

# AI Vendor Due Diligence Checklist

A sequenced checklist for assessing AI vendors, from first engagement through ongoing monitoring. Free resource from AI Act Ready - [aiactready.co.uk/ai-supplier-due-diligence/checklist/](https://aiactready.co.uk/ai-supplier-due-diligence/checklist/)

## Before you engage

- Confirm the vendor's likely EU AI Act role: provider, deployer, importer or distributor.
- Map what data your use case will involve (personal, confidential, regulated).

## Before you sign

- Request certifications: ISO 27001 for security, ISO 42001 for AI management where relevant.
- Request evaluation and bias-testing evidence for the AI system.
- Request the sub-processor list and confirm data flows.
- Confirm the vendor's incident response process and notification SLA.

## Contract terms to include

- Audit rights over the vendor's AI system and processes.
- Transparency commitments matching your own disclosure obligations.
- Incident notification timeframes.
- Clear allocation of EU AI Act roles and responsibilities between buyer and supplier.

## Ongoing monitoring

- Reassess at least annually.
- Reassess immediately after any material change to the vendor's AI system or a reported incident.
- Keep evidence of each review for your own compliance records.

## Red flags

- No documentation available on request.
- Vague or evasive answers on data sourcing.
- No human-oversight design in the product.
- Refusal to share evaluation or bias-testing results.