

AI-BOK TOOLKIT v1.2

AI Procurement Clauses

Companion to the AI Body of Knowledge v1.2

Jan Willem van Veen · ArchiXL · ai-bok.nl

AI Procurement Clause Set

Nineteen contractual clauses, grouped by topic and tagged with applicable risk band and KA anchor, ready to be lifted into procurement frameworks for AI systems, AI services and AI-using applications. Not legal advice - a structurally complete starting point.

1. Purpose and scope

This clause set is designed to be lifted, with minor adaptation, into procurement frameworks for AI systems, AI services and AI-using applications. Clauses are written in deliberately neutral contract-language form. They are *not* legal advice - every adopter must run them past their own legal counsel. They *are* a structurally complete starting point that an organisation buying AI does not have to assemble from scratch.

Clauses are grouped by topic. Each clause: **purpose, clause text, applicability** (low / medium / high risk band, or specific), **AI-BOK anchor** (which KA the clause leans on for governance follow-through).

2. Definitions

For the purposes of these clauses:

- **AI System** has the meaning given in EU AI Act Article 3(1).
- **AI Model** means the trained algorithm component (e.g., foundation model, classifier, generator).
- **Agent / Agentic AI** means an AI System that autonomously plans, acts and adapts to feedback.
- **Cognition Plane** means the architectural layer governing autonomous reasoning, mandates and authority, as defined in the AI-BOK (Module 1 KA3).
- **NHI** means Non-Human Identity - the credential under which an agentic AI acts.
- **Provider** and **Deployer** have the meanings given in EU AI Act Article 3.

3. Clause set

Clause 3.1 - EU AI Act compliance

Purpose: Establish baseline AI Act conformity expectations from the supplier.

The Supplier represents and warrants that, where the Supplier qualifies as a Provider under the EU AI Act in respect of the AI System(s) provided under this Agreement, the Supplier has carried out the conformity assessment procedure applicable to the relevant risk classification,

maintains the technical documentation required under Annex IV, and registers the system(s) in the EU database where applicable. The Supplier shall provide the Customer with such documentation as the Customer reasonably requires to discharge its own obligations as Deployer.

Applicability: all. Anchor: KA10.

Clause 3.2 - Risk classification and impact assessment

The Supplier shall, on request and on changes to the AI System(s), provide a current risk classification of each AI System under the EU AI Act risk taxonomy (minimal / limited / high / unacceptable) and shall co-operate in the Customer's impact assessment process (DPIA, IAMA, FRIA or sectoral equivalent), including provision of architecture, data-source, training-data, evaluation and known-limitation information.

Applicability: all. Anchor: KA9, KA10, KA11.

Clause 3.3 - Article 4 literacy support

The Supplier shall provide, at no additional cost, role-specific training material sufficient for the Customer's staff to discharge the Customer's obligations under EU AI Act Article 4 with respect to the supplied AI System(s). Material shall include at minimum: operator manual, supervisor handbook, escalation playbook, known-limitation summary and a model card or equivalent.

Applicability: all. Anchor: KA13.

Clause 3.4 - Knowledge sources and provenance

Where the AI System(s) consume external knowledge sources (RAG indices, ontologies, document corpora), the Supplier shall maintain provenance records sufficient to identify, for any given response, the contributing source(s). The Customer reserves the right to require signing or trust-grading of contributing sources where the System's risk band warrants it.

Applicability: RAG, generative-AI, agentic. Anchor: KA12.

Clause 3.5 - Model card and evaluation transparency

The Supplier shall provide a current model card for each AI Model in the AI System(s), conforming to the model-card structure adopted in the AI-BOK (intended use, training procedure, performance, limitations, bias analysis, ethical considerations) and shall update the model card upon any material change.

Applicability: all systems incorporating a custom or fine-tuned model. *Anchor:* KA6.

Clause 3.6 - Audit trail and decision artefacts

The Supplier shall ensure that the AI System(s) produce an audit trail sufficient to reconstruct any individual decision or generated output material to the Customer's regulatory obligations, including, where applicable, signed decision artefacts referencing the mandate under which the decision was made.

Applicability: high-risk, agentic. *Anchor:* KA10.

Clause 3.7 - Incident notification

The Supplier shall notify the Customer without undue delay (and in any event within 72 hours of becoming aware) of any incident affecting the AI System(s) that causes or is reasonably likely to cause harm to natural persons, violation of EU AI Act obligations, or material degradation of System safety or accuracy. The notification shall include facts, scope, mitigation status and the Supplier's contact for follow-up.

Applicability: all. *Anchor:* KA8, KA9.

Clause 3.8 - Agentic AI controls (when applicable)

Where the AI System(s) include agentic functionality, the Supplier shall (a) provide a description of the cognition plane elements implemented (mandates, authority register, policy-as-code, escalation thresholds), (b) document the agent's NHI lifecycle (provision, scope, rotation, revocation), and (c) co-operate with the Customer's failure-mode coverage assessment (FM01-FM22 of the AI-BOK).

Applicability: agentic. *Anchor:* KA3, KA9.

Clause 3.9 - Foundation-model dependency

Where the AI System(s) depend on a third-party foundation model, the Supplier shall disclose: (a) the foundation-model provider, (b) the licensing and usage terms applicable to the Customer, (c) data-flow paths (whether prompts/data are retained by the foundation-model provider), (d) the model's known limitations and any provider-issued advisories, and (e) the Supplier's plan in the event of foundation-model deprecation or material change.

Applicability: all systems using third-party foundation models. *Anchor:* KA6, KA9.

Clause 3.10 - Data residency and processing location

Personal data and proprietary content processed by the AI System(s) shall be processed only in locations agreed in writing. The Supplier shall not, without the Customer's prior written consent, route data through jurisdictions not on the agreed list. Where the System uses a third-party foundation model, this clause applies recursively to the foundation-model provider.

Applicability: all systems processing personal data or proprietary content. *Anchor:* KA10.

Clause 3.11 - Cybersecurity and prompt-injection resilience

The Supplier shall implement and maintain protective measures appropriate to the AI System(s)' risk band against (a) direct prompt injection, (b) indirect (data-borne) prompt injection, (c) tool misuse, (d) NHI credential leakage, and (e) sandbox escape, with reference to the AI-BOK agentic failure-mode catalogue (FM01-FM22) as the threat baseline.

Applicability: all agentic and prompt-based systems. *Anchor:* KA9.

Clause 3.12 - Bias testing and ethical use

The Supplier shall conduct bias testing on each AI Model material to the Customer's use case and shall provide bias-audit reports on request. The Supplier shall not deploy the AI System(s) for purposes contrary to the ethical-use policy notified by the Customer.

Applicability: decision-affecting systems. *Anchor:* KA11.

Clause 3.13 - Decommissioning and exit

Upon termination of this Agreement or decommissioning of the AI System(s), the Supplier shall, at the Customer's election, (a) return or destroy Customer data including training data, prompts, knowledge sources and decision logs, (b) provide an exit-archive of model artefacts and evaluation records sufficient for the Customer's retention obligations, and (c) where the System operated under an NHI, co-operate in NHI revocation and authority-register update.

Applicability: all. *Anchor:* KA4, KA3.

Clause 3.14 - Updates, retraining and notification

The Supplier shall give the Customer reasonable advance notice of (a) material model updates, (b) material foundation-model changes (where Clause 3.9 applies), (c) material changes to evaluation methodology and (d) material changes to known limitations. Notice shall include a window in which the Customer may run its own evaluation prior to deployment.

Applicability: all. *Anchor:* KA4, KA6.

Clause 3.15 - Performance, accuracy and degraded-mode

The Supplier shall maintain the AI System(s) within performance and accuracy targets agreed in the Specification. Upon degradation below target, the Supplier shall enter the agreed degraded-mode behaviour and notify the Customer. The Supplier shall not silently change the degraded-mode behaviour without written agreement.

Applicability: all, especially operational / cyber-physical. *Anchor:* KA8, KA9.

Clause 3.16 - Regulator co-operation

The Supplier shall co-operate with the Customer's obligations to regulatory authorities, including providing access to documentation, evidence and personnel within reasonable timescales, subject to lawful confidentiality protections.

Applicability: all. *Anchor:* KA10.

Clause 3.17 - Subcontracting and supply-chain transparency

The Supplier shall disclose any subcontractors, foundation-model providers, data-labelling vendors and other third parties material to the delivery of the AI System(s), shall not change them without notice, and shall flow these clauses down where applicable.

Applicability: all. *Anchor:* KA9, KA10.

Clause 3.18 - Indemnity for AI-specific harms

The Supplier shall indemnify the Customer against losses arising from (a) breaches of Clauses 3.1-3.17, (b) infringement by the AI System(s) of third-party intellectual-property or personality rights through generated output, and (c) regulatory penalties attributable to the Supplier's non-compliance - subject to the limits agreed in the body of this Agreement.

Applicability: all. *Anchor:* KA10.

Clause 3.19 - Continuous improvement and AI-BOK alignment (optional)

The Supplier shall track its own implementation against the AI-BOK reference framework and provide an annual statement of alignment (which knowledge areas at which maturity level), reflecting the AI-BOK version in force at the start of the contract year.

Applicability: strategic / multi-year contracts. *Anchor:* AI-BOK as a whole.

4. Use guidance

- Pick clauses by risk band: low-risk procurement uses Clauses 3.1, 3.3, 3.5, 3.7, 3.10, 3.13; medium-risk adds 3.2, 3.6, 3.11, 3.14, 3.15; high-risk and agentic uses all clauses.
- Tune wording to local procurement standards. The clauses are written as a starting point, not as final contract language.
- Combine with the Customer's standard data-processing addendum (DPA) - these clauses do not replace GDPR DPA obligations.
- For NL public-sector adopters, these clauses align with the VNG AI Governancekader procurement instrument and the BZK Algoritmekader procurement guidance; the AI-BOK clause set is a structured starting point that those instruments reference.