

AI-BOK TOOLKIT v1.2 · NL

AI-inkoopclausules

Aanvulling op de AI Body of Knowledge v1.2

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

AI-inkoopclausuleset

Negentien contractuele clausules, gegroepeerd per onderwerp en voorzien van de toepasselijke risicoband en het KG-anker, gereed om te worden overgenomen in inkoopkaders voor AI-systemen, AI-diensten en AI-gebruikende applicaties. Geen juridisch advies - wel een structureel compleet vertrekpunt.

1. Doel en reikwijdte

Deze clausuleset is ontworpen om, met beperkte aanpassing, te worden overgenomen in inkoopkaders voor AI-systemen, AI-diensten en AI-gebruikende applicaties. De clausules zijn bewust geformuleerd in neutrale contracttaal. Zij vormen *geen* juridisch advies - iedere gebruiker dient ze te laten toetsen door de eigen juridisch adviseur. Zij vormen *wel* een structureel compleet vertrekpunt dat een organisatie die AI inkoopt niet zelf van de grond af hoeft op te bouwen.

De clausules zijn gegroepeerd per onderwerp. Elke clausule bevat: **doel, clausuletekst, toepasselijkheid** (risicoband laag / midden / hoog, of specifiek), **AI-BOK-anker** (het kennisgebied waarop de clausule steunt voor de governance-opvolging).

2. Definities

Voor de toepassing van deze clausules geldt:

- **AI-systeem** heeft de betekenis die daaraan is gegeven in artikel 3, lid 1, van de EU AI Act.
- **AI-model** betekent de getrainde algoritmecomponent (bijv. foundation model, classifier, generator).
- **Agent / Agentische AI** betekent een AI-systeem dat autonoom plant, handelt en zich aanpast op basis van feedback.
- **Cognitievlak** (cognition plane) betekent de architectuurlaag die autonoom redeneren, mandaten en bevoegdheden bestuurt, zoals gedefinieerd in de AI-BOK (Module 1, KG3).
- **NHI** betekent Non-Human Identity - de identiteit (credential) waaronder een agentische AI handelt.
- **Aanbieder** (Provider) en **Gebruiksverantwoordelijke** (Deployer) hebben de betekenis die daaraan is gegeven in artikel 3 van de EU AI Act.

3. Clausuleset

Clausule 3.1 - Naleving EU AI Act

Doel: Vastleggen van de basisverwachtingen ten aanzien van AI Act-conformiteit aan de zijde van de leverancier.

De Leverancier verklaart en garandeert dat, voor zover de Leverancier kwalificeert als Aanbieder in de zin van de EU AI Act ten aanzien van de onder deze Overeenkomst geleverde AI-systemen, de Leverancier de conformiteitsbeoordelingsprocedure heeft doorlopen die van toepassing is op de betreffende risicoclassificatie, de krachtens Bijlage IV vereiste technische documentatie bijhoudt en het systeem of de systemen registreert in de EU-databank waar dat van toepassing is. De Leverancier verstrekt de Opdrachtgever de documentatie die de Opdrachtgever redelijkerwijs nodig heeft om aan diens eigen verplichtingen als Gebruiksverantwoordelijke te voldoen.

Toepasselijkheid: alle. *Anker:* KG10.

Clausule 3.2 - Risicoclassificatie en impactassessment

De Leverancier verstrekt, op verzoek en bij wijzigingen aan de AI-systemen, een actuele risicoclassificatie van elk AI-systeem volgens de risicotaxonomie van de EU AI Act (minimaal / beperkt / hoog / onaanvaardbaar) en verleent medewerking aan het impactassessmentproces van de Opdrachtgever (DPIA, IAMA, FRIA of sectoraal equivalent), waaronder het verstrekken van informatie over architectuur, databronnen, trainingsdata, evaluatie en bekende beperkingen.

Toepasselijkheid: alle. *Anker:* KG9, KG10, KG11.

Clausule 3.3 - Ondersteuning geletterdheid Artikel 4

De Leverancier verstrekt, zonder aanvullende kosten, rolspecifiek trainingsmateriaal dat toereikend is om het personeel van de Opdrachtgever in staat te stellen te voldoen aan de verplichtingen van de Opdrachtgever onder Artikel 4 van de EU AI Act met betrekking tot de geleverde AI-systemen. Het materiaal omvat ten minste: een operatorhandleiding, een handboek voor toezichthoudende medewerkers, een escalatiedraiboek, een samenvatting van bekende beperkingen en een model card of equivalent daarvan.

Toepasselijkheid: alle. *Anker:* KG13.

Clausule 3.4 - Kennisbronnen en herkomst

Voor zover de AI-systemen externe kennisbronnen gebruiken (RAG-indexen, ontologieën, documentcorpora), houdt de Leverancier herkomstregistraties (provenance) bij die toereikend zijn om voor elke gegeven respons de bijdragende bron(nen) te identificeren. De Opdrachtgever behoudt zich het recht voor ondertekening of vertrouwensgradering van

bijdragende bronnen te verlangen waar de risicoband van het Systeem daartoe aanleiding geeft.

Toepasselijkheid: RAG, generatieve AI, agentisch. Anker: KG12.

Clausule 3.5 - Model card en evaluatietransparantie

De Leverancier verstrekt voor elk AI-model in de AI-systemen een actuele model card, conform de model-card-structuur zoals opgenomen in de AI-BOK (beoogd gebruik, trainingsprocedure, prestaties, beperkingen, biasanalyse, ethische overwegingen) en werkt de model card bij elke materiële wijziging.

Toepasselijkheid: alle systemen met een maatwerk- of gefinetuned model. Anker: KG6.

Clausule 3.6 - Audittrail en beslisartefacten

De Leverancier draagt er zorg voor dat de AI-systemen een audittrail produceren die toereikend is om elke individuele beslissing of gegenereerde output die van belang is voor de wettelijke verplichtingen van de Opdrachtgever te reconstrueren, met inbegrip van, waar van toepassing, ondertekende beslisartefacten die verwijzen naar het mandaat waaronder de beslissing is genomen.

Toepasselijkheid: hoog risico, agentisch. Anker: KG10.

Clausule 3.7 - Incidentmelding

De Leverancier stelt de Opdrachtgever zonder onnodige vertraging (en in ieder geval binnen 72 uur na kennisneming) in kennis van elk incident met betrekking tot de AI-systemen dat schade aan natuurlijke personen, schending van verplichtingen onder de EU AI Act, of materiële verslechtering van de veiligheid of nauwkeurigheid van het Systeem veroorzaakt of redelijkerwijs waarschijnlijk veroorzaakt. De melding omvat de feiten, de omvang, de status van de mitigatie en het contactpunt van de Leverancier voor opvolging.

Toepasselijkheid: alle. Anker: KG8, KG9.

Clausule 3.8 - Beheersmaatregelen agentische AI (indien van toepassing)

Voor zover de AI-systemen agentische functionaliteit omvatten, zal de Leverancier (a) een beschrijving verstrekken van de geïmplementeerde cognitievlak-elementen (mandaten, bevoegdhedenregister, policy-as-code, escalatiedrempels), (b) de NHI-levenscyclus van de agent documenteren (uitgifte, reikwijdte, rotatie, intrekking), en (c) medewerking verlenen aan

de beoordeling van de faalmodusdekking door de Opdrachtgever (FM01-FM22 van de AI-BOK).

Toepasselijkheid: agentisch. Anker: KG3, KG9.

Clausule 3.9 - Afhankelijkheid van foundation models

Voor zover de AI-systemen afhankelijk zijn van een foundation model van een derde partij, maakt de Leverancier het volgende kenbaar: (a) de aanbieder van het foundation model, (b) de licentie- en gebruiksvoorwaarden die op de Opdrachtgever van toepassing zijn, (c) de datastromen (of prompts/data door de aanbieder van het foundation model worden bewaard), (d) de bekende beperkingen van het model en eventuele door de aanbieder uitgebrachte waarschuwingen, en (e) het plan van de Leverancier voor het geval het foundation model wordt uitgefaseerd of materieel wijzigt.

Toepasselijkheid: alle systemen die foundation models van derden gebruiken. Anker: KG6, KG9.

Clausule 3.10 - Datalocatie en verwerkingslocatie

Persoonsgegevens en bedrijfseigen content die door de AI-systemen worden verwerkt, worden uitsluitend verwerkt op schriftelijk overeengekomen locaties. De Leverancier zal zonder voorafgaande schriftelijke toestemming van de Opdrachtgever geen data routeren via jurisdicties die niet op de overeengekomen lijst staan. Waar het Systeem gebruikmaakt van een foundation model van een derde partij, is deze clausule recursief van toepassing op de aanbieder van het foundation model.

Toepasselijkheid: alle systemen die persoonsgegevens of bedrijfseigen content verwerken. Anker: KG10.

Clausule 3.11 - Cyberbeveiliging en weerbaarheid tegen prompt injection

De Leverancier implementeert en onderhoudt beschermende maatregelen, passend bij de risicoband van de AI-systemen, tegen (a) directe prompt injection, (b) indirecte (via data binnenkomende) prompt injection, (c) misbruik van tools, (d) lekkage van NHI-credentials, en (e) sandbox escape, met de agentische faalmodi-catalogus van de AI-BOK (FM01-FM22) als dreigingsbasislijn.

Toepasselijkheid: alle agentische en promptgebaseerde systemen. Anker: KG9.

Clausule 3.12 - Biastesten en ethisch gebruik

De Leverancier voert biastesten uit op elk AI-model dat van belang is voor de use case van de Opdrachtgever en verstrekt op verzoek bias-auditrapportages. De Leverancier zet de AI-

systemen niet in voor doeleinden die strijdig zijn met het door de Opdrachtgever kenbaar gemaakte beleid voor ethisch gebruik.

Toepasselijkheid: systemen die beslissingen beïnvloeden. Anker: KG11.

Clausule 3.13 - Uitfasering en exit

Bij beëindiging van deze Overeenkomst of uitfasering van de AI-systemen zal de Leverancier, naar keuze van de Opdrachtgever, (a) data van de Opdrachtgever retourneren of vernietigen, met inbegrip van trainingsdata, prompts, kennisbronnen en beslislogs, (b) een exit-archief verstrekken van modelartefacten en evaluatieregistraties dat toereikend is voor de bewaarverplichtingen van de Opdrachtgever, en (c) waar het Systeem onder een NHI opereerde, medewerking verlenen aan de intrekking van de NHI en de bijwerking van het bevoegdhedenregister.

Toepasselijkheid: alle. Anker: KG4, KG3.

Clausule 3.14 - Updates, hertraining en kennisgeving

De Leverancier stelt de Opdrachtgever met redelijke termijn vooraf in kennis van (a) materiële modelupdates, (b) materiële wijzigingen aan het foundation model (waar Clausule 3.9 van toepassing is), (c) materiële wijzigingen in de evaluatiemethodiek en (d) materiële wijzigingen in bekende beperkingen. De kennisgeving omvat een termijn waarbinnen de Opdrachtgever een eigen evaluatie kan uitvoeren voorafgaand aan ingebruikname.

Toepasselijkheid: alle. Anker: KG4, KG6.

Clausule 3.15 - Prestaties, nauwkeurigheid en degraded mode

De Leverancier houdt de AI-systemen binnen de in de Specificatie overeengekomen prestatie- en nauwkeurigheidsdoelen. Bij verslechtering tot onder de doelwaarde treedt de Leverancier in het overeengekomen degraded-mode-gedrag en stelt de Opdrachtgever daarvan in kennis. De Leverancier wijzigt het degraded-mode-gedrag niet stilzwijgend zonder schriftelijke overeenstemming.

Toepasselijkheid: alle, in het bijzonder operationeel / cyber-fysiek. Anker: KG8, KG9.

Clausule 3.16 - Medewerking aan toezichthouders

De Leverancier verleent medewerking aan de verplichtingen van de Opdrachtgever jegens toezichthoudende autoriteiten, waaronder het binnen redelijke termijnen verlenen van toegang

tot documentatie, bewijsmateriaal en personeel, met inachtneming van rechtmatige vertrouwelijkheidsbescherming.

Toepasselijkheid: alle. Anker: KG10.

Clausule 3.17 - Onderaanneming en ketentransparantie

De Leverancier maakt alle onderaannemers, aanbieders van foundation models, datalabelling-leveranciers en overige derde partijen kenbaar die van wezenlijk belang zijn voor de levering van de AI-systemen, wijzigt deze niet zonder kennisgeving, en legt deze clausules waar van toepassing door in de keten.

Toepasselijkheid: alle. Anker: KG9, KG10.

Clausule 3.18 - Vrijwaring voor AI-specifieke schade

De Leverancier vrijwaart de Opdrachtgever tegen verliezen voortvloeiend uit (a) schendingen van Clausules 3.1-3.17, (b) inbreuk door de AI-systemen op intellectuele-eigendomsrechten of persoonlijkheidsrechten van derden door gegenereerde output, en (c) bestuursrechtelijke boetes toerekenbaar aan niet-naleving door de Leverancier - met inachtneming van de in het lichaam van deze Overeenkomst overeengekomen begrenzingsen.

Toepasselijkheid: alle. Anker: KG10.

Clausule 3.19 - Continue verbetering en AI-BOK-alignering (optioneel)

De Leverancier volgt de eigen implementatie aan de hand van het AI-BOK-referentiekader en verstrekt een jaarlijkse verklaring van alignering (welke kennisgebieden op welk volwassenheidsniveau), op basis van de AI-BOK-versie die van kracht is bij aanvang van het contractjaar.

Toepasselijkheid: strategische / meerjarige contracten. Anker: AI-BOK als geheel.

4. Gebruiksrichtlijnen

- Kies clausules op basis van risicoband: inkoop in de lage risicoband gebruikt Clausules 3.1, 3.3, 3.5, 3.7, 3.10, 3.13; de middenband voegt 3.2, 3.6, 3.11, 3.14, 3.15 toe; de hoge risicoband en agentische systemen gebruiken alle clausules.
- Stem de formulering af op de lokale inkoopstandaarden. De clausules zijn geschreven als vertrekpunt, niet als definitieve contracttaal.
- Combineer met het standaard verwerkersaddendum (DPA) van de Opdrachtgever - deze clausules vervangen de AVG-verwerkersverplichtingen niet.

- Voor Nederlandse publieke organisaties sluiten deze clausules aan op het inkoopinstrument van het VNG AI Governancekader en de inkoophandreiking van het BZK Algoritmekader; de AI-BOK-clausuleset is een gestructureerd vertrekpunt waarnaar die instrumenten verwijzen.