switching charges, including data egress fees, are prohibited from 12 January 2027.

Bad answer: *An export delivered as a bundle of PDFs, or one that goes through a support ticket and an unspecified delay.*

Answer	Date

11. Does the vendor document the system's limits and the cases requiring human verification, in a form you can hold it to?

Hooks to: Articles 13 and 14 of the AI Act (instructions for use, human oversight) bind providers of high-risk systems. Since the AI Omnibus, those obligations apply from 2 December 2027 for Annex III systems. Ask now: that documentation takes longer to produce than the contract takes to sign.

Bad answer: *Accuracy figures with no test set described, or "the system is 99% accurate" without naming a single class of error.*

Answer	Date

12. Can the system be deployed on your own infrastructure and, if not, for what technical reason?

Hooks to: No regulation requires it. The answer tells you what the architecture actually is, and it is the only question on this list whose answer removes questions 4, 5, 6 and 8 instead of documenting them.

Bad answer: *"That's not how our product works", with no technical reason behind it.*

Answer	Date

E · YOUR OWN OBLIGATION

13. Which of the Article 50 transparency obligations does your contract place on you, and are you meeting them?

Hooks to: Article 50 of the AI Act, applicable since 2 August 2026. The provider must ensure that people know they are interacting with an AI system (50(1)) and mark synthetic content in a machine-readable format (50(2)); generative systems already on the market before 2 August 2026 have until 2 December 2026 for that marking. As the deployer, you carry 50(3) (emotion recognition and biometric categorisation) and 50(4) (disclosing deepfakes, and labelling AI-generated text published to inform the public on matters of public interest without human review).

Bad answer: *A contract that says nothing, which does not move the deployer's obligations off you.*

Answer	Date