



# AI-ACT: Vragenlijst voor aankoopdossiers met AI component

Aangezien we als ziekenhuis moeten voldoen aan de AI-wet- en regelgeving (o.a. de AI Act in Europa) én we steeds een grondige evaluatie willen maken van alle AI-toepassingen in onze zorgomgeving, vragen we u om onderstaande vragen in te vullen. Dit geeft ons een eerste, high-level inzicht in de AI-functionaliteit van het product en/of software. Maak in uw antwoorden waar relevant het onderscheid tussen data gebruikt voor het trainen van het model en data gebruikt in de toepassing.

## 1. Type AI-functionaliteit

- Kunt u aangeven of en in welke mate het product gebruikmaakt van AI/zelflerende algoritmes?
- Wat is de kernfunctionaliteit die door het AI systeem wordt uitgevoerd (diagnostiek, workflow-optimalisatie, besluitvorming, monitoring, beeldherkenning, enz.)?
- Is jullie AI systeem gebaseerd op een AI-model voor algemene doeleinden dat in staat is om een breed scala aan verschillende taken competent uit te voeren? Dit geldt niet als u AI modellen van derden gebruikt.  
Voorbeelden van AI-modellen voor algemeen gebruik zijn:
  - Grote taalmodellen (LLM's).
  - Tekst-naar-beeld- of tekst-naar-videomodellen.
  - Grote visusmodellen.
  - Multimodale modellen?
- Welke data van het ziekenhuis gebruikt het AI systeem (cfr overzicht in Annex 1)
- Tot welke categorie behoort het AI systeem volgens de AI Act?
  - (Onaanvaardbaar)
  - Hoog risico
  - Beperkt risico
  - Geen risico

## 2. Werking en training van het AI systeem

- Kan het AI-systeem of de leverancier uitleggen hoe beslissingen of outputs tot stand zijn gekomen, met alle relevante stappen die het doorloopt en op welke informatie het systeem zich baseert? (cfr transparantieplichtingen onder de EU AI Act)
- Op welke data is de AI getraind (bijvoorbeeld: type patiëntgegevens, demografische gegevens, beeldmateriaal)? Is deze training specifiek gebaseerd op Europese of internationale datasets?
- Wordt het AI systeem continu bijgestuurd (zelflerend) of gaat het om een statisch getraind model?
- Zo ja, worden de gegevens van het ziekenhuis of van patiënten van het ziekenhuis gebruikt om het AI algoritme bij te sturen?
- Welke beperkingen heeft het AI systeem? Probeer specifiek te zijn.

### 3. Kill switch en veiligheid

- Is er een kill switch/moeten we het AI-systeem ook gebruiken als we dat niet willen? Geeft de bijgevoegde documentatie aan hoe er kan overgeschakeld worden op een alternatief proces?
- Hoe wordt de nauwkeurigheid en validatie gegarandeerd en eventuele bias in de AI-uitkomsten voorkomen? Is hierover documentatie beschikbaar?
- Bestaat er documentatie over klinische validatiestudies of CE-markering (indien relevant)?
- Bestaat er certificatie voor het AI-systeem? vb NIST
- Welke maatregelen zijn geïmplementeerd om te voorkomen dat het AI-systeem schadelijke, misleidende of klinisch onveilige output produceert?
- Hoe beschermen jullie het AI-systeem tegen AI-beveiligingsrisico's, zoals model poisoning of prompt injection-aanvallen?

### 4. Risico's en risicoclassificatie

- Is het product reeds ingedeeld in een bepaalde risicoklasse onder de AI Act of onder de medische hulpmiddelenwetgeving (MDR)?
- Welke klasse is dit, hoe wordt dit gemotiveerd en is er bijbehorende documentatie?
- Welke risicobeperkende maatregelen worden er genomen, oa verzekering, uitsluiting van bepaalde data, beperking van bepaalde verwerkingen, etc?
- "Beschrijf de exitprocedure: welke stappen zijn voorzien om bij contractbeëindiging onze data (en – indien relevant – AI-modellen) terug te krijgen in een bruikbaar formaat?"
- "Ondersteunt u export en overdraagbaarheid van data of configuraties in gestructureerde, machineleesbare formaten?"

### 5. Dataopslag en -bescherming

- Hoe gaan jullie om met privacy en gegevensbescherming in relatie tot AI?
- Kan bevestigd worden dat jullie geen AI zullen toepassen op onze gegevens of die van patiënten zonder onze uitdrukkelijke toestemming?
- Kan bevestigd worden dat geen van de gegevens van patiënten of van ons ziekenhuis worden gebruikt om het AI systeem te trainen?

### 6. Integratie en gebruik in de workflow

- Hoe is de AI-gebaseerde functie geïntegreerd in de dagelijkse praktijk (bijvoorbeeld: als beslissingsondersteuning in het EPD, zelfstandig toestel, enz.)?
- Is er een opleiding of begeleiding voorzien voor de verantwoordelijken voor de toepassing en voor de eindgebruikers, en hoe wordt die georganiseerd?

### 7. Implementatie, testing, onderhoud en updates

- Wie is hiervoor verantwoordelijk?
- Kan het AI-model worden aangepast aan onze specifieke behoeften? Wie zou dit doen en hoe zouden de kosten/SLA eruitzien?
- Is er een mechanisme voor human oversight geïmplementeerd?
  - Wordt het AI-systeem zodanig ontworpen dat menselijke tussenkomst mogelijk blijft vóór beslissingen met kritieke gevolgen?
  - Zijn er waarborgen dat human oversight ook effectief kan worden uitgeoefend (bv. duidelijke uitleg, tijdige waarschuwingen, override-mogelijkheden)?
- Welk type ondersteuning bieden jullie aan gebruikers om de AI-functionaliteiten effectief te gebruiken?
- Op welke wijze worden updates of nieuwe versies van het AI-algoritme uitgerold en gecommuniceerd?

- Wordt er een proces voorzien om (eventuele) problemen of incidenten te melden en op te volgen?

Graag ontvangen wij uw antwoorden op deze vragen om een eerste inschatting te kunnen maken. Op basis hiervan kunnen we beoordelen of het noodzakelijk is om een diepgaandere risicoanalyse, inclusief een formele AI-risk assessment, te starten.

## Annex 1: overzicht mogelijke gegevens

|                                                                    |
|--------------------------------------------------------------------|
| <b>Patiënt</b>                                                     |
| Patiëntengegevens in het EPD                                       |
| Administratieve identificatiegegevens                              |
| Financiële gegevens                                                |
| Sociale gegevens en gegevens over opleiding, beroep                |
| Psychiatrische gegevens                                            |
| Gezondheidsgegevens                                                |
| Gegevens verwanten in een dossier                                  |
| Gegevens derden in een dossier                                     |
| Genetische gegevens                                                |
| Biometrische gegevens                                              |
| Gegevens over fertiliteit en sexualiteit                           |
| Gerechtelijke gegevens                                             |
| Rijksregisternummer                                                |
| Raciale of etnische gegevens, politieke opvattingen, geloof        |
| Gegevens afkomstig van niet medische sensoren (beeld, geluid, ...) |
| GPS-locatiegegevens                                                |
| Toestemmingen en zorgrelaties                                      |
| Verzekerbaarheid                                                   |
| Klachten                                                           |
| <b>Medewerker</b>                                                  |
| Gegevens medewerkers in het EPD                                    |
| Administratieve personeelsgegevens                                 |
| Financiële gegevens                                                |
| Sociale gegevens en gegevens over opleiding, beroep                |
| Gezondheidsgegevens medewerkers                                    |
| Gerechtelijke gegevens                                             |
| Evaluaties en beoordelingen                                        |
| Klachten                                                           |
| Biometrische gegevens                                              |
| Rijksregisternummer                                                |
| <b>Bezoeker/ Andere</b>                                            |
| Administratieve gegevens                                           |
| Financiële gegevens                                                |
| GPS-locatiegegevens                                                |
| Gegevens afkomstig van niet medische sensoren (beeld, geluid, ...) |
| Gegevens afkomstig van online verkeer                              |
| Andere:                                                            |