

Checklist: AI partner questions that protect your data

Data security and privacy

- How is my data encrypted both in transit and at rest?
- Who within your organisation has access to my data, and how is this access controlled?
- Is my data ever shared with third parties, including AI model providers, for training purposes?
- Do you comply with GDPR (or other relevant data protection regulations) across all regions you operate in?

Data ownership and control

- Do I retain full ownership of my supply chain data?
- Can I request complete data deletion if I terminate the service?
- How do you ensure my sensitive operational data remains confidential?

Explainability and transparency

- Are all AI outputs traceable and explainable?
- Do you log and document prompts, system flows, and decision points for auditability?
- How can I validate or challenge an AI-generated recommendation (e.g., ETAs, routing decisions)?

Reliability and accountability

- What governance framework is in place to handle AI errors?
- How do you ensure accountability for AI-driven mistakes (e.g., inaccurate ETAs, missed compliance steps)?
- Do you provide human oversight (“human-in-the-loop”) for critical supply chain decisions?

Future-proofing and trust

- How are AI models monitored and updated to remain accurate as market conditions change?
- What safeguards are in place to prevent “hallucinations” or unreliable AI outputs from impacting my operations?
- How do you communicate when the system makes an error, and what remediation process is in place?

