



Verantwoord omgaan met AI

Voorstellen



- Niels Dutij
- Adviseur MBO Digitaal bij Programma Cyberveiligheid
- Functionaris voor gegevensbescherming bij meerdere MBO's
- Sinds juli 2025 Certified AI Compliance officer (CAICO)

Er is werk te doen :)

Factsheet AI verordening voor bestuurders

Wat is de AI verordening?

De AI verordening bevat de Europese eisen en kaders voor de ontwikkeling en het gebruik van AI-systemen. Het betreft productveiligheid wetgeving, waarbij AI-systemen worden ingedeeld in verschillende risicocategorieën. Bepaalde AI-systemen worden verboden. Aan andere AI-systemen worden (strengere) regels gesteld.

Het doel is om innovatie te stimuleren, de grondrechten en veiligheid te beschermen, en democratische controle mogelijk te maken.

Wat betekent dit voor de organisatie?

De nieuwe regels hebben impact op de inkoop, ontwikkeling, en het gebruik van AI-systemen in uw organisatie. Om aan deze regels te voldoen zijn maatregelen nodig zoals inrichten van governance, opstellen van documentatie, en het trainen van medewerkers die in aanraking komen met AI-systemen.

Governance

Er moeten interne beleidskaders en procedures worden geïmplementeerd, gericht op onder meer de inkoop en het beheer van AI-systemen. Dit omvat richtlijnen voor risicobeheer, kwaliteitsbeheer en compliance met de geldende regelgeving.

Documentatie

AI-systemen moeten juist worden geclassificeerd en geïnventariseerd. Hoog risico AI-systemen en impactvolle algoritmes moeten worden opgenomen in het algorimtereister.

Training

Gebruikers zullen kennis en expertise moeten opbouwen om te voldoen aan de verplichtingen rondom AI geletterdheid.

Kosten

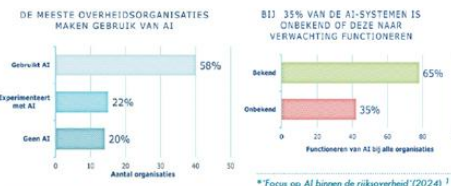
Compliance aan de AI verordening zal kosten met zich meebrengen, onder andere voor de initiële implementatie, het inrichten en onderhouden van de governance, en personele kosten voor training, monitoring, en naleving.

Hoewel deze kosten een investering vergen, zijn ze verwaarloosbaar in vergelijking met de financiële sancties en personele kosten die non-compliance kan veroorzaken.

Waarom is AI (en AI-wetgeving) belangrijk?

Het gebruik van AI neemt steeds verder toe, niet alleen vanwege de voordelen die de technologie biedt, maar ook omdat AI steeds vaker wordt geïntegreerd in traditionele software. De meeste overheid-instellingen maken inmiddels al gebruik van AI¹, maar in veel gevallen ontbreekt adequaat toezicht op het functioneren van deze systemen² (zie afbeeldingen onder³). Dit brengt risico's met zich mee, aangezien AI-systemen mogelijk de veiligheid en grondrechten kunnen schaden.

Om ervoor te zorgen dat AI op een betrouwbare en verantwoorde manier wordt ingezet en om grote misstanden te voorkomen, introduceert de AI-verordening bindende regels voor de ontwikkeling en het gebruik van AI-systemen.



Implementatie bij de rijksoverheid

De rijksbrede implementatie van de AI verordening richt zich op 2 pijlers.

Naleving binnen sector overheid

Gericht op het in kaart brengen en organiseren van AI-toepassingen binnen overheidsorganisaties.

Juridische implementatie en communicatie

Gericht op wetgeving, toezicht en samenwerking binnen Nederland en de EU.

Er is doorlopende ondersteuning beschikbaar bij de implementatie van de AI-verordening voor departementen en uitvoerings-organisaties, middels de werkgroep 'Rijksbrede Implementatie AI Act' en de vraagbaak die te bereiken is via ai-verordening@minbzk.nl. Voor aanvullende richtlijnen kunt u daarnaast terecht bij het Algoritmekader⁴ en de website van Digitale Overheid⁵.

Consequenties van niet-naleving

Reputatieschade

De overheid heeft toegezegd meer te gaan doen om problemen met algoritmen te voorkomen⁶. Het is belangrijk om het vertrouwen van burgers te waarborgen door aan alle vereisten te voldoen, en hiermee tevens negatieve media-aandacht te voorkomen.

Financiële sancties

De AI-verordening legt hoge boetes op voor niet-naleving van de verordening, welke kunnen oplopen tot 35 miljoen euro of 7% van de jaaromzet, afhankelijk van welk bedrag hoger is.

De verordening treedt gefaseerd in werking. Voor overheidsorganisaties zijn de belangrijkste data:



¹) Focus op AI bij de rijksoverheid | Rapport 1 Algemene Rekenkamer

²) Eénheid van risico's AI vaak niet in 1 Nieuwsbericht 1 Algemene Rekenkamer

³) Algoritmekader - Algoritmekader 1

⁴) AI-verordening AI (Artificiële Intelligentie) - Digitale Overheid

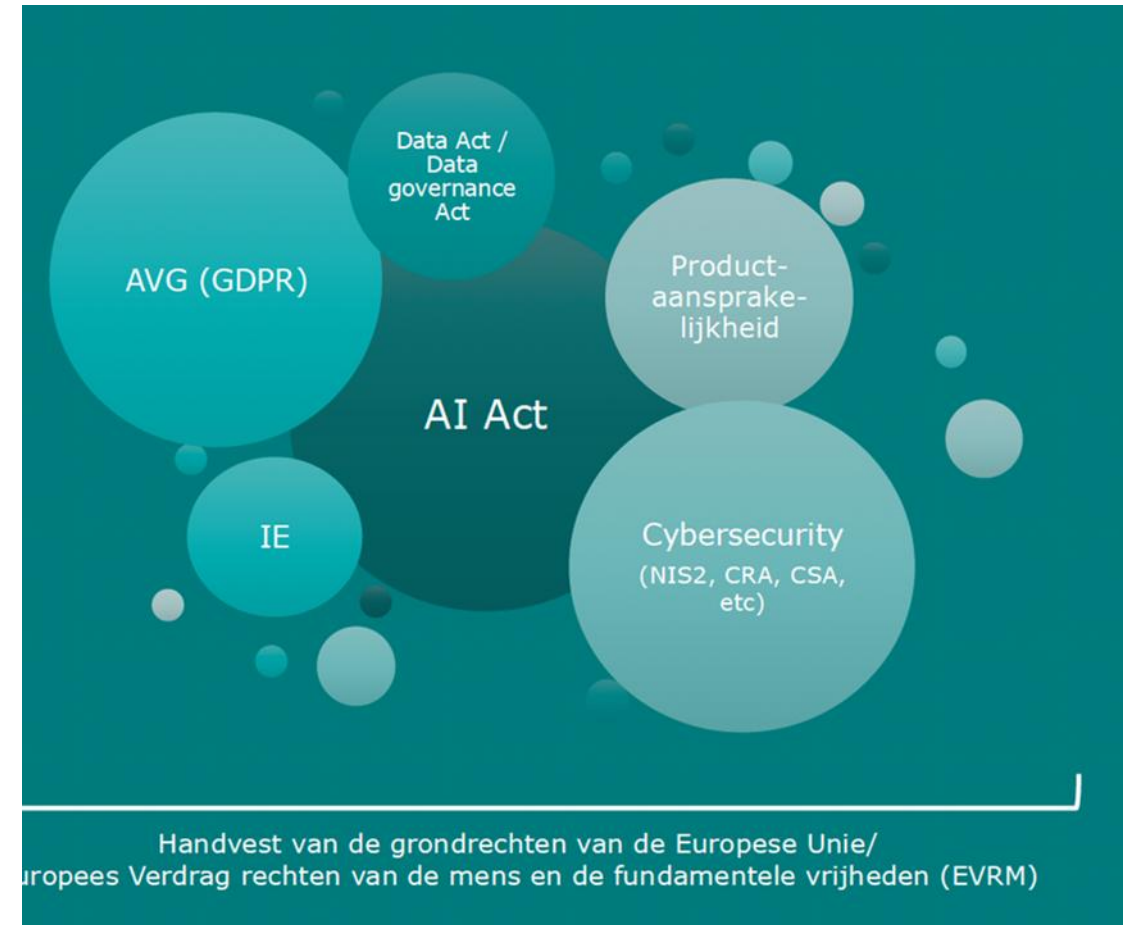
⁵) Overheid gaat meer doen om problemen algoritmen te voorkomen 1 Nieuwsbericht

⁶) Rijksoverheid.nl

- Gefaseerde inwerkingtreding AIA
- Beleid
- Documentatie
- AI geletterdheid

Overzicht van de wetgeving

- Veel verschillende soorten wetgeving omtrent data en technologie
- AI-ACT bestaat naast de AVG



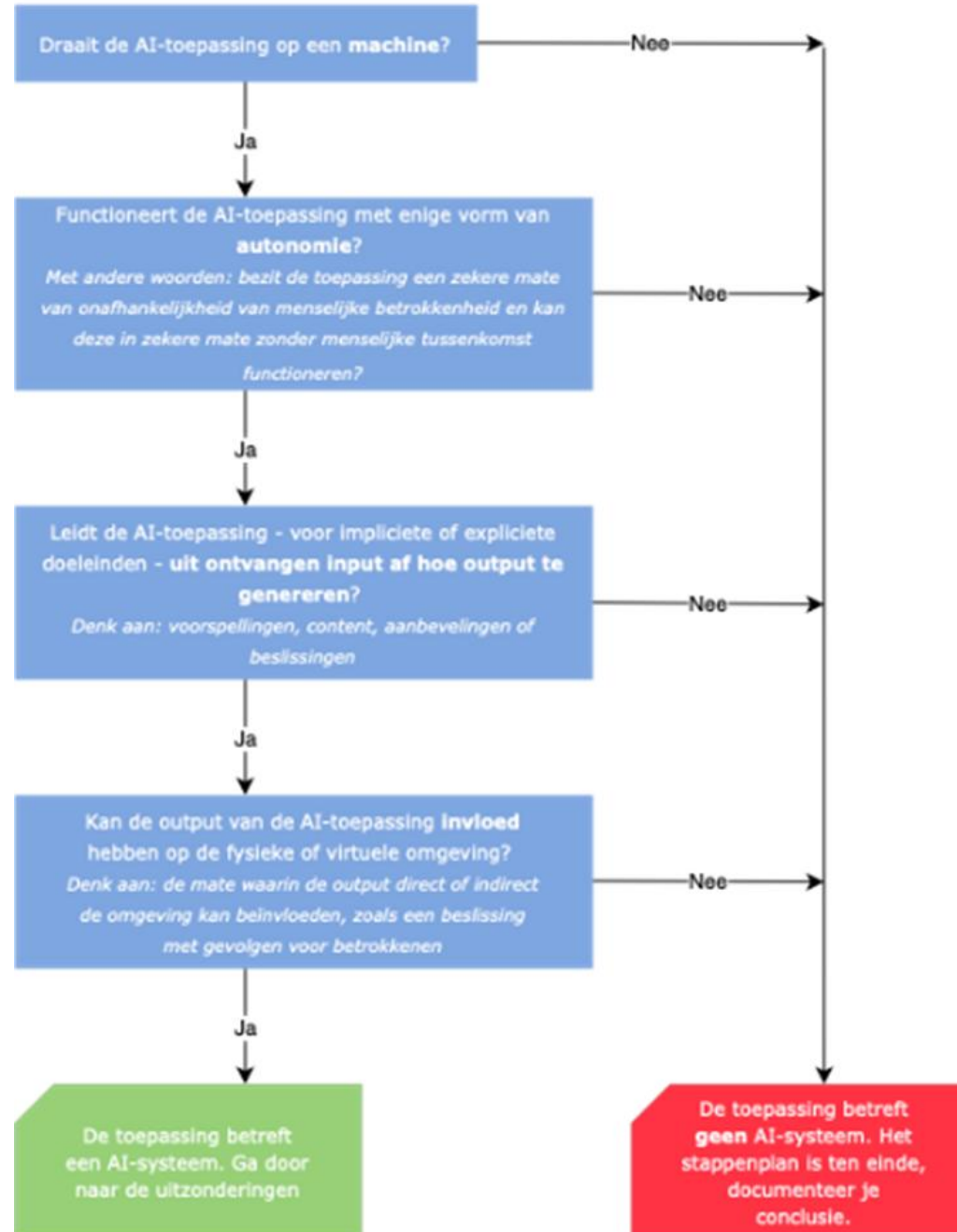
Wat is AI?

Wat is een AI-systeem?

“Een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan aanpassingsvermogen kan vertonen, en dat, voor expliciete of impliciete doelstellingen, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen.”

Autonomie is key!

AI-verordening van toepassing



Operatoren AI Act



Aanbieder

Brengt AI onder eigen naam op de markt



Importeur

Brengt AI naar Europese markt



Gemachtigde

Vertegenwoordigt andermans AI (aanbieder buiten de EU)



Gebruiker

Interacteeert met de AI



Getroffen persoon

Merkt effect van een AI



Gebruiksverantwoordelijke

Bepaalt wijze van inzet van een AI



Distributeur

Iedere schakel tussen aanbieder en gebruiksverantwoordelijke

Let op: voor GPAI-modellen kent de AI Act alleen de operatoren: aanbieder en gemachtigde

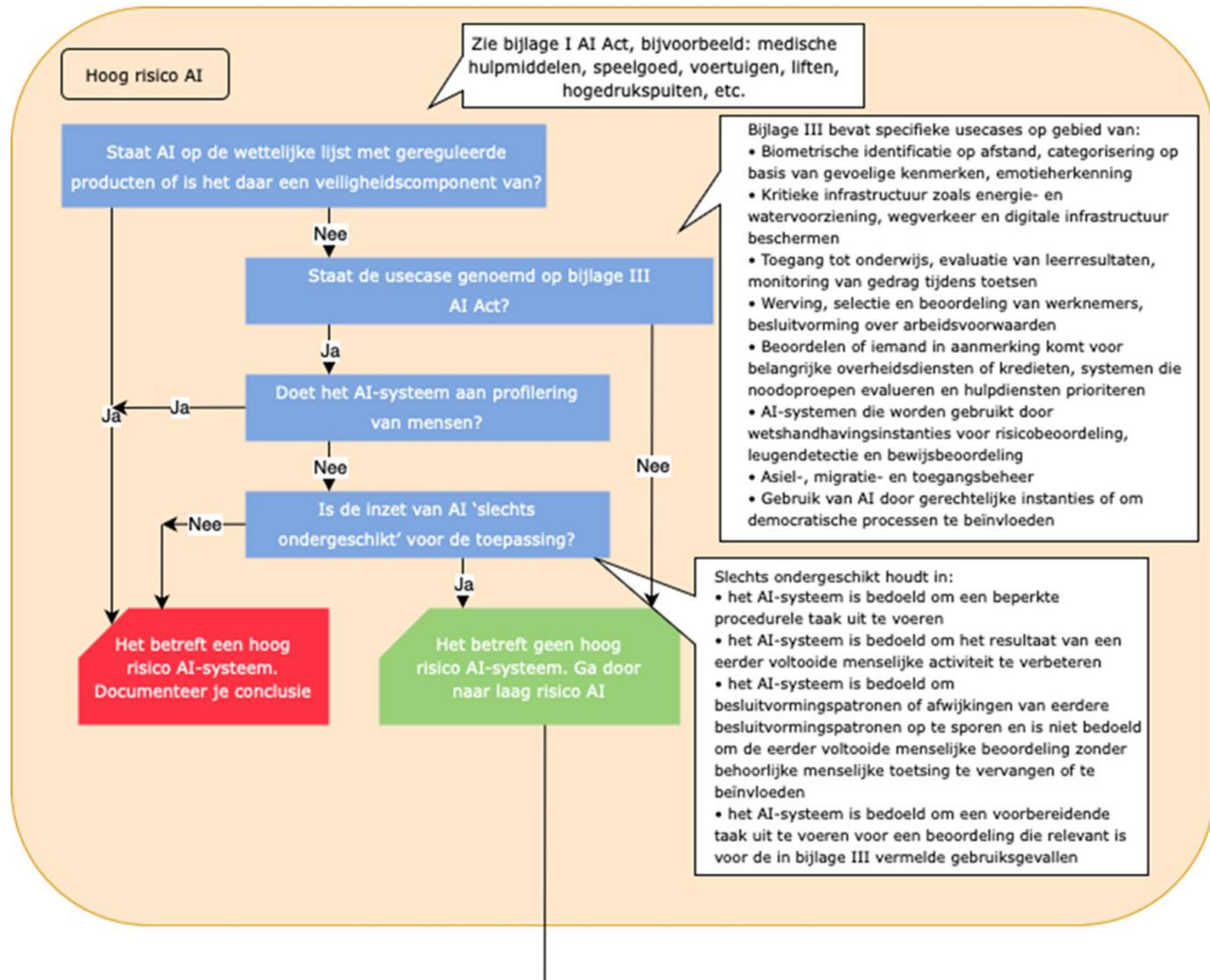
Verschillende soorten AI

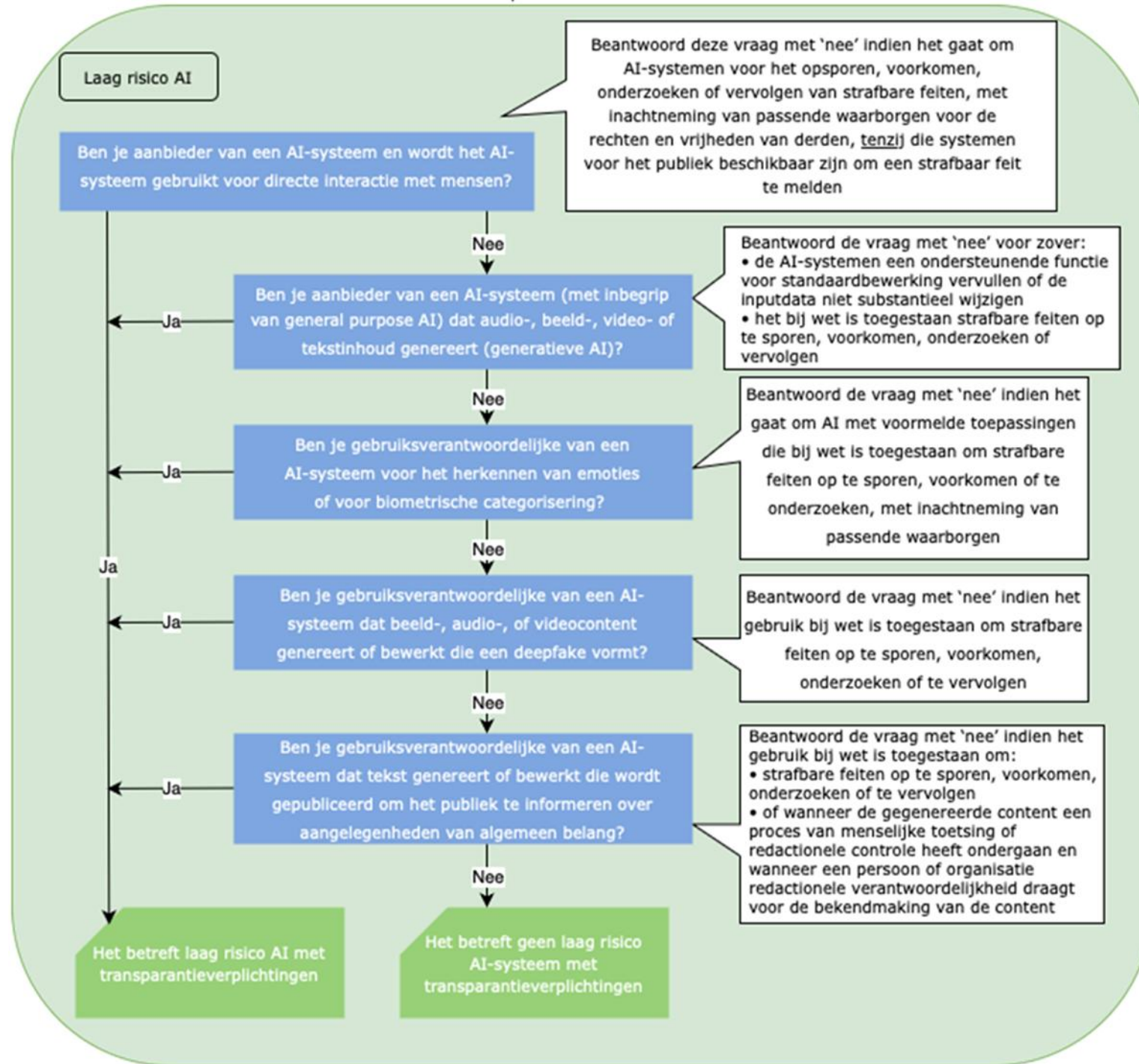


Verboden AI	• Onacceptabele risico's voor gezondheid, veiligheid of fundamentele rechten • Vastgelegd in AI Act (art. 5 AIA)
Hoog risico	• Significante risico's voor gezondheid, veiligheid of fundamentele rechten (art. 6 AIA) • Gereguleerde producten vermeld in Bijlage I • Risicogebieden in Bijlage III met risicotoets
'Laag/beperkt' risico	• Specifieke transparantierisico's • Bepaalde AI-systemen die niet als hoog risico worden beschouwd, maar toch aan bepaalde transparantievereisten moeten voldoen (art. 50 AIA)
General Purpose AI	• Aparte regels voor AI-modellen voor algemene doeleinden (art 51 AIA e.v.) • 'Systemic risk' (art. 55 AIA)
Regulatory sandbox	• Stimuleren van innovatie, gericht op testen en validatie (art. 57 AIA) • Onder direct toezicht van nationale toezichthouder

Verplichtingen hoge risico's

- *Hoog risico* voor gezondheid, veiligheid, grondrechten van personen of voor het milieu
- Classificatie: formeel proces (art. 6 t/m 15 + Bijlage I + III)
 - AI is veiligheidscomponent van gereguleerd product (Bijlage I): liften, speelgoed, medische apparaten, luchtvaart, auto's.
 - AI wordt gebruikt in hoogrisico *use cases* (Bijlage III): kritieke infrastructuur, werkgelegenheid, rechtshandhaving, migratie en onderwijs en beroepsopleiding.
 - AI wordt gebruikt voor *profiling*
 - Uitzonderingen indien AI 'louter ondersteunend' is
- Strenge eisen voor AI-systeem
- Verplichtingen voor zowel aanbieders als gebruiksverantwoordelijken, maar meeste voor aanbieders

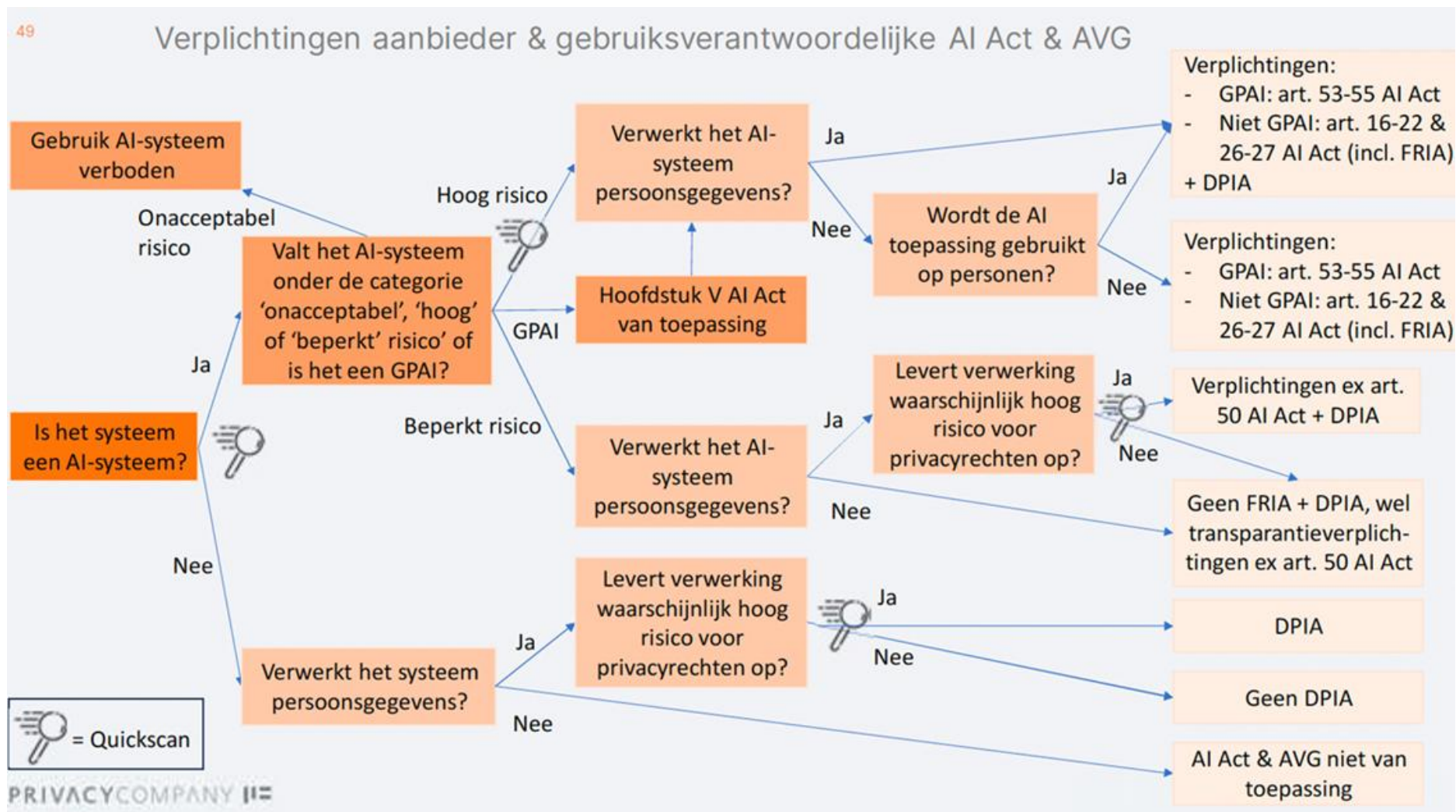




Hoog risico in het onderwijs en als werkgever

- Toegang, toelating en toewijzing tot onderwijs
 - Evalueren van leerresultaten en sturen van het leerproces
 - Beoordelen van het passend onderwijsniveau
 - Monitoren en detecteren van ongeoorloofd gedrag tijdens toetsen
-
- Systemen voor het werven of selecteren van kandidaten
 - Systemen voor het maken van besluiten die gevolgen hebben voor het arbeidscontract en de arbeidsvoorwaarden, voor het verdelen van taken en voor het monitoren en evalueren van werknemers.

Overzicht verplichtingen



FRIA en DPIA



Fundamental Rights Impact Assessment (FRIA)

- Inschatting en mitigatie van risico's voor (grond)rechten en maatschappij bij hoog risico AI-systeem.
- Uitgevoerd door deployers in overheid, semi-overheid, kredietinstellingen en levens/gezondheid verzekering.
- Herhalen indien verouderd.



Data Protection Impact Assessment (DPIA)

- Inschatting en mitigatie van risico's voor privacy en (grond)rechten.
- Uitgevoerd door verwerkingsverantwoordelijke.
- Opnieuw bij veranderde risico's.
- In de AIA wordt verwezen naar artikel 35 AVG. Je mag de resultaten van een DPIA meenemen in een FRIA.



Eisen FRIA (art 27 AIA)

Een assessment moet in ieder geval bevatten:

- een beschrijving van de processen van de gebruiksverantwoordelijke waarin het hoog-risico AI-systeem zal worden gebruikt, in overeenstemming met het beoogde doel;
- een beschrijving van de periode en frequentie waarin elk hoog-risico AI-systeem bedoeld is te worden gebruikt;
- de categorieën van natuurlijke personen en groepen die waarschijnlijk beïnvloed worden door het gebruik ervan in de specifieke context;
- de specifieke risico's op schade voor de categorieën natuurlijke personen of groepen personen;
- een beschrijving van de implementatie van maatregelen voor menselijk toezicht;
- de te nemen maatregelen in geval van de materialisatie van deze risico's, inclusief hun regelingen voor interne governance en klachtenmechanismen."

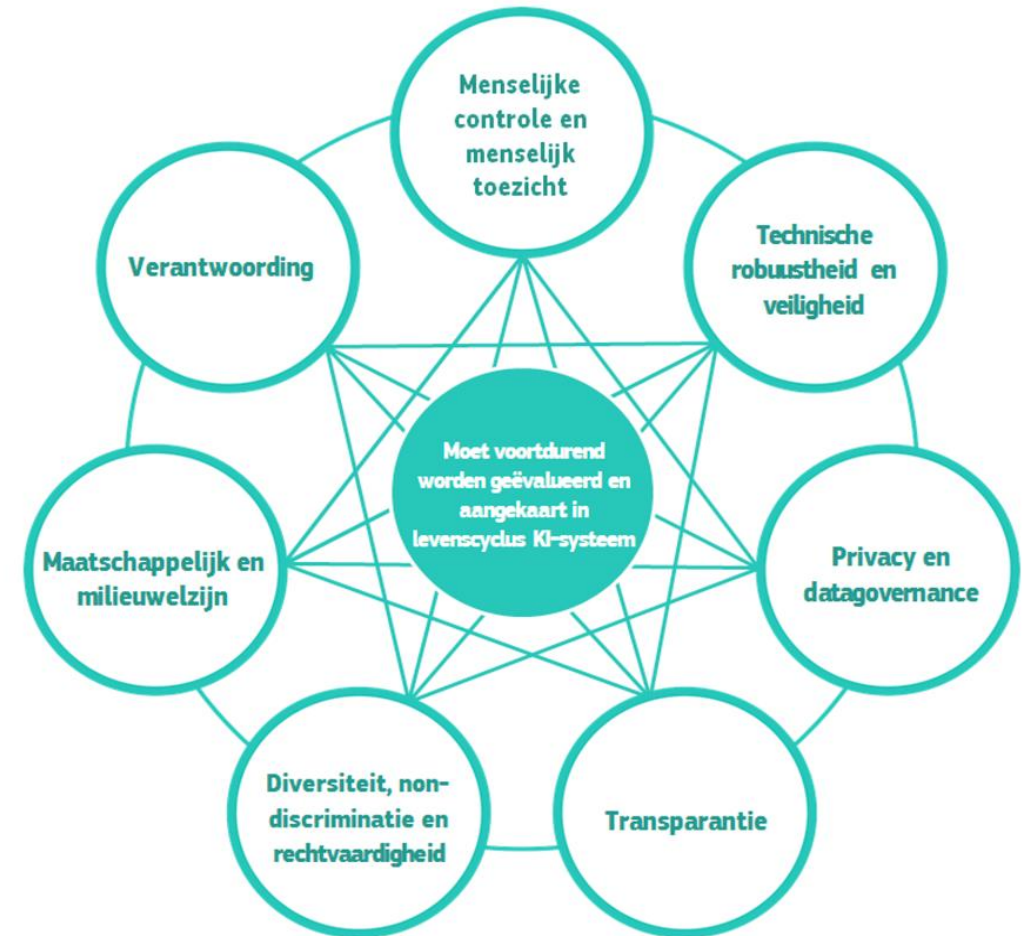
Best practice FRIA

Rijksoverheid: AI Impact Assessment
(ook Engelstalig).

En

Ethics guidelines for trustworthy AI

<https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>



Belangrijkste punten FRIA (1)

Doel en context van het AI-project

- Waarvoor wordt de AI ingezet?
- Hoe functioneert het systeem technisch (leren, redeneren, plannen, suggesties)?

Data, privacy & kwaliteit

- Welke data wordt gebruikt (herkomst, representativiteit)?
- Kwaliteit van de data (bias, volledigheid, accuratesse).
- Privacyaspecten: verwerking persoonsgegevens, geautomatiseerde besluitvorming, naleving AVG.

Belangrijkste punten FRIA (2)

Risico's en mogelijke negatieve effecten

- Discriminatie (bijvoorbeeld genderbias in sollicitantenselectie).
- Onbedoelde en onvoorziene gevolgen voor individuen of doelgroepen.
- Gebruik in processen met belangrijke gevolgen (bijvoorbeeld werving, veiligheid).

Monitoring, bijsturing en aanpassingsvermogen

- Hoe wordt het systeem gemonitord?
- Welke mechanismen bestaan om fouten of bias bij te sturen?
- Plan voor continue evaluatie en verbetering.

Verantwoording en transparantie

- Hoe wordt intern verantwoording afgelegd?
- Hoe opent het systeem zich naar de samenleving toe?
- Vastlegging van het denkproces, beslissingen en afwegingen voor reproduceerbaarheid en verantwoording

Casus: Geautomatiseerde examinering

-  Een examenplatform biedt een geweldige mogelijkheid voor het afnemen van mondelinge examens. Studenten spreken de opdracht in, waarbij het AI-platform tot een score komt.

Dit proces is volledig geautomatiseerd. Docenten en examinatoren krijgen enkel de uitslag, maar hebben geen toegang tot het gemaakte examenwerk.

Er is wel door de medewerkers van het examenplatform de mogelijkheid voor een review van gemaakt werk als examen. Dit is echter reactief.

Opdracht: Welke risico's en maatregelen zien we?



Risico 1: Recht op gelijke behandeling

Is er bias in het AI-model (accenten, taalgebruik, spraakstoornissen)?

Worden kwetsbare groepen (bv. dyslectische of anderstalige studenten) benadeeld?

Vereisten AI-ACT

- AI-systemen moeten worden getest op bias en discriminatie.
- De dataset moet representatief zijn om oneerlijke beoordelingen te voorkomen.

Risico 2: Rechtmatigheid verwerking gegevens

- Hoe wordt stemdata verwerkt en opgeslagen?
- Geautomatiseerde besluitvorming
- Kunnen studenten hun gegevens inzien en laten verwijderen?

Vereisten AVG en AI-ACT

- Studenten moeten inzage krijgen in hun gegevens.
- Er moet een duidelijke grondslag zijn voor het verwerken van biometrische data.
- Dataminimalisatie: Data mag niet langer bewaard worden dan strikt noodzakelijk.

Risico 3: Recht op een eerlijk proces (due process)

- Kunnen studenten hun beoordeling inzien en aanvechten?
- Is er een menselijke controle voordat beslissingen definitief zijn?

Riscio 4: Transparantie

Transparantie en uitlegbaarheid

- Black-box karakter: Studenten en docenten krijgen geen inzicht in hoe de AI tot een score komt.
- Gebrek aan controle: Docenten kunnen de beoordeling niet valideren controleren.
- Gebrek aan uitleg voor studenten: Studenten hebben geen toegang tot hun ingesproken examen of de beoordeling, wat in strijd kan zijn met het recht op uitleg.

Vereisten onder de AI Act:

- De AI moet begrijpelijk en uitlegbaar zijn.
- Studenten en docenten moeten kunnen begrijpen hoe beslissingen tot stand komen.

Risico 5: Aansprakelijkheid en verantwoordelijkheid

Aansprakelijkheid en verantwoordelijkheid

- Wie is verantwoordelijk bij fouten (de school of het platform)?
- Wat zijn de gevolgen voor studenten als ze door een AI-fout onterecht zakken?

Risico 6: Juist gebruik

Training en AI-geletterdheid

- Instructies voor medewerkers over veilige en verantwoorde omgang missen;
- AI-geletterdheid?

Welke risico's zien jullie?



Wat zou ieder ROC moeten regelen?

1

IN KAART BRENGEN
WELKE APPLICATIES
GEBRUIK MAKEN VAN
AI EN RISICO-
INSCHATTING DOEN;

2

WIE BEWAAKT DE
ETHISCHE KANTEN?

3

AI GELETTERDHEID;

4

AI-BELEID
GOVERNANCE
WIE GAAT HIEROVER?

Opdracht



Maak een inhoudsopgave van een AI-beleid.



Documenten SURF!

- AI beleid
 - voor studenten
 - voor medewerkers
- Checklist AI-verordeningen
- Eisen inkoop AI-systemen



Privacy Expertise Centrum

Bedankt voor jullie aandacht!

