

Responsible AI

AI should strengthen human judgement, with clear ownership of data, risk and decisions.

01 / Inventory and purpose

Before an AI use case is adopted, identify its intended purpose, operator, data sources, affected people and decision impact. Assess the applicable AI Act role and risk classification for the concrete system rather than treating every tool as equivalent.

02 / Human oversight and assurance

Set review points for material outputs, test accuracy and failure modes, retain traceability to sources and make escalation possible. Do not put client-confidential information into an AI service without authority, security review and appropriate terms.

03 / Transparency and skills

Provide disclosures when an applicable transparency rule requires them. Support AI literacy for staff and other persons operating AI on our behalf, taking account of their role and context under the amended Article 4. The design should be revisited as the law and system change.

Document status

Original VISIONCYBERX working framework for review. This PDF is not an offer, a signed agreement or evidence of an implemented control. Confirm legal entity details, service scope, commercial terms, annexes and approval before use. A signed engagement document governs.

Official EU references

EU AI Act, Article 4 (consolidated 27 July 2026)

EU AI Act, Article 50 (consolidated 27 July 2026)

GDPR, Article 32