

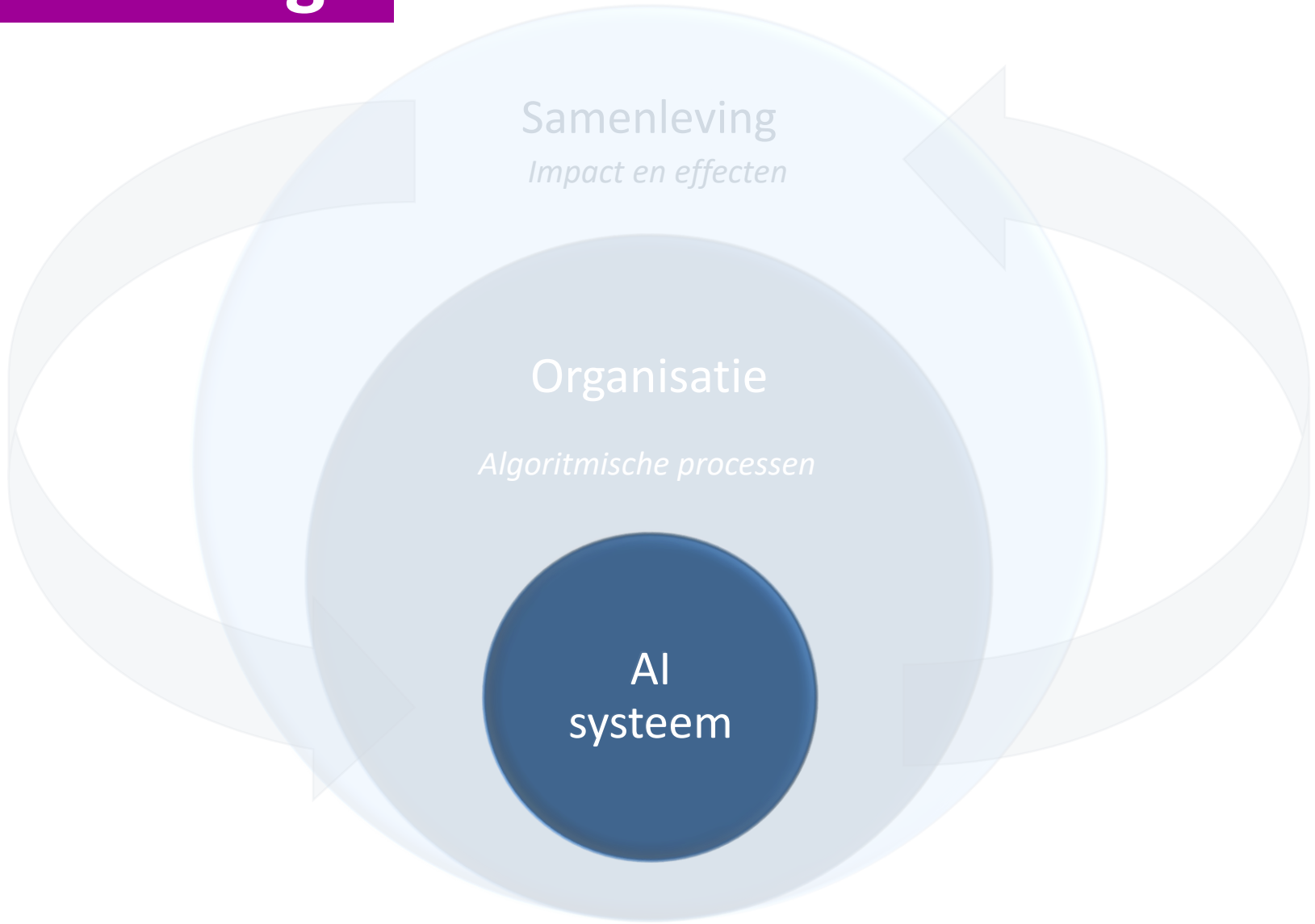
Beheersing van AI:
De AI-verordening is een puzzelstukje

Sven Stevenson

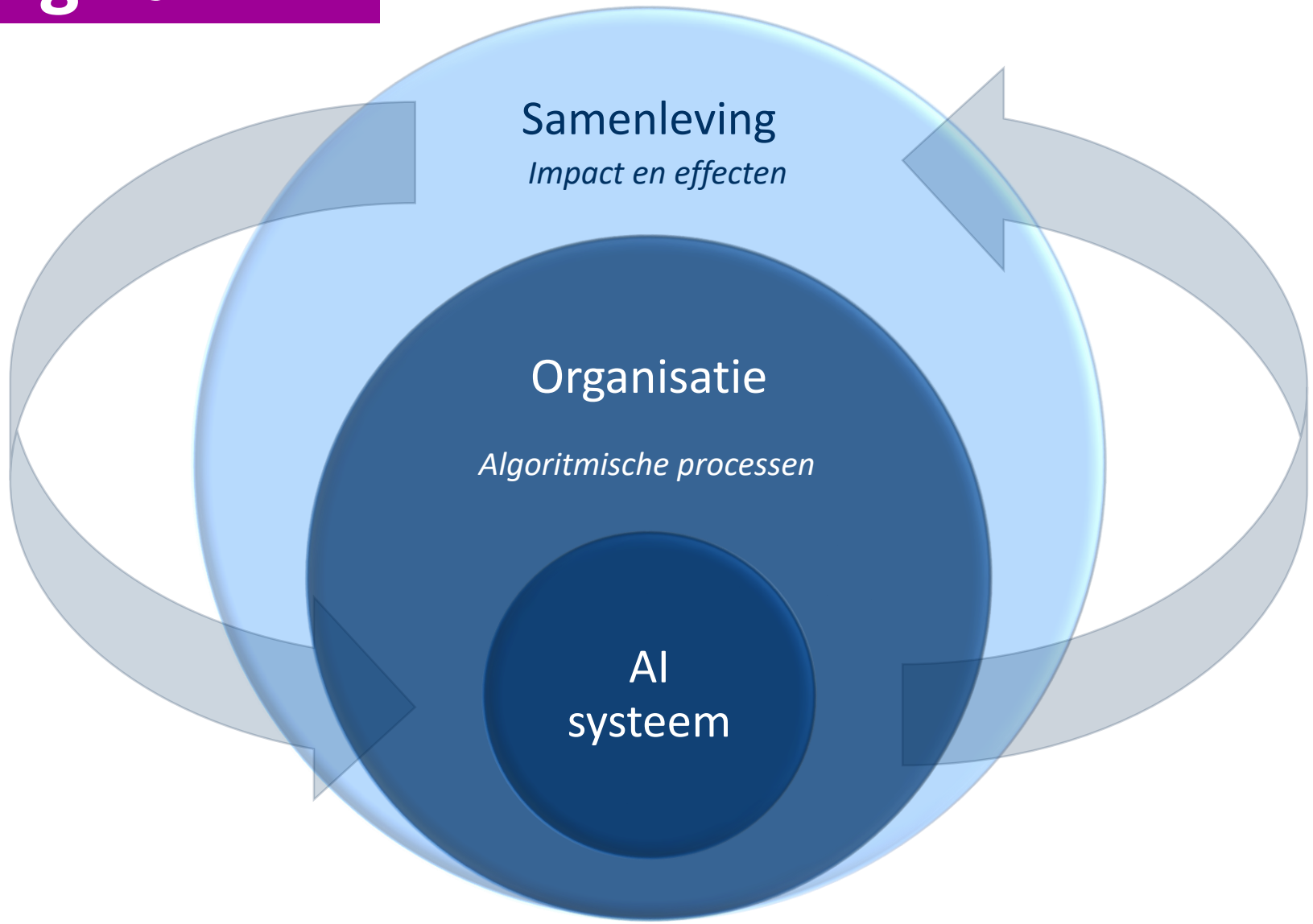
Directie Coördinatie Algoritmes

AUTORITEIT
PERSOONSGEGEVENS

De AI verordening



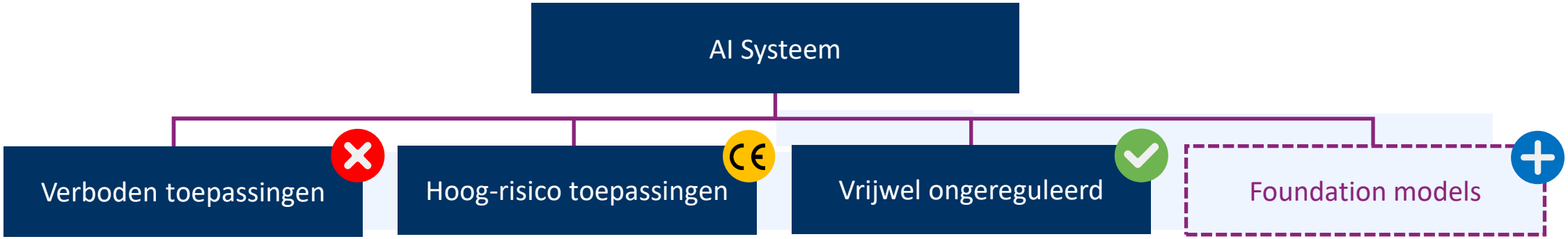
Beheersing van AI



Producttoezicht

- De AI verordening is van toepassing op **AI systemen**.
- De AI verordening gaat vooral over **ontwikkeling van** AI systemen.
- AI systemen moeten **voor ze op de markt** worden gebracht voldoen aan eisen.

Risicogebaseerde regulering



Bepaalde AI-toepassing worden expliciet **verboden**

- Voorbeeld: AI-toepassingen voor *social scoring*

Een brede groep van AI-toepassing die classificeren als **hoog risico** moeten zijn goedgekeurd en voldoen aan specifieke regelgeving voorafgaand en tijdens gebruik (en aanbieding op markt)

- Voorbeeld: AI-toepassingen voor het filteren van sollicitaties

AI-systemen die interactie hebben met personen (of content generen) moeten zichzelf als AI-systeem kenbaar maken

Onderhandelingsvraagstuk is een aparte categorie met specifieke verplichtingen voor aanbieders van foundation models (e.g. GPT4)

- Voorbeeld: specifieke data governance eisen, mede ter verificatie van de geschiktheid van de databronnen

Hoog-risico toepassingen



Voorbeelden:

- Werving en selectie
- Beoordeling studenten en leerlingen
- Rechtspraak
- Kritieke infrastructuur

Publieke dienstverlening

“Toegang tot en gebruik van essentiële particuliere en openbare diensten en uitkeringen:

- AI-systemen die bedoeld zijn om door of namens overheidsinstanties te worden gebruikt om te beoordelen of natuurlijke personen in aanmerking komen voor essentiële overheidsuitkeringen en -diensten, evenals voor het verlenen, beperken, intrekken of terugvorderen van dergelijke uitkeringen en diensten;”

Voorschriften AI systeem

Risicomanagement

Transparantie

Datakwaliteit

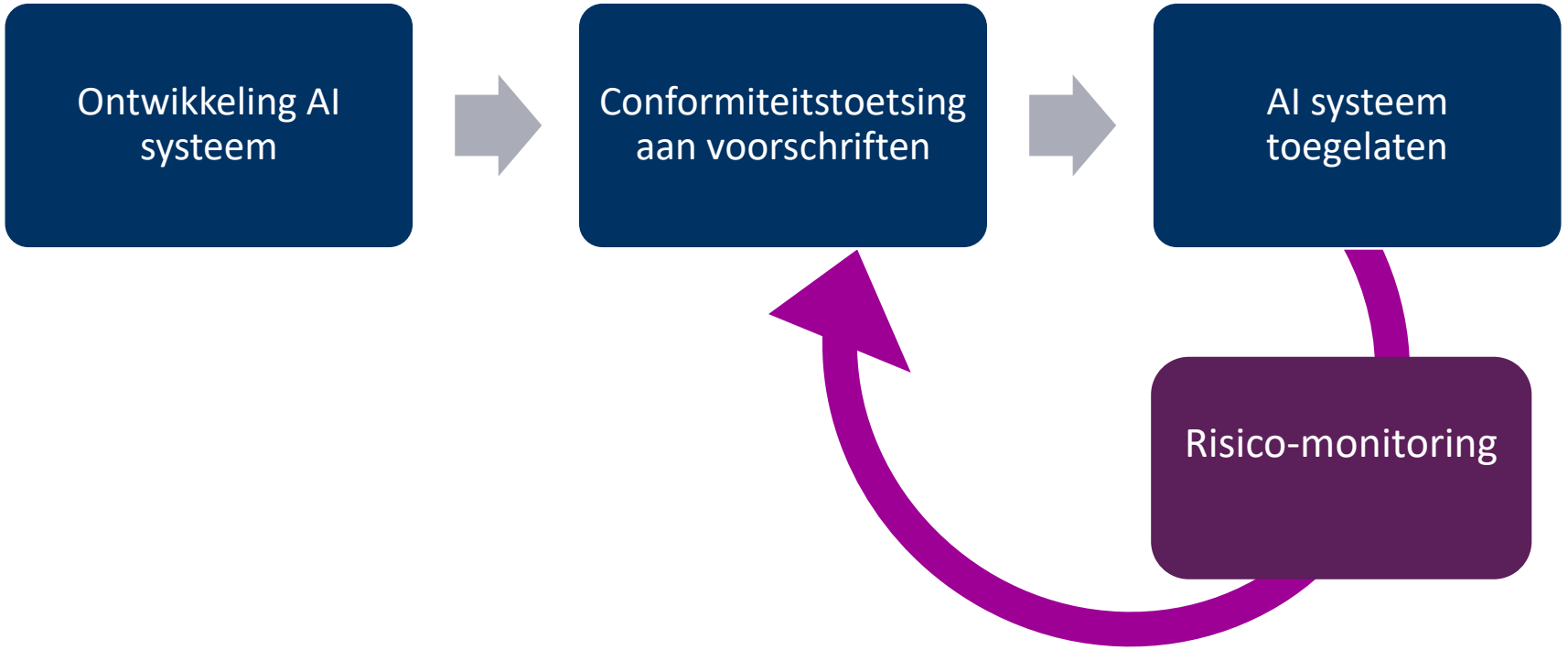
“Human in the loop”

Logging

Documentatie

Conformiteitstoetsing

- Let op: Conformiteitstoetsing is bij veel hoog risico systemen (lees: een bijlage III systemen) een *self assessment*.



Rollen en verantwoordelijkheden

Ontwikkelaar (“aanbieder”) CE

- “een [entiteit] die… een AI-systeem **ontwikkelt** of **laat ontwikkelen** en dat systeem **in de handel brengt** of **in gebruik stelt** onder de eigen naam of merknaam, al dan niet tegen betaling.”
- Moet voldoen aan voorwaarden, bijv. risicomanagement, transparantie en datakwaliteit.
- Moet AI systeem registreren in database, incidenten melden aan toezichthouder en evt. fouten corrigeren, of AI systeem van de markt halen.

Gebruiker

- “een [entiteit], waaronder een overheidsinstantie, agentschap of ander orgaan, onder wiens verantwoordelijkheid een AI-systeem wordt gebruikt.”
- Moet AI systeem gebruiken volgens de gebruiksaanwijzing, zorgvuldig zijn met inputdata, bij incidenten deze melden aan ontwikkelaar en evt. stoppen met gebruik van AI systeem.
- Betrekt informatie over AI systeem in DPIA.

Tegen wie kan de toezichthouder optreden?

Toezichthouder kan eisen dat de exploitant (= zowel de aanbieder als de gebruiker) maatregelen neemt, uit de handel neemt of terugroept

Artikel 65

AI-systeem niet aan de eisen en verplichtingen van deze verordening voldoet, gelast [de toezichthouder] de betrokken exploitant onverwijld passende corrigerende maatregelen te nemen [om het systeem] conform te maken, uit de handel te nemen of terug te roepen.

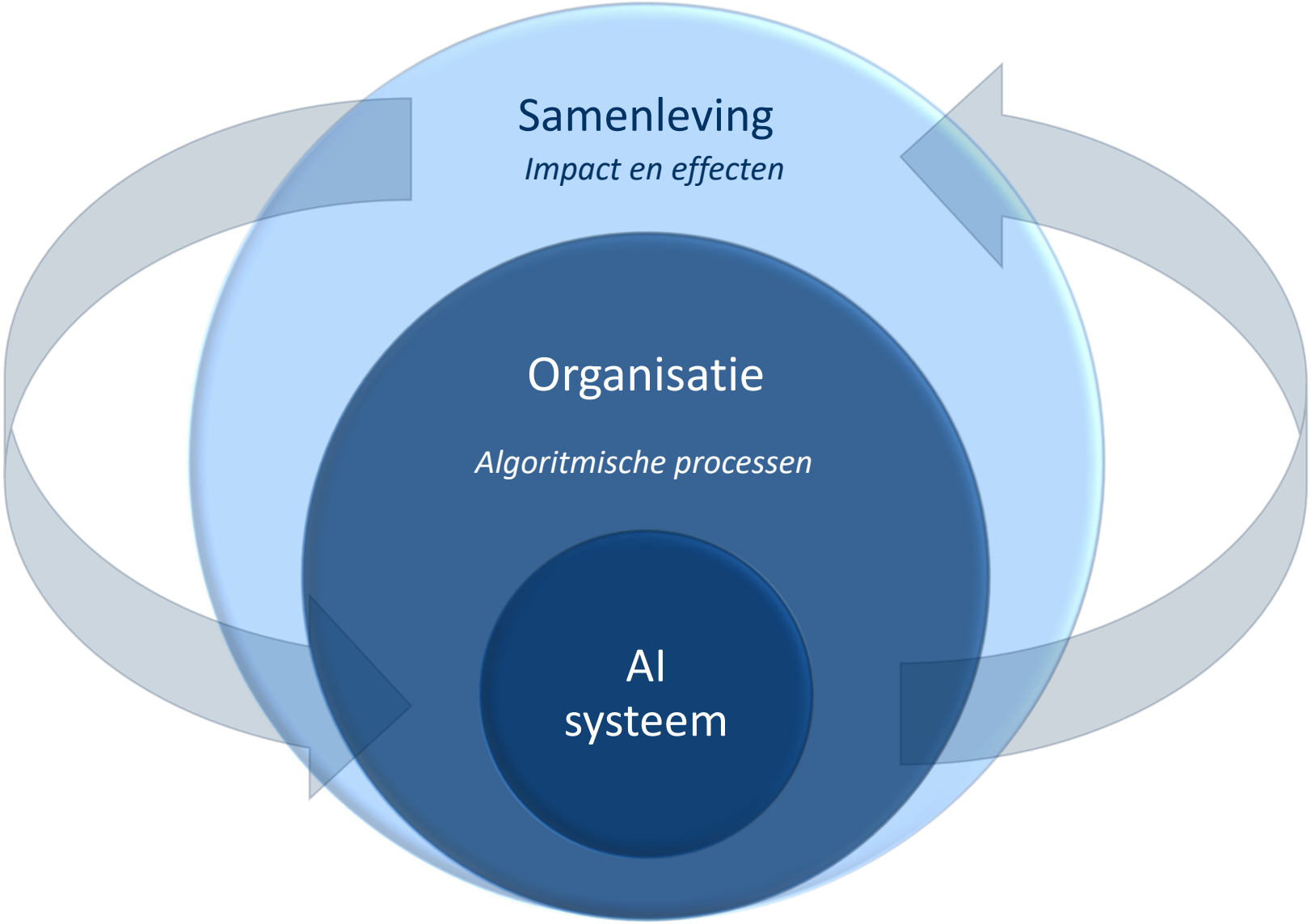
Artikel 67

Indien de markttoezichthouder (…) vaststelt dat een AI-systeem dat voldoet aan deze verordening, toch een risico inhoudt voor de gezondheid of veiligheid van personen, (…) Unie- of interne recht ter bescherming van grondrechten of voor andere aspecten van de bescherming van algemene belangen (…) alle passende maatregelen neemt om ervoor te zorgen dat het betrokken AI-systeem dat risico niet meer inhoudt [of om het systeem] uit de handel te nemen of terug te roepen

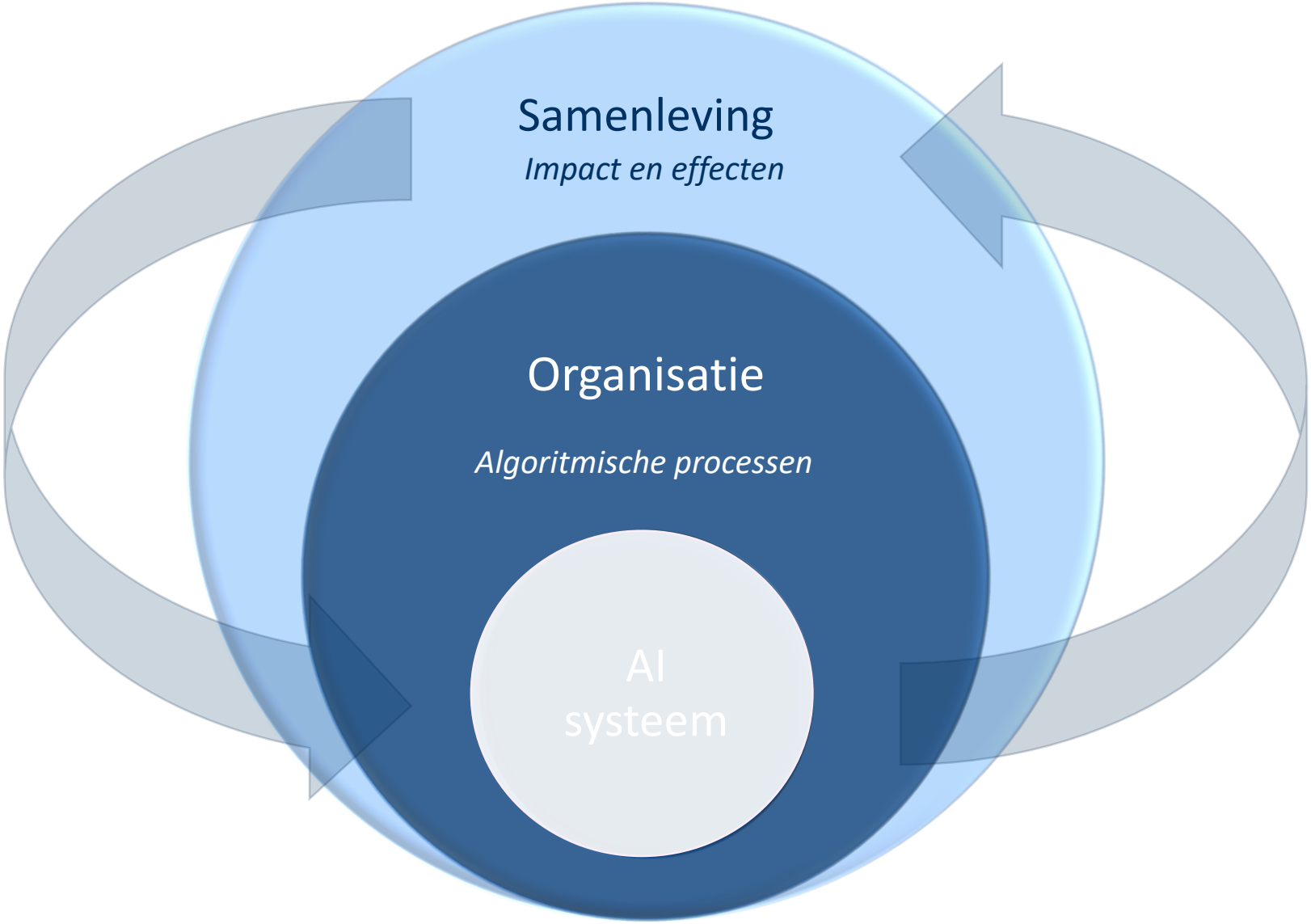
AI verordening – Tijdlijn



Voorbij de AI verordening

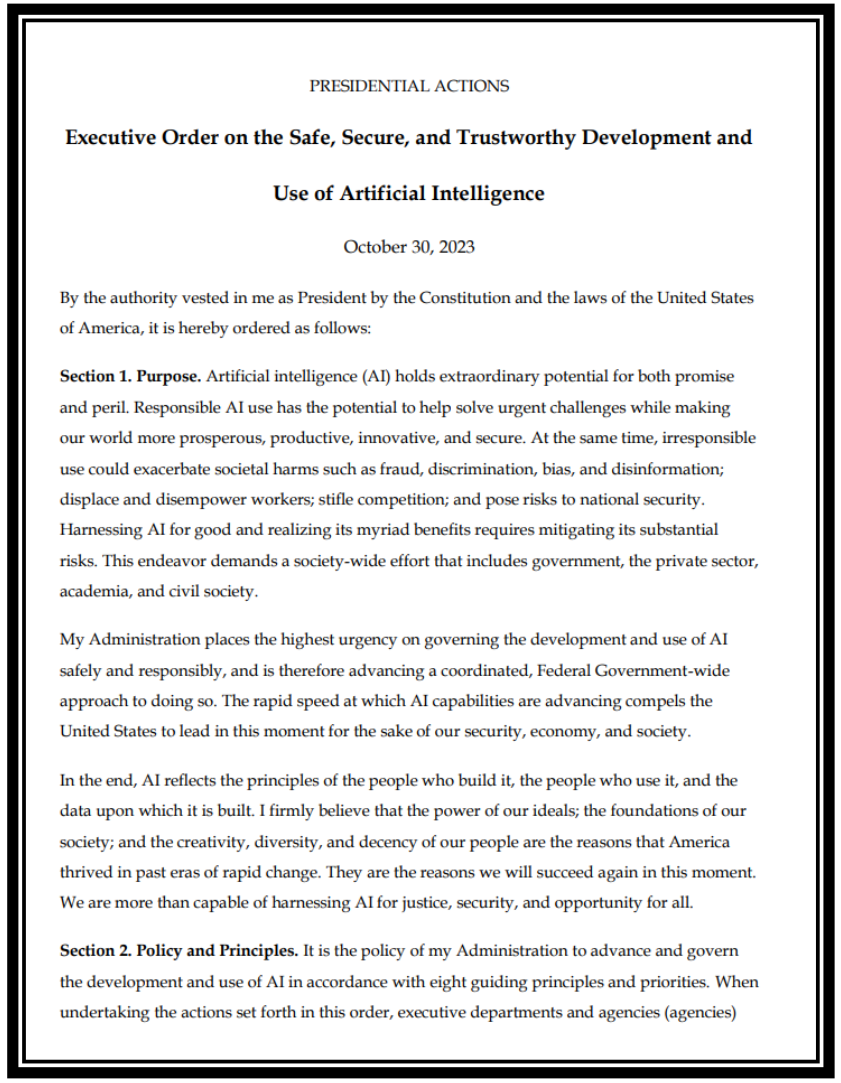


Voorbij de AI verordening



Naar stelsel voor beheersing van AI

- Organisatorische inrichting ter beheersing van AI- en Algoritmische processen. Bijvoorbeeld aanwijzen van:
  - Een Chief AI Officer?
  - Een AI Governance Board?
  - Een Functionaris Algoritmes?



PRESIDENTIAL ACTIONS

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

October 30, 2023

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose. Artificial intelligence (AI) holds extraordinary potential for both promise and peril. Responsible AI use has the potential to help solve urgent challenges while making our world more prosperous, productive, innovative, and secure. At the same time, irresponsible use could exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and pose risks to national security. Harnessing AI for good and realizing its myriad benefits requires mitigating its substantial risks. This endeavor demands a society-wide effort that includes government, the private sector, academia, and civil society.

My Administration places the highest urgency on governing the development and use of AI safely and responsibly, and is therefore advancing a coordinated, Federal Government-wide approach to doing so. The rapid speed at which AI capabilities are advancing compels the United States to lead in this moment for the sake of our security, economy, and society.

In the end, AI reflects the principles of the people who build it, the people who use it, and the data upon which it is built. I firmly believe that the power of our ideals; the foundations of our society; and the creativity, diversity, and decency of our people are the reasons that America thrived in past eras of rapid change. They are the reasons we will succeed again in this moment. We are more than capable of harnessing AI for justice, security, and opportunity for all.

Section 2. Policy and Principles. It is the policy of my Administration to advance and govern the development and use of AI in accordance with eight guiding principles and priorities. When undertaking the actions set forth in this order, executive departments and agencies (agencies)



AUTORITEIT
PERSOONSGEGEVENS