AI Tool Vendor Assessment Checklist

Complete before approving the tool | Tool: _____ | Vendor: _____ | Date: _____

The list of questions is the author's compilation based on the general structure of the initial question lists of the Polish data protection authority (UODO, 2026), the OWASP Top 10 for LLM Applications 2025 list and the requirements of the AI Act. It is not a template published by any of these bodies, nor legal advice. Official UODO lists: uodo.gov.pl.

First: what is the tool for?

UODO recommends first establishing what problem the tool solves and what data it will work on, and only then assessing compliance. Enter:

Use case	
Department / users	
Data class (green / yellow / red)	
Will personal data be involved?	
Does the result affect decisions about people?	

A. Data and contract

Question for the vendor	Why we ask	Vendor's answer	Rating (OK / ? / NO)
Does the vendor use our data (queries, files) to train models? Can this be switched off, and where is this stated in the contract?	Company data should not feed a model available to others.		
Where is the data processed and stored (country, region)? For how long?	A transfer outside the EEA requires a legal basis.		
Does the vendor provide the ability to delete data and history? Within what period?	Control over the data life cycle.		
Are there company accounts with user management, single sign-on (SSO) and an activity log?	Without this we cannot control access after an employee leaves.		
What happens to the data after the contract ends?	Risk of data remaining with the vendor.		

B. GDPR

Question for the vendor	Why we ask	Vendor's answer	Rating (OK / ? / NO)
Will the vendor sign a data processing agreement (Article 28 GDPR) if we enter personal data?	Without an agreement we do not enter personal data.		
Who are the vendor's sub-processors, and does the vendor publish a list of them?	The processing chain.		

Question for the vendor	Why we ask	Vendor's answer	Rating (OK / ? / NO)
Does the use require a data protection impact assessment (DPIA)? Who will carry it out?	It depends on the scale and type of data; this is determined by the data protection officer or a lawyer.		
Do we have to inform the data subjects that the tool is used?	Information obligations.		

C. Security

Question for the vendor	Why we ask	Vendor's answer	Rating (OK / ? / NO)
Does the vendor hold certificates or reports (e.g. ISO/IEC 27001, SOC 2), and can it share them?	Basic confirmation of security maturity.		
Does the vendor inform customers about incidents? Within what time?	We need to know the time limit in order to meet our own obligations.		
Is data encrypted at rest and in transit?	Minimum standard.		
Does the tool protect against prompt injection and disclosure of information from system prompts? How?	Items on the OWASP Top 10 for LLM Applications 2025 list.		

D. Permissions and integrations (for agentic tools)

Question for the vendor	Why we ask	Vendor's answer	Rating (OK / ? / NO)
Which systems does the tool have access to (email, drives, CRM, finance)? Can the scope be limited to read-only?	OWASP: excessive agency.		
Do actions with external effects (sending an email, a payment, changing data) require human approval?	A person is responsible for the consequences.		
Is there a log of all the agent's actions?	The ability to establish what happened.		
Does the product really work as an agent, or is it a rebranded chatbot or automation?	Gartner describes the phenomenon of "agent washing".		

E. AI Act compliance and liability

Question for the vendor	Why we ask	Vendor's answer	Rating (OK / ? / NO)
Which category does the vendor assign the system to (prohibited, high-risk, limited-risk, minimal-risk)? On what basis?	The company's obligations depend on the use, not only on the tool.		
Will the tool be used for recruitment, evaluation or management of employees?	Such uses may fall within the high-risk area (Annex III). Requires legal consultation.		

Question for the vendor	Why we ask	Vendor's answer	Rating (OK / ? / NO)
Does the tool generate content (images, video, text) published externally? Does it label it in a machine-readable way?	Transparency obligations (Article 50).		
How does the contract allocate liability for the tool's errors? Is there a limit on the vendor's liability?	We are the ones answerable to the client.		

F. Costs and continuity

Question for the vendor	Why we ask	Vendor's answer	Rating (OK / ? / NO)
What is the full cost (licences, usage limits, charges for additional queries)?	Gartner lists unclear costs among the reasons for abandoning AI projects.		
What will we do if the vendor changes the terms or withdraws the product? Can we export our data and configuration?	Risk of vendor lock-in.		

Decision

Decision	☐ Approved ☐ Approved with restrictions ☐ Rejected ☐ To be clarified
Restrictions (data classes, users, scope)	
Assessed by / date	
Date of next review	