JANUS COMPLIANCE

AI Vendor Due Diligence Checklist

Redacted sample deliverable for buyer review. Not client-specific advice.

Data Handling

• What personal data is sent to the vendor?

• Can the payload be minimised or pseudonymised?

• Does the vendor use customer data for training by default?

Contracts and Transfers

• Is there a DPA?

• Which subprocessors are involved?

• What transfer mechanism applies if data leaves the UK or EEA?

Security and Operations

• What logging and access controls exist?

• Can retention or zero-retention be configured?

• How does the vendor handle incident notification?

Model and Product Risk

• How are hallucinations or unsafe outputs handled?

• Can we configure human review thresholds?

• Is the system explainable enough for the use case?

Exit Risk

• Can data and logs be exported?

• What lock-in exists?

• What is the fallback plan if the vendor changes pricing or terms?

This checklist is a working aid, not legal advice.