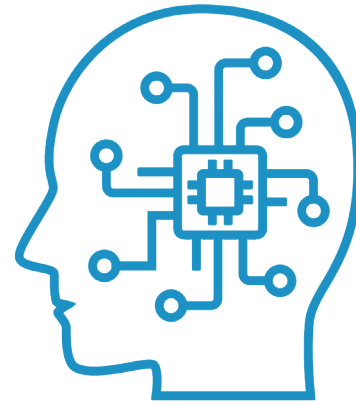


# Intelligent omgaan met de AI-verordening

De opkomst van AI lijkt sinds vorig jaar in een enorme stroomversnelling terecht te zijn gekomen. In veel organisaties wordt al volop gewerkt of geëxperimenteerd met Chat-GPT of CoPilot en/of andere tools. Maar er was al zoveel AI wat we ons niet realiseerden. Ook in de acceptatie en claimverwerking maken we misschien al bewust of onbewust gebruik van kunstmatige intelligentie. Ja, en inderdaad ook bij Netflix, Booking en je navigatie. Maar we gaan het nu hebben over de invoering van de AI-act.



## Wanneer moeten we aan de slag?

U bent al druk met de DORA, misschien ook met de CSRD en waarschijnlijk diverse andere projecten. Dan hebben we voor u ook nog goed en slecht nieuws. Om met het slechte nieuws te beginnen: met de Europese AI-verordening (EU 2024/1689) komt er nog een project bij. De AI-verordening is gepubliceerd op 12 juli 2024 en treedt in werking op 2 augustus 2025. Nog slechter nieuws misschien: de eerste twee hoofdstukken zijn al vanaf 2 februari 2025 van kracht. Een beetje goed nieuws wellicht: de eerste invoering betreft alleen het hoofdstuk over (vanaf februari) verboden praktijken.

Waarschijnlijk doet u daar niet aan, dus u heeft nog tot begin augustus en wie weet valt de impact ook nog wel mee.

## Waar gaat de AI-verordening over?

Het gebruik van kunstmatige intelligentie is niet meer te stoppen, maar het is niet zonder meer risicoloos. Het doel van de AI-verordening is om de ontwikkeling van AI te bevorderen, maar ook om regels te stellen teneinde te zorgen voor betrouwbare en mensgerichte AI-systemen. Het gaat om de bescherming van de in het Europese Handvest verankerde grondrechten, waaronder bescherming van gezondheid, milieu en de democratie.

## Definitie kunstmatige intelligentie

“Een machine-gebaseerd systeem dat is ontworpen om te werken met verschillende niveaus van autonomie 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.”

Het begrip kunstmatige intelligentie wordt ook gedefinieerd, maar ga daarvoor even rustig zitten. Kernbegrippen lijken autonomie en aanpassingsvermogen te zijn. Bij veel van uw systemen zoals polis- en claimsadministratie, de financiële administratie en de talloze Excel-spreadsheets zal doorgaans geen aanpassingsvermogen aan de orde zijn. Maar als bijvoorbeeld uw (al dan niet uitbestede) claimproces automatisch mogelijke signalen van fraude detecteert, dan is de kans groot dat de AI-Verordening betekent dat u flink aan de slag moet met de implementatie van AI-Verordening.

## Vier soorten van AI-systemen

Het belangrijkste gevolg van de AI-verordening is dat u uw systemen moet gaan classificeren in vier soorten AI-systemen:

- 1. Verboden AI-systemen:** Systemen die een onaanvaardbaar risico vormen, zoals subliminale technieken die gedrag manipuleren of AI die kwetsbare groepen zoals kinderen uitbuiten.
- 2. Hoog-risico AI-systemen:** Deze worden ingezet in kritieke sectoren, waaronder ook de financiële industrie. Denk daarbij aan AI-systemen die worden gebruikt voor risicobeoordeling, kredietwaardigheid, fraudedetectie en klantmonitoring. Ze moeten voldoen aan strikte eisen voor transparantie, veiligheid en naleving van regelgeving, om discriminatie, fouten of inbreuken op grondrechten te voorkomen.
- 3. Beperkte-risico AI-systemen:** AI-systemen die bepaalde transparantieplichtingen hebben, bijvoorbeeld chatbots, waarbij gebruikers moeten weten dat ze met AI communiceren.
- 4. Laag-risico AI-systemen:** De meeste AI-toepassingen, zoals spamfilters, waar minimale regelgeving geldt, omdat ze weinig risico vormen voor gezondheid of rechten.

## Hoe vaak komen bepaalde woorden voor in de Europese AI-verordening

- Het woord **'risicobeheersing'** komt 10 keer voor.
- De term **'audit'** komt 4 keer terug, maar vooral in de bijlagen als het gaat om het vaststellen van de effectiviteit van het kwaliteitsbeheersysteem.
- De term **'kwaliteitsbeheer'** komt daarentegen ca. 40 keer voor in de verordening (inclusief de overwegingen).

De classificatie van de systemen heeft grote gevolgen voor de impact van de regelgeving. Vooral de hoog-risico AI-systemen brengen veel verplichtingen met zich mee.

## Risicobeheersing bij de 'hoog-risico AI-systemen'

De meeste aandacht zal moeten uitgaan naar de 'hoog-risico AI-systemen'. Voor deze systemen moeten organisaties een systeem van risicobeheersing ontwikkelen. Dat wil zeggen dat systemen getest moet worden, maar ook worden gemonitord (en er moeten correctiemechanismen zijn).

Op de systemen moet ook menselijk toezicht zijn (artikel 14) en de systemen moeten voldoende nauwkeurig en robuust zijn, maar ook de cyberbeveiliging rondom de systemen moet effectief zijn (artikel 15). Organisaties moeten ook transparant zijn over het gebruik van de AI-systemen. Artikel 49 van de verordening vereist ook dat deze systemen worden geregistreerd in een Europese database, teneinde toezicht mogelijk te maken en transparantie te borgen. Deze database zal op 'gebruikersvriendelijke wijze' openbaar worden gemaakt. Het woord 'risicobeheersing' komt 10 keer voor in de verordening, maar ook de term 'audit' komt 4 keer terug, maar vooral in de bijlagen als het gaat om het vaststellen van de effectiviteit van het kwaliteitsbeheersysteem. De term 'kwaliteitsbeheer' komt daarentegen ca. 40 keer voor in de verordening (inclusief de overwegingen). De soms abstracte formuleringen zullen zeker bij de eerste invoering voor de nodige uitdagingen zorgen.

## Stok achter de deur

De Autoriteit Persoonsgegevens is in Nederland aangewezen als toezichthouder op de naleving van de AI-Verordening en net als bij eventuele non-compliance met de AVG kan de toezichthouder forse boetes opleggen. Bij 'verboden praktijken' kan het zelfs gaan over de hoogste van 7% van de wereldwijde omzet of €35 miljoen. Nu zullen financiële instellingen niet snel in deze categorie belanden, maar non-compliance kan nog steeds leiden tot boetes van 1% tot 3% van de wereldwijde omzet, of €7,5 miljoen tot €15 miljoen.

## Conclusie

Met de invoering van de AI-verordening aan de horizon is het verstandig om een AI-beleid te gaan ontwikkelen voor het gebruik en het classificeren van AI-systemen die binnen de organisatie worden gebruikt. Ook is het op voorhand goed om na te denken over de wijze waarop invulling kan worden gegeven aan de toch wel forse eisen die worden gesteld aan hoog-risico AI-systemen en de organisatie van het kwaliteitsbeheer rondom deze systemen. Maar geen zorgen ...

we helpen u graag daarbij!

Ronald van de Langenberg

Algemeen Directeur InAudit

06-24 48 68 92

