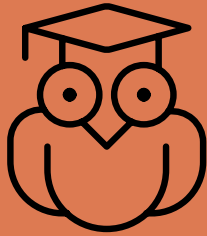


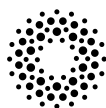
surf.nl

npuls.nl



AI Act in het kort.

SURF



Npuls

AI Act in het kort

4 februari 2025

Geschreven door Sanderijn Kuijvenhoven en Duuk Baten
Met bijdrage van Floortje Jorna, Menno Jehée, Henriette Dietz
en Samuel Kernan Freire



Op deze uitgave is de Creative Commons Naamsvermelding-
GelijkDelen 4.0 Internationaal-licentie (CC BY-SA 4.0) van toepassing.
Bij gebruik van dit werk dient de volgende referentie te worden vermeld:
SURF & Npuls. (2025). AI ACT in het kort.

Inhoud

| | |
|---|----|
| Samenvatting | 4 |
| Introductie | 4 |
| Waarom de AI regelgeving | 7 |
| AI Act tijdelijk | 7 |
| AI Act en andere wetgeving | 8 |
| AI Act begrippenlijst | 9 |
| Rollen met betrekking tot een AI-systeem | 10 |
| Risico-regulering AI Act | 13 |
| Verboden AI-systemen | 13 |
| Hoog risico AI-systemen | 14 |
| Verplichtingen in de AI-verordening | 17 |
| Eisen voor hoog-risico AI-systemen | 18 |
| Eisen voor General Purpose AI modellen | 19 |
| Transparantie verplichtingen bij bepaalde AI-systemen | 19 |
| Overige aspecten van de AI-verordening | 21 |
| AI-geletterdheid – artikel 4 | 21 |
| Onderzoek uitzondering – artikel 2 lid 6 & lid 8 | 21 |
| Uitzondering persoonlijk gebruik – artikel 2 lid 10 | 22 |
| Uitzondering opensource licenties – artikel 2 lid 12 | 22 |
| Wat betekent de AI Act voor onderwijsinstellingen? | 23 |

Samenvatting

De AI Act, ook wel de AI-verordening, bestaat uit regels voor het gebruik van Artificiële Intelligentie (AI) in de Europese Unie (EU). De AI Act gaat gefaseerd van kracht, waarbij in augustus 2027 alle onderdelen van de wet gelden. De AI Act heeft een risico benadering voor AI-systemen. Hierbij wordt er per AI-systeem wordt gekeken of en onder welk risico het AI-systeem valt (verboden AI, hoog risico of transparantie risico). Daarnaast heeft de rol van organisaties bij het AI-systeem invloed op de eisen en maatregelen die organisaties moeten ondernemen om te voldoen aan de wetgeving.

Dit document zet de AI Act uiteen en beschrijft de begrippen die in de AI Act worden gebruikt. Het is bedoeld als hulpdocument bij de AI Act, heb je opmerkingen of vragen hierover? Mail dan naar ai-act@surf.nl of stel ze in de [vraagbaak AI](#).

Introductie

Dit document heeft als doel een eerste introductie te geven op de AI Act (AI-verordening). Het is geen samenvatting van de AI Act en heeft ook niet als doel om als naslagwerk gebruikt te worden. Wel biedt het een eerste startpunt om aan de slag te gaan met de AI Act.

Leeswijzer en disclaimer

Als onderwijsinstelling kom je in aanraking met AI-systemen. Misschien omdat je ze zelf ontwikkelt of omdat deze toegepast willen worden in de organisatie. Bij deze gevallen zal je mogelijk met de AI-verordening te maken gaan krijgen. Dit stuk is samengesteld als eerste inzicht in wat de AI-verordening is. Het is niet een compleet overzicht. Aan de inhoud van deze gids kunnen geen rechten worden ontleend. De wettekst van de AI-verordening blijft altijd leidend.

Wat doen SURF en Npuls met de AI Act?

Binnen SURF zijn op het moment van schrijven de geplande activiteiten om leden te ondersteunen met de AI Act beperkt. De publicatie dit document is een eerste stap. Daarnaast kan je, als werknemer bij een onderwijsinstelling, lid worden van onze [AI-act discussie mailinglist](#) om contact te zoeken met collega's binnen de sector.

Binnen de transformatiehub AI en Data van Npuls worden er een aantal projecten uitgevoerd die de AI Act raken. Als eerst het [referentiekader privacy en ethiek 2.0](#), dit is een tweede versie op het referentiekader privacy en ethiek dat zich ook focust op mbo en AI, waarbij ook de AI Act aanbod komt. Daarnaast het project [onderzoek en ontwerp algoritmeregister](#), dat kijkt naar hoe een algoritmeregister er voor de onderwijssector uit kan zien en of een algoritmeregister wenselijk en haalbaar is. Ook het project [AI- en data geletterdheid](#) raakt de AI Act. Waarbij er een landelijk raamwerk ontwikkeld wordt en praktijkvoorbeelden worden verzameld. Meer informatie over de projecten is te vinden op de [community site](#) van de transformatiehub.

Waarom de AI-regelgeving

De AI-verordening, ook wel bekend als de AI Act, bestaat uit regels voor het gebruik van Artificiële Intelligentie (AI) in de Europese Unie (EU). AI biedt veel kansen en voordelen, bijvoorbeeld voor de gezondheidszorg en efficiëntere productiemethoden. Tegelijkertijd brengt AI ook risico's met zich mee. De AI-act is onderdeel van de Europese AI-strategie en is de allereerste uitgebreide AI-wet ter wereld. Het omvat eisen en kaders voor de ontwikkeling en het gebruik van AI-systemen door overheden en marktpartijen. Het is bedoeld om innovatie en economische ontwikkelingen de ruimte te geven terwijl publieke waarden worden beschermd.

AI Act tijdslijn

De AI Act gaat gefaseerd van kracht. In augustus 2024 is de wet van kracht gegaan. Per fase gaan nieuwe gedeeltes van de wet in werking.¹

Februari 2025 - verboden AI en AI-geletterdheid

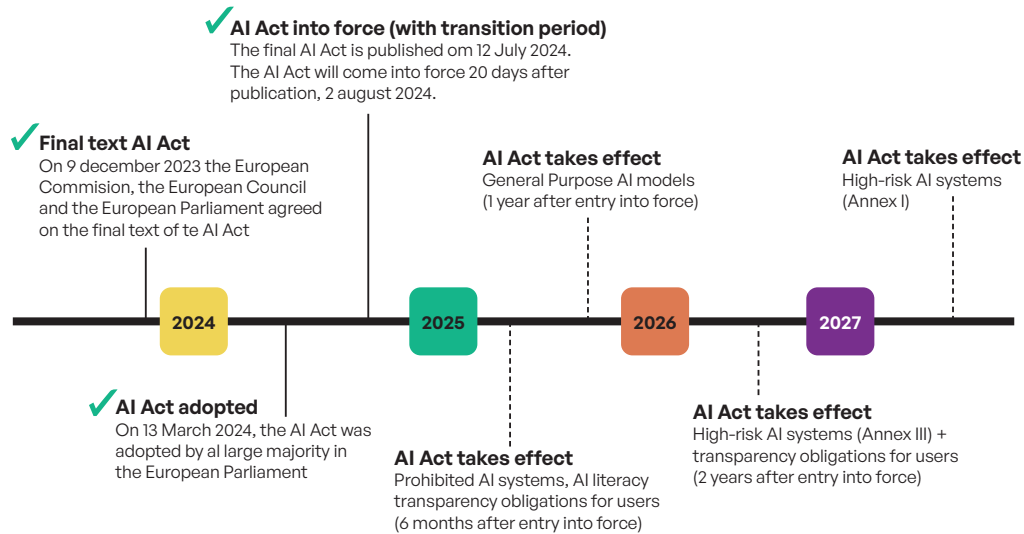
- Augustus 2025 - General Purpose AI modellen
- Augustus 2026 - hoog risico AI-systemen (bijlage 3)
- Augustus 2026 - transparantie verplichtingen voor gebruikers
- Augustus 2027 - hoog risico AI-systemen (bijlage 1)

Verschillende aspecten van de wet behoeven nadere uitwerking. De verwachting hiervoor is dat in de aanloop naar deze data de Europese Commissie/AI Office etc. nog met nadere duiding komt. Bijvoorbeeld voor de AI-testomgevingen voor regelgeving (AI regulatory sandboxes) die vanuit iedere lidstaat op nationaal niveau aangeboden moeten worden.² Daarnaast komt de Europese Commissie met richtlijnen over AI-systeem definities en publiceren ze een archief van praktische voorbeelden voor AI-geletterdheid.³

¹ Art. 113 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

² Art. 57 lid 1 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

³ Press Release (03-02-2025) digital-strategy.ec.europa.eu/en/news/first-rules-artificial-intelligence-act-are-now-applicable



Figuur 1 Tijdslijn AI Act

AI Act en andere wetgeving

De AI Act heeft verschillende raakvlakken met andere (Europese) wetgeving, zoals de AVG, de Digital Service Act, wetgeving over intellectueel eigendom, etc. De AI Act zal vaak in aanraking komen met deze andere wetgevingen. Maar het vervangt de andere wetten niet. Zo kunnen de AVG en de AI Act naast elkaar van toepassing zijn.

AI Act begrippenlijst

Hier volgen de begrippen en definities zoals het in de AI Act staat beschreven.

AI-systeem – artikel 3 lid 1

“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.”⁴

Volgens de AI Act moet een systeem om als AI te worden beschouwd als het aan de volgende eisen voldoet:

- Op een machine gebaseerd zijn.
- Op een bepaald niveau van autonomie functioneren.
- Kan na inzet aanpassingsvermogen vertonen.
- In staat zijn om uit ontvangen input af te leiden hoe output te genereren (zoals voorspellingen, inhoud, aanbevelingen of beslissingen).
- Output kunnen genereren die van invloed kan zijn op fysieke of virtuele omgevingen.

AI-model voor algemene doeleinden (General Purpose AI model) – artikel 3 lid 63

“AI-model voor algemene doeleinden”: een AI-model, ook wanneer het is getraind met een grote hoeveelheid data met behulp van self-supervision op grote schaal, dat een aanzienlijk algemeen karakter vertoont en in staat is op competente wijze een breed scala aan verschillende taken uit te voeren, ongeacht de wijze waarop het model in de handel wordt gebracht, en dat kan worden geïntegreerd in een verscheidenheid aan systemen verder in de AI-waardeketen of toepassingen verder in de AI-waardeketen, met uitzondering van AI-modellen die worden gebruikt voor onderzoek, ontwikkeling of prototypingactiviteiten alvorens zij in de handel worden gebracht.”⁵

AI-systeem voor algemene doeleinden (General Purpose AI-systeem of GP AI-systeem) – artikel 3 lid 66

“Een AI-systeem dat is gebaseerd op een AI-model voor algemene doeleinden en dat verschillende doeleinden kan dienen, zowel voor direct gebruik als voor integratie in andere AI-systemen.”⁶

⁴ Art. 3 lid 1 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

⁵ Art. 3 lid 63 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

⁶ Art. 3 lid 66 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

Let op het verschil van een GPAI-model en een GPAI-systeem. Een GPAI-model kan niet worden geclassificeerd onder een risicocategorie. Voorbeelden van GPAI-modellen zijn GPT-4 van OpenAI of BERT van Google. Onder GPAI wordt dus niet traditionele softwaresystemen verstaan of systemen die regels volgen die door natuurlijke personen zijn vastgesteld om automatisch handelingen uit te voeren.

Een GPAI-systeem is het systeem waar in een model gebruikt kan worden voor een specifiekere toepassing. Bij een GPAI-systeem kan er wel een risico classificering plaatsvinden. Een voorbeeld van een GPAI-systeem is ChatGPT, dat gebruik maakt van verschillende GPAI-modellen van OpenAI zoals GPT-4. Dit systeem kan voor verschillende doeleinden toegepast worden. De specifieke toepassing die gebruikt wordt moet bekeken worden in het licht van de AI Act. Bijvoorbeeld het systeem gebruiken om lerende te beoordelen valt onder een hoog risico toepassing, terwijl het systeem gebruiken om te brainstormen niet onder hoog risico valt. Ongeacht het risico van het systeem, let erop dat er geen persoonsgegevens, auteursrechten of bedrijfsgeheimen gedeeld worden in deze systemen.

Rollen met betrekking tot een AI-systeem

Aanbieder (provider) – artikel 3 lid 3

“Een natuurlijke of rechtspersoon, overheidsinstantie, agentschap of ander orgaan die/dat een AI-systeem of een AI-model voor algemene doeleinden ontwikkelt of laat ontwikkelen en dat systeem of model in de handel brengt of het AI-systeem in gebruik stelt onder de eigen naam of merk, al dan niet tegen betaling.”⁷

Gebruiksverantwoordelijke (deployer) – artikel 3 lid 4

“Een natuurlijke of rechtspersoon, overheidsinstantie, agentschap of ander orgaan die/dat een AI-systeem onder eigen verantwoordelijkheid gebruikt, tenzij het AI-systeem wordt gebruikt in het kader van een persoonlijke niet-beroepsactiviteit.”⁸

De aanbieder is kort gezegd degene een AI-systeem ontwikkelt en/of onder eigen naam op de markt brengt. De gebruiksverantwoordelijke is degene die een AI-systeem inzet. Naast aanbieder en gebruiksverantwoordelijke zijn er nog een aantal andere rollen, zoals importeur, distributeur, operator of gemachtigde.⁹

⁷ Art. 3 lid 3 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

⁸ Art. 3 lid 4 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

⁹ Art. 3 lid 5, lid 6, lid 7, lid 8 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

De kern van de AI Act is de risicoclassificering van specifieke toepassingen van AI-systemen bij de rol die een organisatie heeft met betrekking tot het AI-systeem. Nu de verschillende rollen met betrekking tot een AI-systeem zijn toegelicht, kan er gekeken worden naar de verschillende risico categorieën en de bijbehorende verplichtingen.

Risico-regulering AI Act

De AI Act maakt gebruik van risicoclassificering voor AI-systemen, die in deze sectie verder uiteengezet zullen worden. Sommige AI-systemen brengen een onaanvaard risico met zich mee die als een gevaar voor de mens worden beschouwd en zijn daarom verboden en niet gebruikt mogen worden. Zoals, gezondheidsrisico's, veiligheidsrisico's en fundamentele rechten kunnen in het geding komen.

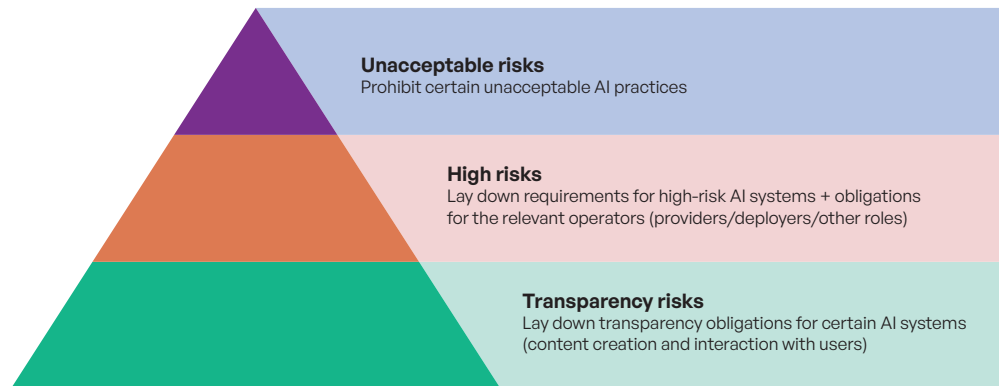
Daarnaast zijn er ook AI-systemen met hoge risico's op de veiligheid of grondrechten. Door AI-systemen in te delen in verschillende risico categorieën kunnen er verschillende eisen aan deze systemen gesteld worden. De risiconiveaus die zijn gedefinieerd: verboden AI, hoog risico AI en AI met transparantie verplichtingen, zijn terug te zien in figuur 1. De verschillende risico's en de bijpassende AI-systemen zullen hieronder verder worden toegelicht.

Verboden AI-systemen

AI-systemen die een onaanvaard risico met zich meebrengen, zijn volgens de AI Act verboden. Hierbij gaat het over (artikel 5 lid 1)¹⁰:

- Systemen die gericht zijn op menselijk gedrag te manipuleren of te misleiden.
- Systemen die misbruik maken van de kwetsbaarheden van personen als gevolg van leeftijd, handicap of sociale of economische situatie.
- AI-systemen voor social scoring. AI-systemen die mensen beoordelen op basis van sociaal gedrag of persoonlijke kenmerken.
- AI gebaseerde voorspelde risicobeoordelingen voor criminaliteit.
- Systemen die worden gebruikt om mensen op basis van biometrische gegevens te categoriseren in bepaalde gevoelige categorieën.

¹⁰ Art. 5 lid 1 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689



Figuur 2 Risicoclassificering AI-systemen

- Het gebruik van AI-systemen voor biometrische identificatie op afstand in real-time in openbare ruimten.
- Het ongericht scrapen van gezichtsafbeeldingen van internet of camerabeelden om databanken voor gezichtsherkenning aan te leggen of aan te vullen.
- Emotieherkenning op de werkplek of in het onderwijs

Dit laatste is voor het onderwijs het meest relevant. De AI Act geeft hiervoor nog geen verdere verduidelijkingen waaraan gedacht kan worden bij deze onderdelen. Een voorbeeld zou kunnen zijn emotie herkenning via audio-opname tijdens een presentatie.

Hoog risico AI-systemen

AI-systemen die een negatief effect hebben op de veiligheid of de grondrechten worden als systemen met een hoog risico beschouwd en worden onderverdeeld in twee categorieën:

1. AI-toepassingen in producten die onder de EU-wetgeving op het gebied van productveiligheid vallen. Voorbeelden hiervan zijn speelgoed, luchtvaartuigen, auto's, medische hulpmiddelen en liften (Bijlage I in de AI Act).¹¹
2. AI-systemen op acht verschillende gebieden (Zie Bijlage III in de AI Act voor de gehele lijst).¹² Een van de specifiek genoemde gebieden is onderwijs. Daarnaast wordt ook het gebruik van AI in werving en selectie als hoog-risico benoemd.

¹¹ Bijlage 1 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

¹² Bijlage 3 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

Hoog risico toepassingen van AI-systemen binnen het onderwijs:¹³

- AI-systemen om toegang of toelating tot onderwijs te regelen.
- AI-systemen om leeruitkomsten te evalueren, inclusief als die uitkomsten worden gebruikt om het leerproces van natuurlijke personen te sturen.
- AI-systemen die worden ingezet om het geschikte niveau van onderwijs voor een individu te beoordelen.
- AI-systemen die bedoeld zijn om te worden gebruikt voor het monitoren en detecteren van ongeoorloofd gedrag van studenten tijdens toetsen.

Voorbeelden van hoog risico toepassingen van AI-systemen binnen het onderwijs

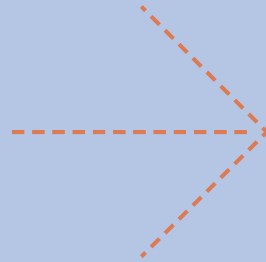
- Een AI-systeem dat aan de hand van motivatiebrieven van lerende toelating bij een opleiding beoordeelt.
- Een AI-systeem dat het gedrag van lerende tijdens een examen monitort en beoordeelt op verdacht gedrag (proctoring systemen).

Hoog risico toepassingen binnen werkgelegenheid, personeelsbeheer en toegang tot zelfstandige arbeid:¹⁴

- AI-systemen die gebruikt worden voor recruitment of selectie van natuurlijke personen.
- AI-systemen die gebruikt worden voor het maken van beslissingen die de voorwaarden rond het werk beïnvloeden.

¹³ Bijlage 3.3 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

¹⁴ Bijlage 3.4 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689



Verplichtingen in de AI-verordening

Eisen voor hoog-risico AI-systemen

De kans is aanwezig dat je dusver gelezen hebt en je nu afvraagt, welke eisen brengen hoog risico AI-systemen met zich mee. Dat hangt af van welke rol je als organisatie hebt in relatie tot het systeem.

Aanbieders van hoog risico AI-systemen moeten aan bepaalde eisen voldoen om ervoor te zorgen dat hun AI-systemen betrouwbaar, transparant en controleerbaar zijn:¹⁵

- Een risicomanagement systeem opzetten gedurende de gehele levenscyclus van het AI-systeem.
- Data governance uitvoeren en ervoor zorgen dat de opleidings-, validerings- en test-gegevensreeksen relevant en voldoende representatief zijn en, voor zo ver mogelijk, geen fouten bevatten en volledig zijn met het beoogde doel.
- Technische documentatie opstellen om compliance aan te tonen en autoriteiten de informatie te geven om die compliance te beoordelen.
- Hun AI-systeem zo ontwerpen dat het automatisch gebeurtenissen registreert die relevant zijn voor het identificeren van risico's op nationaal niveau en ingrijpende wijzigingen gedurende de levenscyclus van het systeem.
- Het geven van gebruiksinstructies aan gebruiksverantwoordelijke om ervoor te zorgen dat zij aan de eisen voldoen.
- Hun AI-systeem zo ontwerpen dat gebruiksverantwoordelijke menselijk toezicht kunnen implementeren
- Hun AI-systeem zo ontwerpen dat gebruiksverantwoordelijke menselijk toezicht kunnen implementeren.
- Hun AI-systeem zo ontwerpen dat het de juiste niveaus van nauwkeurigheid, robuustheid en cyberbeveiliging wordt bereikt.
- Een kwaliteitsmanagementsysteem opzetten om naleving te garanderen.

Gebruiksverantwoordelijke hebben ook verplichtingen bij het inzetten van een hoog risico AI-systeem:¹⁶

- Een belangrijke verplichting met belangrijke gevolgen voor een mogelijke aansprakelijkheidsdiscussie met de aanbieder is dat de gebruiksverantwoordelijke het hoog-risico AI-systeem moet **gebruiken in overeenstemming met de gebruiksinstructies van de provider**.

¹⁵ Art 16 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

¹⁶ Art. 26 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

- De gebruiksverantwoordelijke heeft ook de verplichting om zoveel mogelijk **menselijk toezicht** in te stellen en de **invoergegevens en werking van het systeem te controleren**. De gebruiksverantwoordelijke moet de geautomatiseerde logboeken ten minste zes maanden bewaren.
- Daarnaast is het voor overheidsorganisaties en organisaties die publieke diensten leveren ook verplicht om een **Fundamental Rights Impact Assessment** (FRIA) uit te voeren¹⁷.

Let op, het is mogelijk om van gebruiksverantwoordelijke naar aanbieder te veranderen bij een hoog risico AI-systeem, namelijk als:

- De gebruiksverantwoordelijke hun eigen naam of merk op het hoog risico-systeem zet.
- De gebruiksverantwoordelijke een aanzienlijke wijziging aan het hoog-risico AI-systeem aanbrengt die niet door de aanbieder was voorzien en waardoor het systeem niet meer aan de eisen voldoet.
- De gebruiksverantwoordelijke een aanzienlijke wijziging aan het hoog-risico AI-systeem aanbrengt die niet door de aanbieder was voorzien en waardoor het beoogde doel van de aanbieder van het systeem veranderd.

Eisen voor General Purpose AI modellen

GPAI-modellen worden specifiek gereguleerd en geclassificeerd onder de AI Act. Hierdoor kan het niet een hoog risico bevatten. Let op dat een GPAI-systeem wel een hoog risico kan vormen.

Alle aanbieders van GPAI-modellen moeten¹⁸:

- Technische documentatie leveren
- Gebruiksaanwijzingen leveren
- Voldoen aan de auteursrecht richtlijn
- Een samenvatting publiceren over de content die voor training is gebruikt.

Aanbieders die hun GPAI-model onder een gratis en open licentie publiekelijk beschikbaar stellen, hoeven alleen te voldoen aan de auteursrecht richtlijn en de samenvatting over de content die voor training is gebruikt publiceren, tenzij het een GPAI-model met systeem risico's is.

¹⁷ Rijksoverheid AI-verordening Gids p.15 Gids AI-verordening | versie 1.0 - oktober 2024 (overheid.nl)

¹⁸ Art. 53 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

Systeemrisico's bij General Purpose AI-modellen

Alle aanbieders van GPAI-modellen met systeem risico's moeten aan extra verplichtingen voldoen. Een GPAI-model wordt gezien als GPAI-model met systeem risico's als het aan de volgende criteria voldoet:¹⁹

- Het heeft high impact capabilities, geëvalueerd op basis van passende technische instrumenten en methodes, inclusief indicatoren en benchmarks.
- Op basis van een besluit van de Europese commissie ambtshalve of na een gekwalificeerde waarschuwing door het 'wetenschappelijk panel', dat een GPAI-model over mogelijkheden of effecten beschikt die gelijkwaardig zijn aan die van het vorige punt.

Alle aanbieders van GPAI-modellen met systeemrisico's moeten:²⁰

- Modevaluaties uitvoeren, inclusief het uitvoeren en documenteren van contradictietests om systeemrisico's te identificeren en te beperken.
- Beoordelen en beperken van mogelijke systeemrisico's, inclusief de bronnen ervan.
- Ernstige incidenten en mogelijke corrigerende maatregelen traceren, documenteren en zonder onnodige vertraging rapporteren aan de 'AI Office' en relevante nationale bevoegde autoriteiten.
- Zorgen voor een adequaat niveau van cybersecurity,

Transparantie verplichtingen bij bepaalde AI-systemen

Sommige AI-systemen hebben transparantie verplichtingen. Dit geldt voor:²¹

- AI-systemen die bedoeld zijn voor interactie met natuurlijke personen.
- AI-systemen, waaronder GPAI-systemen, die synthetische audio, beeld, video of tekst inhoud genereren.
- Emotieherkenning systemen of biometrische categorisering systemen.

Wanneer een AI-systeem hieronder valt gelden de volgende verplichtingen. Hierbij moeten aanbieders:²²

- De gebruiker informeren zodat voor diegene duidelijk is dat er geen interactie met een mens plaatsvindt.
- Daarbij moet in sommige gevallen, de inhoud op een machine leesbare manier worden gelabeld zodat deze kan worden geïdentificeerd als kunstmatig gegenereerde of gemanipuleerde inhoud.

¹⁹ Art. 55 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

²⁰ Art. 55 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

²¹ Art. 50 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

²² Art. 50 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

Als gebruiksverantwoordelijke zitten hier ook nog een verplichting aan:²³

- Als gebruiksverantwoordelijke van systemen die audio, beeld of video genereren moeten ervoor zorgen dat duidelijk is dat de inhoud kunstmatig genereerd of gemanipuleerd is.
- Gebruiksverantwoordelijke van een AI-systeem dat teksten genereerd of bewerkt die gepubliceerd worden om het publiek te informeren over aangelegenheden van algemeen belang, moet er duidelijk gemaakt worden dat de tekst kunstmatig is genereerd of is bewerkt.

²³ Art. 50 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

Overige aspecten van de AI-verordening

Naast het bovenstaande zijn er een aantal onderdelen van de AI-verordening die specifiek nog interessant zijn om te benoemen.

AI-geletterdheid – artikel 4

De AI Act benoemt dat zowel aanbieders als gebruiksverantwoordelijken, ongeacht de risico-classificering van het systeem, maatregelen moeten nemen om te zorgen dat personeel en andere personen die AI-systemen exploiteren en gebruiken voldoende AI-geletterd zijn. Dit staat in de wettekst in artikel 4 omschreven als: *“Aanbieders en gebruiksverantwoordelijken van AI-systemen nemen maatregelen om, zoveel als mogelijk, te zorgen voor een toereikend niveau van AI-geletterdheid bij hun personeel en andere personen die namens hen AI-systemen exploiteren en gebruiken, en houden daarbij rekening met hun technische kennis, ervaring, onderwijs en opleiding en de context waarin de AI-systemen zullen worden gebruikt, evenals met de personen of groepen personen ten aanzien van wie de AI-systemen zullen worden gebruikt.”*²⁴

Onderzoek uitzondering – artikel 2 lid 6 & lid 8

De AI Act benoemt een aantal uitzonderingen op de wetgeving met betrekking tot onderzoek naar AI-systemen of modellen. Namelijk als deze specifiek ontwikkeld zijn voor zuiver wetenschappelijk onderzoek of met wetenschappelijke ontwikkeling als enige doel.

Zo wordt er genoemd in artikel 2 lid 6: *“Deze verordening is niet van toepassing op AI-systemen of AI-modellen, met inbegrip van hun output, die specifiek zijn ontwikkeld en in gebruik gesteld met wetenschappelijk onderzoek en wetenschappelijke ontwikkeling als enig doel.”*²⁵

Artikel 2 lid 8: *“Deze verordening is niet van toepassing op onderzoeks-, test- of ontwikkelingsactiviteiten met betrekking tot AI-systemen of AI-modellen voor zij in de handel worden gebracht of in gebruik worden gesteld. Dergelijke activiteiten worden uitgevoerd in overeenstemming met het toepasselijke Unierecht. Testen onder reële omstandigheden vallen niet onder die uitsluiting.”*²⁶

²⁴ Art. 4 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

²⁵ Art. 2 lid 6 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

²⁶ Art. 2 lid 8 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

Oftewel, zodra je de vruchten van het wetenschappelijk onderzoek in de handel gebracht worden of in gebruik worden gesteld, verlaat je deze uitzondering en gelden de regels van de AI Act. Zodra het wetenschappelijk onderzoek onder reële omstandigheden gaat uitvoeren en testen gelden de regels van artikel 60.²⁷

Uitzondering persoonlijk gebruik – artikel 2 lid 10

De AI Act is niet voor zuiver persoonlijk gebruik van AI-systemen van toepassing. Zo luidt artikel 2 lid 10: *“Deze verordening is niet van toepassing op verplichtingen van gebruiksverantwoordelijken die natuurlijke personen zijn die AI-systemen gebruiken in het kader van een louter persoonlijke niet-professionele activiteit.”*²⁸

Uitzondering open source licenties – artikel 2 lid 12

Een laatste uitzondering op de AI Act is het vrijgeven van AI-systemen onder open source licenties. Dit wordt benoemd in artikel 2 lid 12: *“Deze verordening is niet van toepassing op AI-systemen die worden vrijgegeven onder vrije en open source licenties, tenzij zij in de handel worden gebracht of in gebruik worden gesteld als AI-systemen met een hoog risico of als een AI-systeem dat onder artikel 5 of artikel 50 valt.”*²⁹

²⁷ Art. 60 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

²⁸ Art 2 lid 10 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

²⁹ Art 2 lid 12 AI Act eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:L_202401689

Wat betekent de AI Act voor onderwijsinstellingen?

Allereerst hebben onderwijsinstellingen zich aan deze wet te houden. Er zijn specifieke toepassingen van AI-systemen in het onderwijs die als hoog risico toepassingen genoemd worden. Hierdoor is de kans groot dat dit van toepassing is op onderwijsinstellingen. Daarnaast zullen er bij het toepassen van deze AI-systemen binnen een instelling extra maatregelen genomen moeten worden. Zo is het belangrijk om uit te vinden of je als instelling aanbieder of gebruiksverantwoordelijke bent van deze hoog risicosystemen om je volgende stappen te gaan bepalen.

De Gids AI-verordening van de Rijksoverheid raadt aan hiervoor 4 stappen te volgen:³⁰

Stap 1 (Risico): Valt ons (AI-)systeem binnen één van de risicocategorieën?

Stap 2 (AI): Is ons systeem ‘AI’ volgens de AI-verordening?

Stap 3 (Rol): Zijn wij de aanbieder of gebruiksverantwoordelijke van het AI-systeem?

Stap 4 (Verplichtingen): Aan welke verplichtingen moeten wij ons houden?

Ter toevoeging aan de stappen van de Gids AI-verordening van de Rijksoverheid zijn er drie stappen die je kunt ondernemen. Als eerst kan je gaan inventariseren welke AI-systemen er gebruikt worden binnen de organisatie om vervolgens na te gaan welke rol de organisatie heeft en onder welk risico het systeem valt. Daarnaast gelden vanaf februari 2025 de eisen voor AI-geletterdheid.

1. Inventarisering

Om te weten in hoeverre de AI Act van toepassing is op de instelling is het belangrijk om te weten welke AI-systemen en GPAI-modellen er binnen je instelling worden ontwikkeld, ingekocht en gebruikt. Daarom is het handig om alvast een inventarisering te maken van alle AI-systemen die worden gebruikt binnen de instelling.

Voor de instellingen geldt er (nog) geen verplichting voor een Algoritmeregister. Het is wel raadzaam om de AI-systemen hierin op te nemen.

2. Rolbepaling & risicobepaling bij inventarisering

De verantwoordelijkheden bij de AI-Act verschillen erg van de rol die je als organisatie hebt bij een AI-systeem. Zo zijn er meer verplichtingen voor aanbieders (providers) van AI-systemen

³⁰ rijksoverheid.nl/documenten/brochures/2024/10/16/gids-ai-verordening

dan voor gebruiksverantwoordelijken (deployers) van AI-systemen. Het kan verstandig zijn om bij de inventarisering van AI-systemen ook meteen vast te leggen of je aanbieder of gebruiker bent.

De AI Act werkt met een risico benadering. AI-systemen kunnen gecategoriseerd worden in verboden AI-systemen, hoog risico AI-systemen, AI-systemen met transparantie verplichtingen en 'overige' AI-systemen. Tijdens de inventarisatie is het wijs om ook meteen te kijken onder welke risicoclassificering het AI-systeem valt. Zo moeten verboden AI-systemen gedetecteerd worden en uit gefaseerd worden. Daarnaast krijg je meer inzicht in de verplichtingen van je organisatie bij AI-systemen met andere risico's.

3. AI-geletterdheid

Sinds februari 2025 geldt de regelgeving over verboden AI en AI-geletterdheid in werking. Artikel 4 van de AI Act stelt dat: *"Aanbieders en gebruiksverantwoordelijken van AI-systemen nemen maatregelen om, zoveel als mogelijk, te zorgen voor een toereikend niveau van AI-geletterdheid bij hun personeel en andere personen die namens hen AI-systemen exploiteren en gebruiken, en houden daarbij rekening met hun technische kennis, ervaring, onderwijs en opleiding en de context waarin de AI-systemen zullen worden gebruikt, evenals met de personen of groepen personen ten aanzien van wie de AI-systemen zullen worden gebruikt."*

Het is verstandig om binnen je instelling het gesprek over verantwoord gebruik van AI te organiseren. Doe dit met een brede interdisciplinaire groep van collega's: IT, data, privacy, informatiebeveiliging, docenten. Daarnaast is het raadzaam om medewerkers vertrouwd te maken met de voor- en nadelen van AI door middel van trainingen.

