



Ministerie van Economische Zaken
en Klimaat

Artificial Intelligence – Hoe nu verder?

Over de AI Act in internationale context.

12 september 2023

Lisa Vermeer, EZK

Directie Digitale Economie



Voorstellen

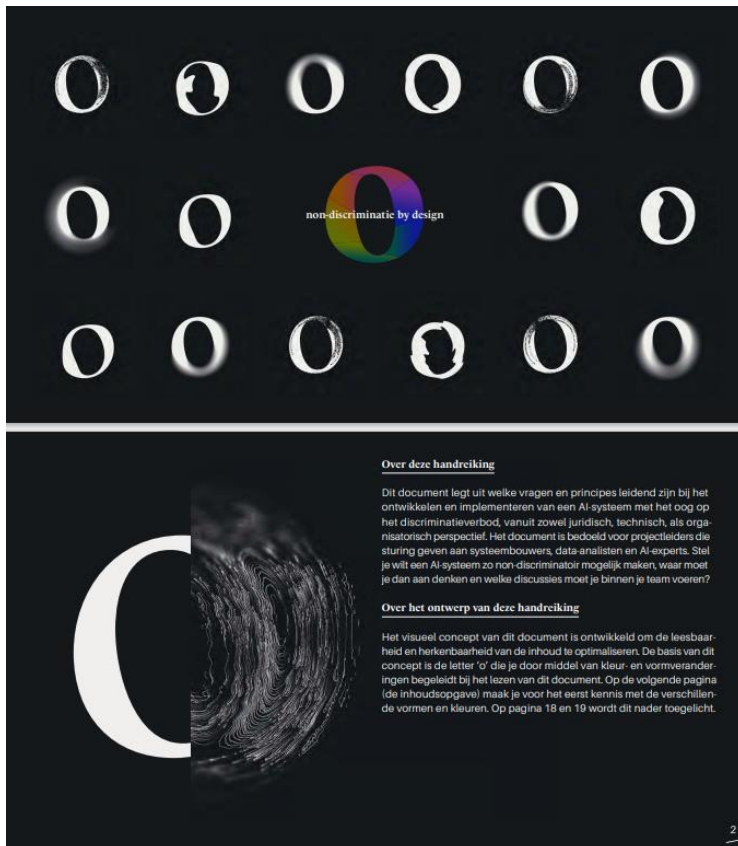
- > Sinds 2021 coördinator Nederlandse positie over de AI Act in Brussel
- > Meer dan 10 jaar AI-beleidmaker
 - Buitenlandse Zaken
 - Economische Zaken en Klimaat
- > Onderzoek: internationale AI-wetgeving en strategieën bij ICNL
- > Diplomatie: bevorderen mensenrechten bij inzet digitale technologie bij BZ
- > Beïnvloeden EU: adviseur bij de griffie van de Tweede Kamer en Europa decentraal
- > Helaas geen internet governance meer



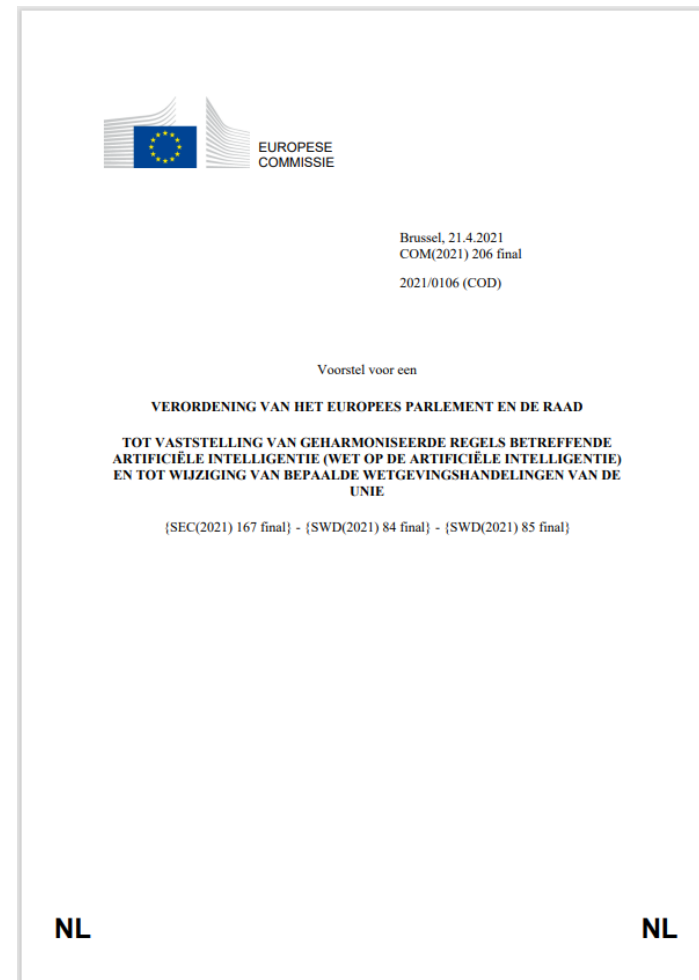


AI reguleren

- > Van zachte handreikingen naar harde wetgeving
- > Geen *regulatory void* (AVG etc.) maar ook geen AI-specifieke regels
- > Meerjarige onderhandelingen in Brussel



Handreiking Non-discriminatie by design
Opgesteld in opdracht van BZK
Ontwerp: Julia Janssen

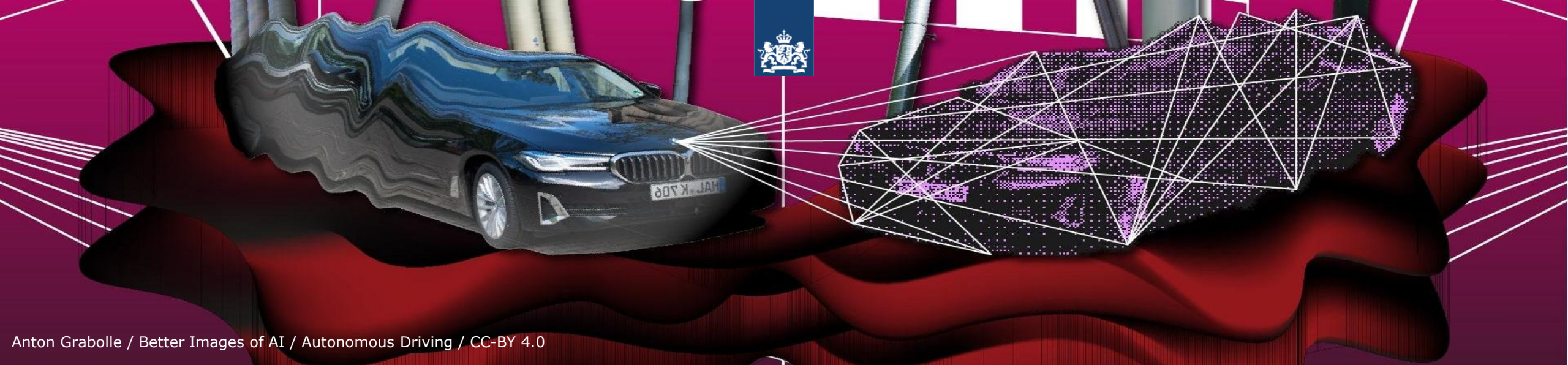




Doelen van de Europese AI-verordening

- > EU-burgers vertrouwen geven in AI zodat AI wordt omarmd
- > Geharmoniseerde regels om risico's van AI-systemen te voorkomen en te beperken
 - Veiligheid
 - Gezondheid
 - Fundamentele rechten
- > Fragmentatie van de markt tegengaan
- > Wereldwijd de standaard voor betrouwbare AI stellen





Anton Grabolle / Better Images of AI / Autonomous Driving / CC-BY 4.0

De aanpak van de AI-verordening

- › **Productregulering** met AI-systeem als product
- › AI-systeem moet aan **eisen** voldoen voordat het wordt gebruikt of verkocht ('op de markt gebracht'), zoals risicomangement
- › Horizontale regels voor **publieke en private sector**
- › **Verplichtingen** voor aanbieder en gebruikers, zoals conformiteit beoordelen
- › **Rechten** voor natuurlijke personen, zoals **klachtrecht**
- › Europees en nationaal **toezicht** op eisen en gebruik



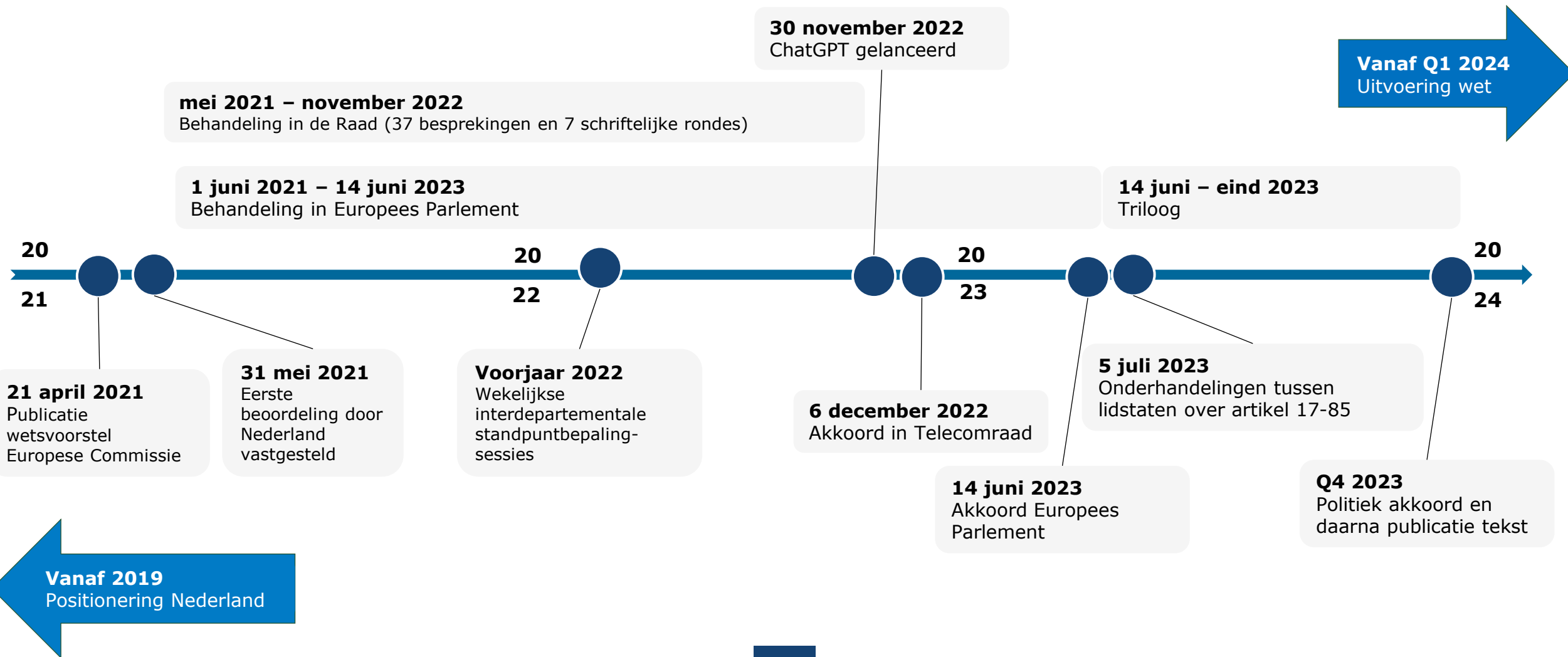
Risicocategorieën



- › Verbieden van praktijken met *onaanvaardbaar* risico
 - Biometrische identificatie publieke ruimte t.b.v. rechtshandhaving (met uitzonderingen)
 - Social scoring
- › Transparantie vereisten voor *bepaalde* systemen
 - O.a. deepfakes en chatbots
- › Foundation models, generieke AI-systemen en generatieve AI
 - Zoals GPT-4 en ChatGPT
- › Eisen aan *hoog-risico* AI systemen
 - Bepaalde toepassingen binnen rechtshandhaving, asiel/migratie en rechtspraak
 - Vooral eisen aan de ontwikkeling van het systeem (provider)
- › Vrijwillige gedragscodes
 - Let op: alles is nog onderwerp van **onderhandelingen**, kan verschillende kanten op in de uiteindelijke wet.



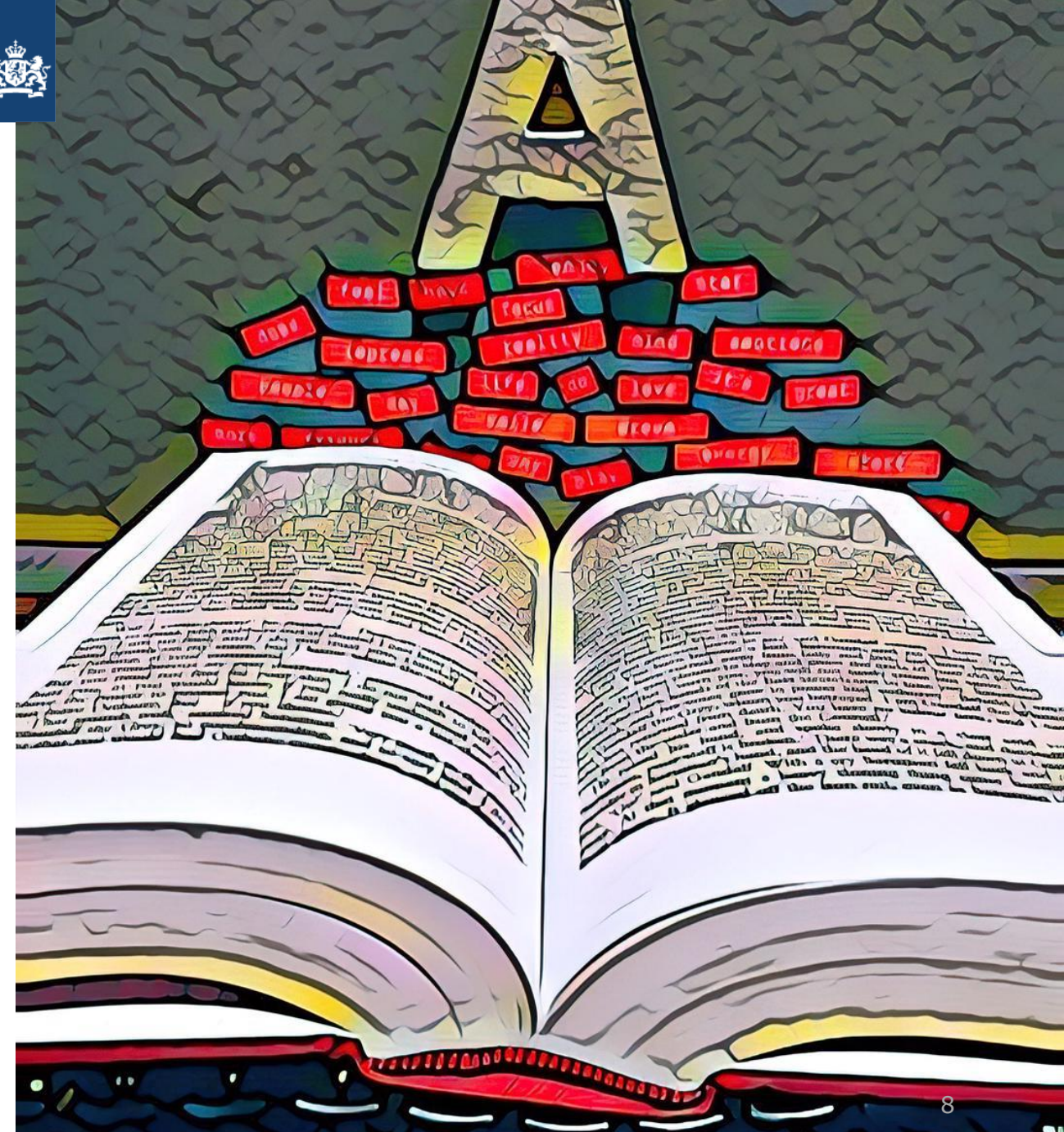
Tijdlijn Europese AI-verordening





Internationale context

- › Europese aanpak: niet markt, niet staat, maar **regels** (*Brussels effect*, *GDPR*)
 - Annex II producten – ja
 - Annex III gebieden – twijfel
- › Europese en internationale standaarden
 - Conformiteit
 - Risicobeheer
 - NB: transparantie aandachtspunt*
- › Nuttige wildgroei aan AI-principes en initiatieven?
 - VN SG en Tech Envoy, G7, G20, OECD, UNESCO, GPAI, REAIM





Ministerie van Economische Zaken
en Klimaat

Bedankt! Vragen?

Lisa Vermeer, EZK



AI systemen met specifieke risico's door interactie

- > AI die communiceert met natuurlijke personen
- > AI die emoties herkent
- > AI die mensen profileert op basis van biometrische gegevens
- > Deepfakes

- > Oplossing: transparantie





Hoog risico AI en gereguleerde producten



- > AI-systemen in producten of op zichzelf staand die al door een onafhankelijke partij moeten worden beoordeeld (annex II)
- > Zoals:
 - Speelgoed
 - Machines
 - Liften
 - Radioapparatuur
 - Medische hulpmiddelen
 - Landbouwvoertuigen
 - Drones



Hoog risico AI in bepaalde toepassingsgebieden

- › AI-systemen bedoeld voor gebruik in acht toepassingsgebieden ('use cases')
- 1. Biometrische identificatiesystemen
- 2. Veiligheid in kritieke infrastructuur (digitaal, verkeer, water, gas, verwarming, electriciteit)
- 3. Onderwijs en opleiding
- 4. Werkgelegenheid, werving en selectie
- 5. Essentiele private en publieke uitkeringen en diensten (toeslagen)
- 6. Rechtshandhaving
- 7. Migratie, asiel en grensbewaking
- 8. Judiciële en democratische processen





The work illustrates a popular type of algorithm called a genetic evolution.
Rens Dimmendaal / Better Images of AI / Man / CC-BY 4.0

Eisen aan hoog-risico AI en diens aanbieder

- › Conformiteit beoordelen
 1. Risicomanagement
 2. Data en databeheer
 3. Technische documentatie
 4. Logs bewaren
- › Registreren in Europese database
- › CE-markering hanteren
 5. Transparantie en gebruikersinstructie
 6. Human oversight mogelijk
 7. Accuraatheid en robuustheid
 8. cyberveiligheid
- › Monitoren mogelijk maken



Verplichtingen voor gebruikers van AI

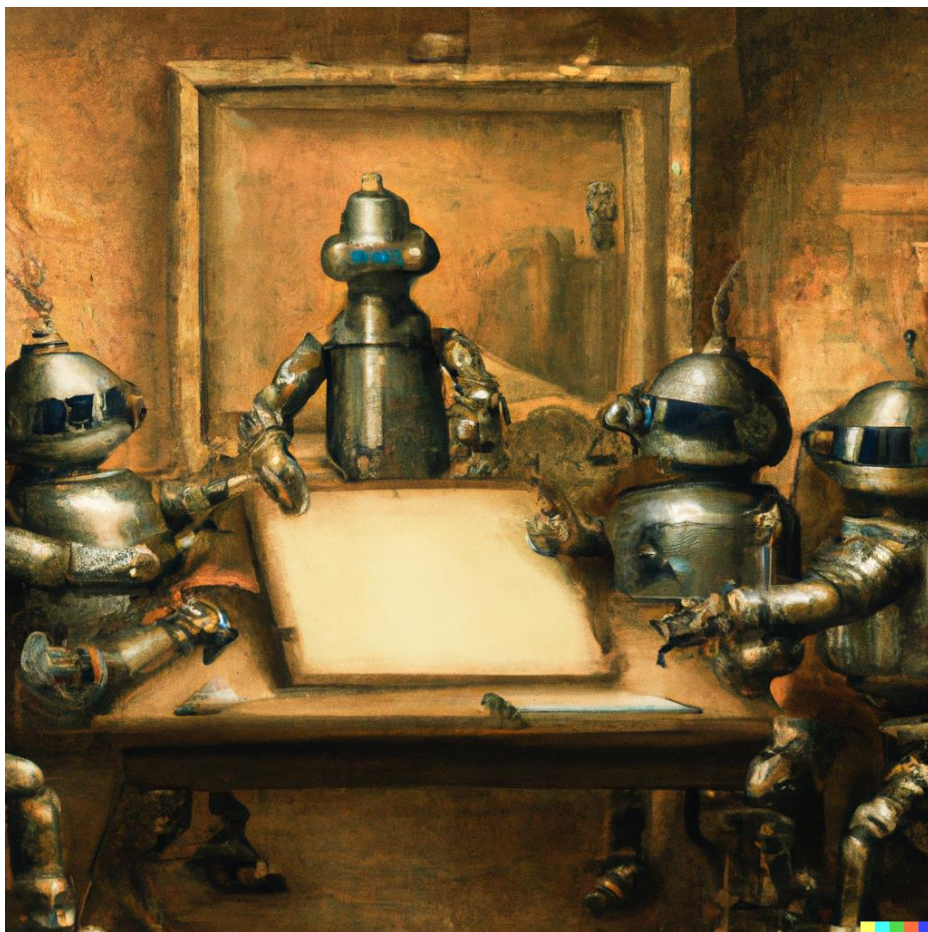


Image created by Dall-E, prompt design by Cas Mevissen

- > **Gebruiker in de AI Act** is de entiteit die het AI-systeem inzet, niet de persoon die met de gevolgen te maken krijgt.
- > Verplichtingen AI-verordening:
 - Gebruiken volgens de handleiding van de aanbieder
 - Menselijk toezicht instellen
 - Werking van het systeem monitoren en loggen
 - Risico's rapporteren
 - Relevante trainingsdata gebruiken
- > Bij aanpassing systeem: gebruiker wordt aanbieder



Conformiteit beoordelen

- > Beoordeling door **derde partij** (NoBo)
 - Gereguleerde producten (annex II)
 - AI-systemen voor biometrische identificatie
- > Beoordeling door **aanbieder zelf**
 - Alle andere hoog-risico toepassingsgebieden
- > **Geen** beoordeling
 - Andere risicocategorie dan hoog-risico
- > Vrijwillige afspraken (Codes of Conduct) om aan eisen te voldoen worden aangemoedigd



