PELS RIJCKEN HIGHBERG

Whitepaper

AI Act voor overheden

Impact en voorbereiding

De Artificiële Intelligentie Verordening (AI Act) is op 13 maart 2024 definitief goedgekeurd door het Europees Parlement. De AI Act is daarmee de eerste vorm van regelgeving ten aanzien van kunstmatige intelligentie in de EU en richt zich onder andere op ontwikkelaars, distributeurs en gebruikers van AI-systemen. Dat zijn systemen die bijvoorbeeld worden ingezet voor voorspellingen, classificaties en analyses. Met de komst van deze verordening worden burgers en bedrijven in de EU beter beschermd tegen onverantwoord gebruik van AI.

De AI Act gaat uit van een risico-gebaseerde aanpak. Dat betekent dat afhankelijk van het domein waarin een AI-systeem wordt ingezet, meer of minder strenge regels gelden. Transparantie over de manier waarop AI-systemen tot stand zijn gekomen en de vraag welke technieken en datasets daarvoor zijn gebruikt spelen daarbij een belangrijke rol. De potentiële impact op overheden kan groot zijn en vraagt om tijdige voorbereiding.

De AI Act is van toepassing als je in je werkproces algoritmes gebruikt die onder de definitie van AI-systeem in de AI Act vallen. Hiervoor is onder andere vereist dat AI-systemen zelfstandig resultaten kunnen afleiden uit ingevoerde gegevens. Enige mate van autonomie is dus vereist. Ontbreekt het hieraan, dan valt de betreffende AI-toepassing niet onder deze verordening.

Risicogebaseerde aanpak

De AI Act onderscheidt een aantal risicocategorieën. Zoals gezegd, het uitgangspunt is dat hoe groter het risico is, hoe strenger de regels zijn die hiervoor gelden.

Verboden AI

De hoogste risicocategorie bevat AI-systemen die een dermate grote inbreuk maakt op fundamentele (mensen)rechten dat deze in beginsel is **verboden**. Voorbeelden hiervan zijn AI-systemen bedoeld voor emotieherkenning op de werkvloer, manipulatie van menselijk gedrag en van kwetsbare groepen, sociale kredietsystemen, realtime biometrische identificatie op afstand in de publieke ruimte voor rechtshandhaving en voorspelling van strafbaar gedrag op basis van profilering.

Certified B Corporation

Let op: dit verbod wordt al van kracht na **zes maanden** na inwerkingtreding van de AI Act.

Hoog risico AI - meest gereguleerd

Veruit de meeste verplichtingen uit de AI Act gaan gelden voor zogenaamde hoog risico AI-toepassingen. Een AI-systeem valt in beginsel in deze categorie als wordt voldaan aan één van de volgende voorwaarden:

- Het AI-systeem is een product (of een veiligheidscomponent hiervan) waarvoor op grond van de in bijlage 1 van de AI Act genoemde regelgeving een conformiteitsbeoordeling door een derde partij noodzakelijk is (bijvoorbeeld medische apparatuur en radioapparatuur)
- Het valt onder één van de toepassingsgebieden die zijn opgenomen op de limitatieve lijst in bijlage 3 van de AI Act

In deze laatste categorie valt een aantal specifiek benoemde AI-toepassingen, zoals op het gebied biometrische identificatie, het beheer van kritieke (digitale) infrastructuur, toelating tot onderwijs of opleidingen, werving en selectie van medewerkers, toegang tot essentiële dienstverlening van de overheid (zoals gezondheidszorg of uitkeringen), rechtshandhaving, migratie-, asiel- en grens-beheer, rechtsbedeling of het beïnvloeden van democratische processen.

Rollen en vereisten

Heb je te maken met een hoog risico AI, dan is het van belang om te beoordelen welke rol of rollen je als organisatie vervult. De belangrijkste hiervan zijn die van Gebruiksverantwoordelijke (de organisatie die het AI-systeem gebruikt, in het Engels: de Deployer) en die van Aanbieder (de organisatie die het AI-systeem ontwikkelt, in het Engels: de Provider). Daarnaast zijn er specifieke regels voor de rollen van Importeur, Vertegenwoordiger in de EU en Distributeur.

Belangrijke eisen waaraan een **Aanbieder** moet voldoen zijn:

- Ervoor zorgen dat bij de ontwikkeling van de AI-toepassing aan alle eisen voor hoog risico AI-systemen wordt voldaan (o.a. op het gebied van risicomanagement, trainings- en validatiedata, technische documentatie en transparantie)
- Werken op basis van een kwaliteitsmanagementsysteem
- Het uitvoeren van een conformiteitsassessment
- Registratie in een EU-database

Ben je als organisatie (tevens) de **Gebruiksverantwoordelijke**, oftewel de gebruiker van een hoog risico AI-systeem, dan gelden onder andere eisen op de volgende terreinen:

- Menselijk toezicht bij de toepassing van het AI-systeem
- Gebruik van kwalitatief goede data
- Monitoring van de uitkomsten en ingrijpen als daar aanleiding voor is
- Het bijhouden van logbestanden
- Indien van toepassing: het informeren van werknemers of hun vertegenwoordiging

Voor overheden en uitvoerders van publieke diensten die hoog risico AI-systemen gebruiken, geldt daarnaast nog de eis dat hiervoor een mensenrechten assessment moet worden uitgevoerd (bijvoorbeeld een IAMA).

Voor hoog risico AI-toepassingen gaat in de meeste gevallen een overgangstermijn van **twee tot drie jaar** gelden, afhankelijk van het risico. Hoog risicosystemen die reeds in gebruik zijn, vallen (nog) niet onder de AI Act. Dit betekent dat voor nieuwe hoog risico toepassingen de nieuwe regels vanaf 2026 (deels) van toepassing zullen zijn.

Uitzondering - hoog risico AI-systemen zonder hoog risico

AI-systemen waarvan duidelijk is dat deze geen significant risico vormen op schade voor veiligheid, grondrechten en gezondheid hoeven niet te worden aangemerkt als hoog risico. De AI Act geeft hiervoor vier mogelijkheden. Het gaat dan om AI-systemen die:

- Slechts een **beperkte procedurele taak** uitvoeren
- Gebruikt worden voor het **verbeteren van uitkomsten van menselijke activiteit** (controleren op taal- en spelfouten in een brief)
- Slechts een **voorbereidende taak** hebben (vertalen van brondocumenten, indexeren of koppelen van data)
- Afwijkingen in **menselijke beslispatronen** signaleren

Let op: mocht je als aanbieder van mening zijn dat er sprake is van één van bovenstaande uitzonderingen, dan dien je dit schriftelijk te kunnen onderbouwen. Bij een AI-systeem dat gebruik maakt van profilering van natuurlijke personen, mogen deze uitzonderingen niet worden toegepast.

Laag risico AI - transparantievereisten

Voor AI-toepassingen die niet onder de categorieën verboden of hoog risico vallen, maar wel output genereren, gelden transparantievereisten. Zo moet het voor degene die met deze output te maken krijgt duidelijk moet zijn dat de content door AI is gegenereerd. Een voorbeeld van een laag risico AI-systeem is het gebruik van een chatbot die vragen van burgers of klanten beantwoordt, of een door AI gegenereerde brief of afbeelding. Leveranciers van chatbots, deepfake technieken of generatieve AI-systemen, zoals het populaire ChatGPT van OpenAI, moeten duidelijk aangeven wat de risico's zijn bij het gebruik van deze tools en waarvoor deze (beter) niet ingezet kunnen worden.

De impact van de AI Act op overheden

De potentiële impact van de AI Act op organisaties in zowel de publieke als private sector is groot. Voor overheden geldt dat AI-systemen die zij gebruiken bij het toekennen van bepaalde rechten aan burgers als hoog risico AI classificeren. Denk hierbij aan AI-systemen die gebruikt worden bij de toekenning van uitkeringen, toeslagen en studiefinanciering. Daarnaast gelden ook AI-systemen die worden gebruikt bij de opsporing, de rechtspraak of het beheer van het wegen, sluizen en in de energievoorziening onder de categorie hoog risico.

Startpunt

Om op tijd aan de verplichtingen uit de AI Act te kunnen voldoen is het van belang hiermee nu al een begin te maken. Daartoe kun je in ieder geval de volgende stappen zetten:

- Inventariseer welke toepassingen en algoritmen die in gebruik zijn kwalificeren als AI
- Bepaal welke risiconiveau hierop van toepassing is (verboden, hoog of laag)
- Bepaal welke rol je als organisatie hebt in de ontwikkeling en het gebruik van de AI (Aanbieder en/of Gebruiksverantwoordelijke)
- Breng in kaart aan welke wettelijke eisen moet worden voldaan
- Stel vast welke acties nog nodig zijn en stem dit (indien van toepassing) af met de Aanbieder

Een groot deel van de verplichtingen die de AI Act oplegt, zoals goed risicomanagement, zorgvuldige selectie van data en het vastleggen van ontwerpkeuzes, zijn reeds best practices bij de ontwikkeling van AI-systemen. Indien je hieraan nog niet voldoet, is het sowieso verstandig om hieraan aandacht te besteden.

Onze dienstverlening voor verantwoorde inzet van AI

Highberg en Pels Rijcken beschikken samen over alle juridische, ethische, technische en organisatorische kennis die nodig is voor verantwoord datagebruik en om grip te krijgen op AI. Wij kunnen u helpen door:

- Met u in kaart te brengen in welke mate binnen uw organisatie gebruik gemaakt wordt van **AI**
- Het classificeren van uw **AI-systemen** in de juiste **risicocategorie**
- Het uitvoeren van een mensenrechtentoets, bijvoorbeeld een **IAMA**
- Advisering over **data ethiek** en **datagovernance** bij het gebruik van AI en algoritmes
- Met u beleid te ontwikkelen voor besluitvorming op basis AI, inclusief bijbehorend juridisch en ethisch kader

Over Highberg en Pels Rijcken

Highberg en Pels Rijcken werken nauw samen in de advisering en ondersteuning van overheden bij digitalisering en verantwoord datagebruik. We kijken hierbij nadrukkelijk niet alleen naar wat kan en wat mag, maar ook naar wat wenselijk is. De expertises van Highberg en Pels Rijcken zijn hierbij in hoge mate complementair, zodat we in staat zijn om van begin tot eind te helpen bij de implementatie van nieuwe wet- en regelgeving.

Wilt u meer weten over de AI Act, of wat wij in bredere zin voor u kunnen betekenen?
Neem dan contact op met een van onderstaande contactpersonen:

Contactpersonen Highberg/Pels Rijcken

Laura Natrop
Manager Digital Law, Highberg
t 06 207 035 92, laura.natrop@highberg.com

Sebastiaan Bouthoorn
Senior consultant AI Act, Highberg
t 06 515 805 37, sebastiaan.bouthoorn@highberg.com

Christian Verhagen
Partner, Highberg
t 06 133 760 49, Christian.verhagen@highberg.com

Jeroen Naves
Partner, Pels Rijcken
t 06 537 362 31, jeroen.naves@pelsrijcken.nl