

PROCUREMENT CHECKLIST

AI Vendor Selection Checklist

Functional, technical and organisational criteria for a resilient selection decision.

Working template

Version 1.0 | Updated 07/2026

Published by Augmentry

01

Prepare the assessment

Assess evidence rather than claims and involve business, engineering, security, privacy, procurement and governance.

Rating scale

- Met: credible evidence is available
- Partial: gap and action are named
- Open: clarification required before decision
- Not met: risk or exclusion criterion
- Not applicable: document the reason

Assessment details

Provider: [name] | Product: [name/version] | Use case: [purpose] | Assessors: [roles] | Date: [YYYY-MM-DD]

02

1. Need and functional fit

The use case and measurable value are defined.	☐	☐	☐	☐	☐
Limitations and unsuitable uses are documented.	☐	☐	☐	☐	☐
Pilot, acceptance and success criteria are agreed.	☐	☐	☐	☐	☐
Alternatives including self-hosting and non-AI solutions were considered.	☐	☐	☐	☐	☐

03

2. Data and privacy

Data locations, subprocessors and transfers are transparent.	☐	☐	☐	☐	☐
Retention, deletion and use for training or product improvement are controllable.	☐	☐	☐	☐	☐
Data minimisation, tenant isolation and access controls are clear.	☐	☐	☐	☐	☐
Contractual roles and required privacy assessments are understood.	☐	☐	☐	☐	☐

04

3. Information security

A security concept, ownership and relevant evidence are available.	☐	☐	☐	☐	☐
Encryption, identity, logging and vulnerability processes are appropriate.	☐	☐	☐	☐	☐
AI-specific attacks and misuse scenarios are addressed.	☐	☐	☐	☐	☐
Incident channels, response times and responsibilities are contractual.	☐	☐	☐	☐	☐

05

4. Model quality and transparency

Model, version, changes and key dependencies are traceable.	☐	☐	☐	☐	☐
Quality evidence reflects the intended context of use.	☐	☐	☐	☐	☐
Hallucination, bias, robustness and known limitations are disclosed.	☐	☐	☐	☐	☐
Grounding, explainability and human control are technically feasible.	☐	☐	☐	☐	☐

06

5. Governance and the AI Act

Provider, deployer and other possible market roles have been reviewed.	☐	☐	☐	☐	☐
Potential triggers and requirements to review are documented.	☐	☐	☐	☐	☐
Transparency, human oversight and logging are supported.	☐	☐	☐	☐	☐
Changes that may affect regulatory triggers are communicated.	☐	☐	☐	☐	☐

07

6. Operations, cost and exit

Availability, support, capacity and recovery are credible.	☐	☐	☐	☐	☐
Total cost including integration, operations, monitoring and switching is transparent.	☐	☐	☐	☐	☐
Data, prompts, configuration and logs can be exported or deleted.	☐	☐	☐	☐	☐
An exit plan limits uncontrolled provider dependency.	☐	☐	☐	☐	☐

Decision and actions

Criterion / risk	Rating	Action	Owner	Due

Decision: [approve / approve with conditions / further pilot / reject] | Approved by: [role] | Next review: [date]

Sources and legal status

Reviewed on 17 July 2026. The Digital Omnibus has been adopted and signed but has not been published in the Official Journal and is not yet in force. Commission guidelines are non-binding; drafts are additionally preliminary.

1. Regulation (EU) 2024/1689

Binding Official Journal text

<https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=en>

2. Digital Omnibus PE-CONS 30/26

Signed text, not yet in force

<https://data.consilium.europa.eu/doc/document/PE-30-2026-INIT/en/pdf>

3. Procedure status 2025/0359(COD)

Official publication status

<https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2025%2F0359%28COD%29>

4. Commission guidelines on the AI-system definition

Non-binding interpretive aid

<https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application>

5. Commission guidelines on prohibited practices

Non-binding interpretive aid

<https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>

6. Commission guidelines for GPAI providers

Non-binding interpretive aid

<https://digital-strategy.ec.europa.eu/en/policies/guidelines-gpai-providers>

7. Commission guidelines on high-risk systems

Preliminary draft, non-binding

<https://digital-strategy.ec.europa.eu/en/policies/guidelines-ai-high-risk-systems>

Important notice

This non-binding technical assessment and template provides initial orientation. It is not legal advice, a legally binding classification, or a conformity assessment. Privacy, certification and organisation-specific requirements require separate review.



AUGMENTRY

Turn the template into resilient practice.

Augmentry connects AI governance with engineering practice. We support adaptation, technical implementation and adoption across real teams and system landscapes.

Vendor-neutral. Engineering-led. Grounded in practice.

Start an enquiry: augmentry.de/en/contact