

AI Procurement Evidence Pack + RFP Question Bank

A practical pack for buying and selling AI responsibly. Free resource from AI Act Ready - aiactready.co.uk/ai-procurement/checklist/

Evidence checklist - request before signing

- Risk classification of the AI system (unacceptable / high-risk / limited-risk / minimal-risk)
- Model and training-data documentation
- Security certifications (ISO 27001, SOC 2, etc.)
- ISO 42001 certification status, if any
- DPIA / FRIA status where personal data or fundamental rights are affected
- Incident response process and notification commitments
- Sub-processor / sub-contractor list

RFP question bank

- What is the risk classification of your AI system under the EU AI Act, and why?
- Where does your training data come from, and how is provenance documented?
- What evaluation and bias testing has the model undergone, and how often is it repeated?
- How is human oversight designed into the system?
- What security certifications do you hold?
- Who are your sub-processors, and what data do they receive?
- What is your incident notification process and SLA?
- Which EU AI Act role do you hold for this system (provider, deployer, importer, distributor)?

Red flags - pause or stop the deal

- 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
- No incident response process

Contract pointers

Add warranties on the answers given above, audit rights, transparency commitments, incident notification timeframes, and clear allocation of EU AI Act roles between buyer and supplier.