# Inhoud

Afgelopen 02 april 2024 is de eerste belangrijke wet op AI (artificiële intelligentie) in werking getreden. Deze nieuwe wetgeving zal effect gaan hebben op het gebruik en de exploitatie van Ai-systemen binnen de Europese Unie. Artificiële intelligentie biedt veel mogelijkheden voor de EU, maar het komt ook met potentiële risico's. De Europese Unie wil de EU-burgers behoeden voor de gevaren van AI, zonder dat dat burgers hun voordeel daar niet meer uit kunnen halen.

## 1. Algemene informatie

> 1.1 Wat is de AI-verordening?

De AI-verordening is Europese wetgeving waar de lidstaten, zoals Nederland, zich aan moeten houden. De AI-verordening bevat een groot aantal regels over hoe omgegaan moet worden met AI. Er is nauwelijks wetgeving over AI. Dat komt omdat AI pas onlangs in een stroomversnelling is gekomen.  De Europese Unie vindt het belangrijk om AI te reglementeren, aangezien AI aanzienlijke gevaren kent. De Europese Unie is zich ook bewust van de voordelen van AI. Met deze verordening behoedt de Europese Unie de burgers van de unie voor de gevaren van AI, maar biedt zij ook ruimte voor de voordelen ervan.

De verordening is van toepassing op alle AI-systemen die binnen de unie beschikbaar worden gesteld (ook als iemand buiten de EU dat doet).

> 1.2 Wat is een AI-systeem?

Om deze verordening goed uit te leggen, is het belangrijk uit te leggen wat AI volgens de verordening is  De AI-verordening ziet een systeem als een AI-systeem als is voldaan aan de volgende voorwaarden:
-1 Het is een machinegebaseerd systeem (een systeem dat draait op technologieën en computers en geautomatiseerd taken kan uitvoeren);
-2 Het systeem is ontworpen om (deels) zelfstandigheid te kunnen werken.
-3 Het systeem *kan* zichzelf aanpassen, zelfs nadat het uitgebracht is.
-4 Het systeem genereert op basis van input van gebruikers uitkomsten (zoals voorspellingen, beslissingen en dergelijke) die invloed kunnen hebben op fysieke of digitale omgevingen, of op beide

Wanneer aan al deze voorwaarden voldaan is, wordt het systeem gezien als een AI-systeem en dient het te voldoen aan de verplichtingen uit deze verordening. Voorwaarden 3 en 5 zijn niet verplicht, deze zijn enkel bedoeld om het 'grijze gebied' waar niet duidelijk is of deze definitie van toepassing is te verkleinen.

> 1.3 Wanneer wordt de verordening van toepassing?

De AI-verordening is in werking getreden op 02 april 2024. Het is belangrijk om op te merken dat de verordening nog niet gelijk van toepassing is op bedrijven/ondernemers in de EU wanneer zij in werking getreden is. In het geval van de AI-verordening treden de meeste bepalingen pas op 02 april 2026 in werking. Dat geldt trouwens niet voor alle regels. Ik zal hierna een kort overzicht geven van alle onderwerpen binnen de verordening die op een andere datum toegepast worden. Wanneer ik een onderwerp niet noem, kun je aanhouden dat deze vanaf 02 april 2026 geldt.

- de eerste onderdelen van de AI-verordening hebben betrekking op een paar algemene bepalingen/definities, en veel belangrijker **Welke AI-systemen volledig verboden worden**. Deze onderwerpen worden van toepassing vanaf 02 oktober 2024, 6 maanden na de inwerkingtreding.

- Bepalingen m.b.t. AI-systemen voor algemeen gebruik, de bevoegde autoriteiten vanuit de overheid en de sancties op het overtreden van de verordening worden 12 maanden na de inwerkingtreding van toepassing, op 02 april 2025

- classificatie als een systeem met een hoog risico **op basis van de 1ste manier** wordt pas van toepassing 36 maanden na de inwerkingtreding, op 02 april 2027.

Onderstaande staat een tabel waarin alle datums en de daarbij horende bepalingen nogmaals verwerkt staan. Alles wat niet in deze tabel staat wordt van toepassing verklaard op 02 april 2026.

| Van toepassing op: 02 okt. 2024 | Van toepassing op: 02 apr. 2025 | Van toepassing op: 02 apr. 2027 |
|---|---|---|
| Volledig verboden systemen (zie 2.1) | Sancties op overtredingen | Classificatie hoog-risico systemen d.m.v. andere wetten (zie 3.2) |
| Algemene definities | Bepalingen voor AI-systemen voor algemene doeleinden (zie 3.3) | |
| | Bevoegde instanties van de overheid | |

*Hoe zit het met toepassing op de systemen zelf, die voor toepassing van de verordening al in handel waren?*

Ook gelden er verschillende termijnen in het geval dat een systeem al in handel is, voordat de AI-verordening van toepassing wordt. Deze zijn:
- Op reeds bestaande verboden AI-systemen staat geen verlengde toepassingstermijn. Deze handelingen zijn verboden en strafbaar zodra artikel 5 van de verordening van toepassing verklaard is (vanaf 02//10//2024)

- Er zijn een aantal systemen binnen de Europese Unie die als ‘grootschalige IT-systemen’ aangemerkt worden. Alle grootschalige IT-systemen die voor 02//04//2027 in gebruik gesteld zijn, dienen uiterlijk op 31 december 2030 in overeenstemming te zijn met de verordening. Van een grootschalig IT-systeem is niet snel sprake, deze zal ook niet verder uitgewerkt worden.

- AI-systemen die als systemen met een hoog risico aangemerkt worden en die voor 02//04//2026 op de markt gebracht zijn, vallen enkel onder deze verordening indien deze systemen op of na 02//04//2026 aanzienlijke wijzigingen ondergaan. Indien het gaat om AI-systemen die overheidsinstanties dienen, worden deze uiterlijk op 02//04//2030 in conformiteit met de verordening gebracht. AI-systemen die na 02//04//2026 op de markt gebracht worden, dienen gelijk in overeenstemming met de verordening te zijn.

- AI-systemen voor algemene doeleinden, ongeacht of zij een systeemrisico hebben, die voor 02//04//2025 op de markt gebracht zijn, dienen uiterlijk op 02//04//2027 aan alle plichten uit de verordening te voldoen.

> 1.4 Algemene beginselen van AI-systemen

Bij het toetsen of AI-systemen in overeenstemming zijn met de verordening kan een aantal beginselen worden gebruikt:

- invloed en toezicht door mensen: AI wordt ontwikkeld als instrument dat mensen dient. Het eerbiedigt menselijke waardigheid en persoonlijke autonomie. Dit betekent dat het systeem altijd goed rekening zal houden met o.a. dat mensen hun eigen keuzes kunnen maken en dat het niet tegen de grondrechten van de mens ingaat. . AI functioneert op een wijze waarop mensen controle en toezicht kunnen houden

- technische robuustheid en veiligheid: AI-systemen zijn robuust. Hiermee wordt bedoeld dat ze bestendig zijn tegen veranderingen van situaties, en dat het niet makkelijk is voor een systeem om fouten te maken of een technische storing te krijgen. Daarnaast werken AI-systemen zodanig dat onbedoelde of onverwachte schade zoveel mogelijk voorkomen of beperkt wordt. Zij zijn bestand tegen pogingen van derden om prestaties of gebruik te wijzigen.

- privacy en databeheer: AI-systemen worden ontwikkeld op basis van bestaande EU-wetgeving die ziet op privacy en gegevensbescherming, zoals de AVG.

- transparantie: mensen die gebruik maken van een AI-systeem worden in kennis gesteld dat zij communiceren met een AI-systeem, alsmede de mogelijkheden en beperkingen van het systeem en welke rechten zij hebben.

- diversiteit, non-discriminatie en billijkheid: AI-systemen worden ontwikkeld zodat inclusie van diverse factoren gewaarborgd wordt. Gelijke toegang, gendergelijkheid en culturele diversiteit worden bevorderd. Discriminerende effecten en ongerechtvaardigde vertekeningen dienen zo goed mogelijk voorkomen te worden

- sociaal en ecologisch welzijn: AI-systemen worden op duurzame en milieuvriendelijke manier ontwikkeld. Daarnaast worden AI-systemen op zodanige manier ontwikkeld, dat iedereen hier zijn/haar voordeel uit kan trekken.

## 2. Verschillende categorieën van AI

> 2.1 Volledig verboden vormen van AI

Er zijn een aantal systemen waarvan het aanbieden, in gebruik stellen of gebruiken volledig verboden wordt. Vanaf 02 oktober 2024 wordt dit van toepassing op de volgende type systemen:

- **Gebruik van manipulatieve, bedrieglijke of vergelijkbare technieken:** Ieder systeem dat van 1 dezer technieken gebruik maakt, waardoor de gebruikende persoon beperkt wordt tot het maken van een beslissing of een beslissing maakt die hij/zij anders niet gemaakt zou hebben, wordt volledig verboden.

- **Exploitatie kwetsbare personen:** Ieder systeem dat kwetsbare personen op basis van leeftijd, gebrek, sociale/economische status etc. exploiteren, waardoor een redelijke kans bestaat dat een persoon zichzelf of een ander leed toe brengt, wordt volledig verboden.

- **Classificatie + nadelige behandeling**: Ieder systeem dat personen of groepen classificeert op basis van sociaal gedrag of karakteristieken, wat leidt tot nadelige behandeling van deze of andere personen, wordt volledig verboden.

- **Risicoprofilering op basis van karakteristieken:** Ieder systeem dat voorspelt hoe groot de kans is dat iemand een overtreding begaat enkel op basis van personaliteit of karakteristieken, wordt volledig verboden.

- **Ongericht nemen van gezichtsbeelden:** Ieder systeem dat ongericht gezichtsbeelden neemt van het internet of CCTV-beelden, met het doel om gezichtsherkenningsdatabanken uit te breiden, wordt volledig verboden.

- **Afleiden van emoties:** Ieder systeem dat bedoeld is om emoties af te leiden van personen binnen een werk- of onderwijsomgeving, wordt volledig verboden. Hiervoor wordt een uitzondering gemaakt wanneer dit gebeurd m.b.t. medische redenen of veiligheidsredenen.

- **Categorisering door biometrische gegevens:** Ieder systeem dat gebruik maakt van biometrische gegevens om personen in categorieën in te delen, waardoor bepaalde gegevens (ras, politieke status, etc.) geschat kunnen worden, wordt volledig verboden.

- **Biometrische identificatie op afstand in ‘real time’:** Ieder systeem dat hiervan gebruik maakt in openbare ruimten met het doel van rechtshandhaving, wordt volledig verboden.

> 2.2 AI-systemen met een hoog risico

Een aantal AI-systemen worden als systemen met een hoog risico gezien. Deze systemen worden niet direct verboden, maar dienen wel aan een groot aantal extra verplichtingen te voldoen. Er zijn twee manieren waarop een systeem gezien kan worden als een systeem met hoog risico.

De eerste manier is wanneer het systeem onder bepaalde andere wetgevingen van de Unie valt. Deze manier specifiek is pas van toepassing vanaf 02 April 2027, 3 jaar na de inwerkingtreding. Het systeem wordt dan als veiligheidscomponent aan een product toegevoegd of het systeem zelf is het product. Daarnaast is er de verplichting dat het relevante product door een ander persoon of bedrijf  gekeurd wordt. Wanneer aan beide van deze voorwaarden voldaan is, word gewerkt met een systeem met hoog risico. Onderaan dit onderdeel is een extra paragraaf toegevoegd waarin uitgelegd wordt wat bedoeld wordt met 'bepaalde andere wetgevingen van de unie'.

Naast deze (redelijk vage) manier geeft de AI-verordening ook een duidelijkere 2$^{de}$ manier op basis waarvan AI-systemen gezien kunnen worden als systemen met een hoog risico. Als het systeem voldoet aan 1 van de volgende voorwaarden valt het hieronder:

- **Biometrische herkenning op afstand:** Alle systemen die bedoeld zijn voor biometrische herkenning op afstand, worden gezien als systemen met een hoog risico. Met biometrische herkenning wordt bedoeld een AI-systeem dat bedoeld is voor identificatie van personen zonder dat zij hier actief in betrokken zijn. Dit gebeurt door gebruik van biometrische gegevens die zijn opgenomen in een referentiebank.

- **Gebruik van biometrische gegevens:** Alle systemen die bedoeld zijn om biometrische gegevens (persoonsgegevens, vaak fysieke kenmerken zoals huidskleur of vorm van het gezicht) te gebruiken voor categorisatie of herkenning van emoties, worden gezien als systemen met een hoog risico.

- **Veiligheidscomponent essentiële systemen:** Alle systemen die bedoeld zijn als een veiligheidscomponent bij essentiële systemen, het wegverkeer of het verspreiden van gas/water/elektriciteit, worden gezien als systemen met een hoog risico. Met essentiële systemen wordt bedoeld alle systemen belangrijk voor het leveren van een essentiële dienst zoals politie en justitie, ziekenhuispersoneel, etc.

- **Toegang tot onderwijsinstellingen:** Alle systemen die bedoeld zijn om personen toegang te verlenen tot onderwijsinstellingen worden gezien als systemen met een hoog risico.

- **Evalueren onderwijsresultaten:** Alle systemen die bedoeld zijn om onderwijsresultaten te evalueren of te beoordelen welk scholingsniveau op een persoon toepasselijk is, worden gezien als systemen met een hoog risico.

- **Werving- en selectie bij werk:** Alle systemen die bedoeld zijn als hulpmiddel bij de werving- en selectieprocedure in een werkomgeving, bijvoorbeeld om de beste kandidaten te selecteren, worden gezien als systemen met een hoog risico.

- **Essentiële bestuursdiensten en - uitkeringen:** Alle systemen die beoordelen of bepaalde mensen in aanmerking komen voor overheidsdiensten of uitkeringen worden gezien als systemen met een hoog risico.

- **Risicoschatting levens- en gezondheidsverzekeringen:** Alle systemen die bedoeld zijn om risicoprofielen op te stellen in het kader van levens- of gezondheidsverzekeringen worden gezien als systemen met een hoog risico.

- **Reageren op noodoproepen:** Alle systemen die bedoeld zijn voor het reageren op of evalueren van noodoproepen worden gezien als systemen met een hoog risico.

- **Systemen in strafzaken:** Alle systemen die bedoeld zijn voor het beoordelen van bewijs, voor het beoordelen van de kans of iemand slachtoffer wordt, voor het beoordelen van bepaalde persoonlijkheden of bij gebruik van detectie, opsporing en veroordeling van misdrijven, worden gezien als systemen met een hoog risico.

- **Migratie:** De meeste systemen die bedoeld zijn in relatie tot migratie of andere situaties waarbij mensen uit het buitenland komen, worden gezien als systemen met een hoog risico.

- **Gebruik door rechters:** Alle systemen die bedoeld zijn voor rechters om onderzoek te doen naar het recht of om feiten te interpreteren, worden gezien als systemen met een hoog risico.

- **m.b.t. stemrecht:** Alle systemen die bedoeld zijn om stemmen van mensen (in politieke zin) te veranderen, worden gezien als systemen met een hoog risico.

- **Uitzonderingen:** Er zijn een aantal uitzonderingen, waarin een systeem aan een van de voorwaarden uit deze lijst voldoet maar alsnog niet als een systeem met hoog risico gezien wordt. Hiervan is sprake **wanneer het systeem geen significant risico op schade voor de gezondheid, veiligheid of grondrechten van personen houdt**. Dit onder meer doordat de besluitvorming van personen (vrijwel) niet beïnvloed worden door het systeem. Een voorbeeld wanneer hiervan sprake is, is wanneer het systeem enkel een zeer nauwe procedurele taak, zoals het verzenden van al geschreven brieven of het bijhouden van veranderingen in een document, vervult.

<u>1. Harmonisatiewetgeving waarin systemen als ‘hoog risico’ gezien worden</u>

<u>> 2.3 AI-systemen voor algemene doeleinden</u>

Wanneer geen sprake is van een verboden AI-systeem of een AI-systeem met een hoog risico, valt het systeem binnen de categorie ‘AI-systemen voor algemene doeleinden. Dit is in principe de restcategorie voor AI-systemen. Echter, er is wel een onderverdeling te maken binnen deze systemen. Sommige AI-systemen worden aangeduid als ‘AI-systemen voor algemene doeleinden **met een systeemrisico’**. Een Ai-systeem heeft een systeemrisico wanneer het beschikt over capaciteiten met een grote impact. Hiervan is sprake wanneer het aantal zwevendekommabewerkingen groter is dan 10^25. Dit is een eenheid die gebruikt wordt om de rekenkracht van computersystemen aan te duiden.

Naast het beschikken over capaciteiten met grote impact is het ook mogelijk dat een AI-systeem aangemerkt wordt als een AI-systeem met een systeemrisico wanneer de Het AI-bureau bepaald dat het systeem een vergelijkbare impact heeft. Het AI-bureau is de instelling van de Europese Unie die zich bezig houdt met controleren of iedereen de AI-verordening goed naleeft. Bij het bepalen of een AI-systeem een grote impact heeft, worden met een aantal omstandigheden rekening gehouden, waaronder de parameters, de input en de output van het systeem, hoeveel gebruikers het systeem zal hebben, alsmede verzamelde data op basis van verschillende benchmarks en evaluaties.

Wanneer een AI-systeem voor algemene doeleinden een systeemrisico heeft, dient het aan een aantal extra voorwaarden te voldoen. Wanneer er geen sprake is van een systeemrisico, is wel nog sprake van een AI-systeem voor algemene doeleinden en dient aan de daarvoor bestemde verplichtingen voldaan te zijn.

## > 2.4 Tabel verboden systemen en systemen met een hoog risico

Onderstaande is een tabel opgericht om te verduidelijken wanneer sprake is van een volledig verboden systeem of een systeem met een hoog risico. Als het systeem onder 1 van deze onderwerpen valt, is het aannemelijk dat het systeem verboden is of een hoog risico heeft.

| Volledig verboden systemen | | Systemen met een hoog risico |
|---|---|---|
| **Gebruik van manipulatieve, bedrieglijke of vergelijkbare technieken** | | **Veiligheidscomponent of product onder ‘bepaalde harmonisatiewetgeving’** |
| **Exploitatie kwetsbare personen** | | **Biometrische herkenning op afstand** |
| **Classificatie + nadelige behandeling** | | **Gebruik van biometrische gegevens** |
| **Risicoprofilering op basis van karakteristieken** | | **Veiligheidscomponent essentiële systemen** |
| **Ongericht nemen van gezichtsbeelden** | | **Toegang tot onderwijsinstellingen** |
| **Afleiden van emoties** | | **Evalueren onderwijsresultaten** |
| **Categorisering door biometrische gegevens** | | **Werving- en selectie bij werk** |
| **Biometrische identificatie op afstand in ‘real time’** | | **Essentiële bestuursdiensten en -uitkeringen** |
| | | **Risicoschatting levens- en gezondheidsverzekeringen** |
| | | **Reageren op noodoproepen** |
| | | **Systemen in strafzaken** |

| | | |
|---|---|---|
| | | **Migratie** |
| | | **Gebruik door rechters** |
| | | **m.b.t. stemrecht** |

## 3. Plichten en voorwaarden voor (aanbieders van) AI-systemen

> 3.1 AI-geletterdheid en de transparantieverplichting

Er zijn twee verplichtingen waar een AI-systeem altijd aan moet voldoen. Het maakt daarbij niet uit om welk soort AI-systeem het gaat.

De eerste verplichting die geldt is dat iedereen die met AI werkt, tot op bepaalde mate AI-geletterd is. Dit betekent dat iedereen die met AI wil werken, technische kennis en ervaring moet hebben. Het is ook belangrijk dat diegene een opleiding heeft gevolgd, waar AI tot bepaalde mate in terugkomt. Hoewel dit niet verplicht is, kan dit veel helpen om aan deze verplichting te voldoen. Daarnaast moet deze persoon niet alleen weten hoe hij/zij/die met AI werkt, maar ook bewust zijn van de risico's van AI.

De tweede verplichting voor alle AI-systemen is om te zorgen voor voldoende transparantie. Met transparantie wordt bedoeld dat voor gebruikers altijd duidelijk is dat zij in aanraking komen met een AI-systeem. Zij weten daarnaast ook welke rechten en plichten zij hebben wanneer zij met het systeem in aanraking komen, en hoe ze het model moeten gebruiken. Omdat transparantie een heel belangrijke verplichting is voor de EU, hebben ze deze plicht opgedeeld in een aantal onderdelen. Deze zijn:

- **Interactie met het systeem:** Het systeem wordt ontworpen op een manier dat altijd duidelijk is voor gebruikers dat zij in aanraking komen met een AI-systeem. Hieraan kan bijvoorbeeld voldaan worden d.m.v. een bericht voorafgaande de eerste interactie met het systeem, waar duidelijk op staat dat dit een AI-systeem is.

- **Vermelding gegenereerde inhoud:** Wanneer het systeem in zijn output een audio- beeld- video- of tekstinhoud genereerd, wordt gezorgd dat altijd duidelijk is dat het gaat om een kunstmatig gegenereerde of gemanipuleerde inhoud. Dus wanneer het systeem iets genereert is altijd duidelijk aan iemand die dit ziet dat het om de resultaten van een AI-systeem gaat. Er wordt goed voor gezorgd dat alle resultaten die het systeem genereert doeltreffend en betrouwbaar zijn.

- **Zorgvuldige verwerking persoonsgegevens:** wanneer het systeem emoties herkent of biometrische gegevens verwerkt, wordt de gebruiker daar duidelijk en volledig over geïnformeerd. Persoonsgegevens worden verwerkt in overeenstemming met overige wetgeving betreffende privacyregels. Deze worden dus met dezelfde zorgvuldigheid verzorgd als bij andere situaties waarin persoonsgegevens verwerkt worden.

- **Gebruik van deep fakes:** wanneer het systeem als output een 'deep fake' genereert wordt duidelijk gemaakt dat de output gegenereerd of gemanipuleerd is. Met een deep fake wordt bedoeld een output in de vorm van een beeld-, audio-, of videomateriaal dat een gelijkenis vormt aan een bestaand persoon, voorwerp, plaats of andere entiteit of gebeurtenis. In het geval dat deze deep fake voor artistieke, creatieve, satirische of fictieve doeleinden gebruikt wordt, kan deze vermelding op zodanige wijze gedaan worden, dat genot van de output niet belemmerd wordt.

- **Tekst voor algemeen belang:** Wanneer tekst gegenereerd wordt om het publiek te informeren over aangelegenheden voor algemeen belang, word bekend gemaakt dat de tekst gegenereerd of gemanipuleerd is door middel van een AI-systeem

- **Verstrekking informatie:** Alle relevante informatie die nodig is in het kader van transparantie, dus alle informatie die belangrijk is om te voldoen aan bovenstaande voorwaarden, wordt uiterlijk op het moment van 1ste interactie met het AI-systeem verstrekt.

<u>> 3.2 Plichten en voorwaarden voor systemen met een hoog risico</u>

Wanneer een systeem aangeduid wordt als een systeem met een hoog risico, dient het aan een flink aantal andere voorwaarden te voldoen. Ieder van deze plichten wordt onderstaande uitgelegd. Er zijn ook een paar plichten m.b.t. het trainen en testen van AI-systemen met een hoog risico, deze staan uitgewerkt in paragraaf 2 van onderdeel 3.4.

*1. Systeem voor risicobeheer*

De eerste plicht is het verzorgen van een systeem voor risicobeheer. Dit is een systeem dat tijdens de gehele levensduur van het AI-systeem bepaalde taken uitvoert. Deze wordt periodiek herzien en geactualiseerd. De taken van het systeem voor risicobeheer zijn:

- Het analyseren en vaststellen van risico's voor de gezondheid, veiligheid of grondrechten

- Het inschatten en evalueren van risico's die kunnen voordoen i.v.m. redelijkerwijs te voorzien misbruik

- Het evalueren van overige risico's die zich kunnen voordoen n.a.v. door het systeem verzamelde data, nadat het systeem in handel gebracht is

- Het vaststellen van gerichte en gepaste maatregelen om de risico's uit het eerste punt aan te pakken.

Met risico's wordt in deze paragraaf bedoeld risico's die uitgesloten of beperkt kunnen worden door het ontwikkelen of ontwerpen van het AI-systeem, of door het verstrekken van informatie. Het systeem voor risicobeheer en de daarbij behorende maatregelen worden zodanig ingesteld dat het resterende risico als 'aanvaardbaar' gezien kan worden. Hiervoor kan worden gezorgd door risico's uit te sluiten voor zover technisch mogelijk en de overige risico's zoveel mogelijk te beperken, alsmede door correcte informatie te verstrekken. Ook belangrijk is dat het AI-systeem goed getest wordt zodat nodige maatregelen getroffen kunnen worden voor het in handel brengen daarvan.

*2. Systeem voor kwaliteitsbeheer*

Het systeem voor kwaliteitsbeheer is een systeem dat toegevoegd wordt aan elk AI-systeem met een hoog risico, wat ervoor zorgt dat alle bepalingen uit de AI-verordening (en eventuele andere plichten) gewaarborgd worden. In het systeem voor kwaliteitsbeheer worden schriftelijke beleidslijnen, procedures en instructies opgenomen t.a.v. de volgende aspecten:

- een strategie voor naleving van de regelgeving
- technieken, procedures en systematische maatregelen voor het ontwerp van het AI-systeem en de kwaliteitscontrole daarvan
- procedures voor het inspecteren, testen en valideren van het AI-systeem, die regelmatig uitgevoerd worden
- technische specificaties en middelen die worden toegepast om te zorgen dat het AI-systeem in overeenstemming is met geharmoniseerde normen uit de unie
- systemen voor alles gerelateerd aan databeheer en andere handelingen m.b.t. datagegevens
- het systeem voor risicobeheer
- het opzetten, toepassen en onderhouden van het systeem voor monitoring
- procedures i.v.m. het melden van een ernstig incident
- communicatie met relevante autoriteiten, alsmede met andere operatoren, klanten en andere belanghebbenden
- systemen en procedures voor registratie van alle relevante documentatie
- het beheer van hulpmiddelen
- een kader waarin de verantwoordelijkheid van het management en ander personeel uiteen gezet wordt

*3. Training van het systeem*

AI-systemen worden getraind op data. Op basis van de AI-verordening dient data die gebruikt wordt om AI te trainen te voldoen aan bepaalde kwaliteitseisen. Ook voor validatie en testen van het systeem op basis van data gelden deze vereisten.

De datareeksen worden onderworpen aan praktijken op het gebied van databeheer, die gelijk zijn aan het doel van het AI-systeem. Deze praktijken hebben onder andere betrekking op:
- processen voor verzameling van de data
- relevante verwerkingsactiviteiten van de data
- beoordeling van de beschikbaarheid, kwantiteit en geschiktheid van benodigde datareeksen
- beoordelingen met het oog op vertekeningen, die gevolgen kunnen hebben voor gezondheid of veiligheid van personen, nadelige effecten op grondrechten, etc. alsmede passende maatregelen om deze vertekeningen op te sporen, te voorkomen en te beperken

Daarnaast dienen de datareeksen ook relevant, representatief, zoveel mogelijk foutenvrij en volledig te zijn, hierbij lettend op het beoogde doel van het AI-systeem. Verder wordt bij de datareeksen ook rekening gehouden met enige geografische, contextuele, functionele of gedragsomgevingen waarin het AI-systeem gebruikt wordt.

*4. Registratie & technische documentatie*

Tijdens de levensduur van een AI-systeem met een hoog risico dient heel veel informatie bijgehouden te worden. De plicht van registratie staat ervoor dat het AI-systeem een toevoeging (of iets vergelijkbaars daaraan) krijgt, waardoor alle gebeurtenissen van het AI-systeem automatisch geregistreerd worden. Met welke informatie opgenomen moet worden kan gedacht worden aan ten minste: de duur van elk gebruik (incl. begin- en einddatum), een referentiebank aan de hand waarvan inputdata gecontroleerd wordt, de inputdata aan de hand waarvan de zoekopdracht een resultaat leverde, en enige identificatie van personen die betrokken zijn bij de verificatie van resultaten.

Ook is het zeer belangrijk correcte technische documentatie bij te houden. Deze wordt opgemaakt voordat het systeem in handel gebracht wordt en is altijd geactualiseerd en wordt zo helder mogelijk gemaakt voor enige relevante autoriteiten. Onderstaande is een checklist toegevoegd van alle onderwerpen die in de technische documentatie verwerkt dienen te worden.

*> Checklist technische documentatie*

Onderstaande informatie dient ten minste in de technische documentatie voor te komen.

**- Algemene beschrijving van het systeem**

- Het doel van het systeem, de naam van de aanbieder en de versie van het systeem

- Hoe het systeem reageert op andere software, incl. andere AI-systemen

- Versies van software en eventuele updates daaraan

- Vormen waarin het AI-systeem mee in handel gebracht wordt, b.v. downloads of API's

- De hardware waarop het systeem moet worden uitgevoerd

- Indien het systeem onderdeel is van een product de externe kenmerken, markeringen en interne lay-out van dat product

- Een basisbeschrijving van de gebruikersinterface en enige andere gebruiksinstructies

**- Beschrijving van de elementen van het systeem**

- Alle stappen en methoden die zijn uitgevoerd voor het systeem te ontwikkelen

- De ontwerpspecificaties van het systeem, voornamelijk m.b.t. de algemene logica van het systeem en de algoritmen

- Een beschrijving van de systeemarchitectuur

- Datavereisten voor de informatiebladen waarop trainingsmethoden en -technieken zijn beschreven

- een beoordeling van de maatregelen voor menselijke toezicht

-beschrijvingen van alle vooraf bepaalde wijzigingen aan het AI-systeem

- De gebruikte validatie- en testprocedures

- alle gehanteerde cyberbeveiligingsmaatregelen

**- Overige technische documentatie**

- Gedetailleerde informatie over monitoring, werking en controle van het systeem

- Een beschrijving van de geschiktheid van de prestatiestatistieken

- een gedetailleerde omschrijving van het systeem voor risicobeheer

- een beschrijving van alle relevante wijzigingen die door da aanbieder tijdens de levensduur van het systeem worden aangebracht

- Een lijst met Europese wetgeving die geheel of gedeeltelijk toegepast wordt

- (Een kopie van) de EU-conformiteitsverklaring

- een gedetailleerde omschrijving van het ingevoerde systeem dat de prestaties van het AI-systeem evalueert.

*5. Menselijk toezicht*

Wanneer een AI-systeem met een hoog risico ontworpen wordt, dient dit ten alle tijden zodanig te gebeuren dat tijdens de gehele levensduur van het systeem menselijk toezicht gehouden kan worden. Dit toezicht ziet erop dat risico's m.b.t. gezondheid, veiligheid en grondrechten door gebruik van het systeem voorkomen of beperkt worden. De toezichthouder wordt in staat gesteld een aantal dingen te doen zodat hij zijn taak goed kan vervullen:

- Hij kan relevante capaciteiten van het systeem goed begrijpen en monitoren. Daarnaast kan hij enige onregelmatigheden, storingen of onverwachte prestaties opsporen en aanpakken

- Hij blijft bewust van de mogelijke neiging om automatisch of te veel vertrouwen op de outputs van het systeem te vertrouwen

- Hij kan de output van het systeem juist interpreteren

- Hij kan in alle specifieke situaties besluiten het systeem niet te gebruiken of de output te kunnen negeren

- Hij kan ingrijpen in de werking van het systeem of het systeem onderbreken

- Bovenstaande dienen gelezen te worden als minimum. Indien passend worden ook andere loggingcapaciteiten toegevoegd.

*6. Monitoringssysteem*

Ook wordt een systeem voor monitoring toegevoegd aan het AI-systeem. Dit systeem voor monitoring verzamelt, documenteert en analyseert alle relevante data van gebruikers van het systeem. Andere bronnen van interactie, zoals interacties met andere AI-systemen, worden ook hierin meegenomen. Voordat het systeem van monitoring ontworpen wordt, word hiervoor een plan opgezet. Het systeem voor monitoring wordt gebaseerd op dit plan. Het monitoringssysteem is actief tijdens de gehele levensduur van het AI-systeem.

*7. Melding ernstige incidenten*

Wanneer een 'ernstig' incident zich voordoet, dient de aanbieder bij wie dit gebeurde een melding hiervan te maken bij de relevante marktautoriteit. Dit is de instelling die namens het AI-bureau toeziet op naleving van de AI-verordening binnen een bepaalde lidstaat. Deze melding wordt altijd zo snel mogelijk gedaan, maar gebeurt uiterlijk binnen 15 dagen. Onder ernstig incident worden de volgende soort incidenten die direct of indirect veroorzaakt zijn door het AI-systeem verstaan:

- het indirect of direct veroorzaken van het overleiden van of ernstige schade aan de gezondheid van een persoon

- het indirect of direct veroorzaken van een ernstige en onomkeerbare verstoring van belangrijke infrastructuur

- het indirect of direct veroorzaken van een schending van de verplichtingen uit het unierecht ter bescherming van de grondrechten

- het indirect of direct veroorzaken van ernstige schade aan eigendommen of het milieu

Na melding verricht de aanbieder onderzoek naar de oorzaak van het incident, en zorgt hij dat corrigerende maatregelen toegepast worden. De aanbieder werkt hierbij samen met de bevoegde autoriteiten.

*8. CE-markering*

De meeste producten binnen de Europese Unie dienen een CE-markering op zich te dragen. Dit is een markering waarmee duidelijk gemaakt wordt, dat voldaan is aan alle relevante wetgeving van de EU. Hiermee stelt de aanbieder zich ook verantwoordelijk voor dat het product overeenkomt met alle relevante wetgeving. De CE-markering wordt op een duidelijke manier op het product geplaatst. Wanneer het product (of alleen het AI-systeem indien er geen product is) enkel online beschikbaar is, mag de markering ook online aangebracht worden. Er mogen geen andere markeringen aangebracht worden die door iemand anders gezien kunnen worden als een CE-markering. De CE-markering wordt pas toegevoegd nadat de conformiteitsprocedure voldaan is.

*9. Conformiteitsprocedure*

Wanneer een aanbieder een AI-systeem op de markt wil brengen, dient hij eerst een conformiteitsverklaring te krijgen (conformiteit = in overeenstemming met). Deze conformiteitsverklaring is een manier om te laten zien aan relevante autoriteiten dat het AI-systeem voldoet aan alle relevante eisen van de AI-verordening. Om deze verklaring te mogen opstellen, moet eerst voldaan zijn aan een conformiteitsbeoordeling. Er zijn 2 manieren waarop de conformiteitsbeoordeling kan plaatsvinden

De eerste procedure is de interne controle. Deze wordt door aanbieder zelf uitgevoerd. Deze bestaat uit 3 stappen. Als eerst wordt gecontroleerd of het systeem voor kwaliteitsbeheer voldoet aan alle eisen. Vervolgens wordt nagegaan of de technische documentatie volledig is en aan alle eisen voldoet. De derde stap is om te controleren of het ontwerp- en ontwikkelingssysteem en het systeem voor monitoring overeenkomen met de technische documentatie.

De tweede procedure is de beoordeling van het systeem van kwaliteitsbeheer en technische documentatie met betrokkenheid van een aangemelde instantie. De aangemelde instantie is een instantie die zich bij de lidstaat heeft aangemeld om op een bepaald werkveld conformiteit met de Europese wetgeving te beoordelen. Beide het systeem voor kwaliteitsbeheer en de technische documentatie worden uitvoerig bestudeerd door de aangemelde instantie voordat deze tot een beslissing komt. Na de procedure dient tevens toegang tot het systeem voor kwaliteitsbeheer verleend te worden aan de aangemelde instantie, zodat deze periodiek opnieuw toetst of nog steeds aan alle voorwaarden voldaan is.

De aanbieder mag in de meeste situaties zelf beslissen welke procedure hij volgt. Echter, er zijn een paar situaties waarin hij verplicht is de 2$^{de}$ procedure te volgen:
- het systeem behoort niet tot een geharmoniseerde norm of een gemeenschappelijke specificatie
- De geharmoniseerde norm is niet of enkel deels toegepast
- de gemeenschappelijke specificatie bestaat wel maar is niet toegepast
- in gevalle van een AI-systeem dat bedoeld wordt voor werk m.b.t. rechtshandhaving, immigratie of asiel treed de markttoezichtautoriteit altijd als aangemelde instantie op in het kader van de beoordeling. De aanbieder heeft dus geen eigen keuze meer bij wie hij zijn verzoek indient.

Wanneer sprake is van een AI-systeem dat als hoog risico aangemerkt, met uitzondering van systemen voor verwerken van biometrische gegevens en systemen die als systemen met een hoog risico aangemerkt worden op basis van bepaalde harmonisatiewetgeving (zie hiervoor paragraaf 2.2.1), gaan deze altijd voor conformiteitsbeoordeling via de interne controle.

Iedere keer dat een AI-systeem aanzienlijk veranderd wordt, dient deze opnieuw aan de conformiteitsbeoordelingsprocedure te voldoen. Wanneer een AI-systeem doorgaat met leren en hierdoor veranderd nadat het op de markt gebracht is, geld dit niet als substantiële wijziging zolang de technische documentatie dit goed bijhoudt.

Na goedkeuring stelt de aanbieder zelf een conformiteitsverklaring op, waaruit blijkt dat het AI-systeem aan alle relevante eisen en voorwaarden voldoet. Op verzoek wordt een kopie hiervan voorgelegd aan een nationale bevoegde autoriteit. In bijlage 5 wordt de informatie uit elkaar gezet, die verwacht wordt van de aanbieder. In de conformiteitsverklaring wordt ten minste opgenomen:

- de naam en het type van het AI-systeem
- de naam en adres van de aanbieder en een eventuele gemachtigde
- een vermelding dat de conformiteitsverklaring volledig voor verantwoordelijkheid van aanbieder komt
- een vermelding dat het systeem in overeenstemming is met alle relevante wetgeving
- indien het systeem persoonsgegevens verwerkt, verzameld of op een andere manier met persoonsgegevens in aanmerking komt, een vermelding dat het systeem ook voldoet aan de relevante wetgeving m.b.t. privacy en verwerking van persoonsgegevens
- vermelding van eventuele toegepaste geharmoniseerde normen of andere gemeenschappelijke specificaties
- indien toepasselijk de naam en het identificatienummer van de aangemelde instantie en een beschrijving van de uitgevoerde conformiteitsbeoordelingsprocedure
- de plaats en datum van de afgifte van de conformiteitsverklaring alsmede de naam en functie van de persoon die ondertekent.

*10. Registratie EU-databank*

De commissie en de lidstaten van de EU zorgen ervoor dat een Europese AI-databank opgezet wordt. Wanneer een aanbieder een systeem met een hoog risico op de markt brengt, dienen beide de aanbieder en het AI-systeem geregistreerd te worden in deze EU-databank. Als een systeem gewoonlijk gezien zou worden als systeem met hoog risico, maar het onder een uitsluitingsgrond valt, dient het alsnog in de databank opgenomen te worden. Hoewel de databank algemeen toegankelijk en openbaar is, wordt registratie van systemen m.b.t. rechtshandhaving, migratie, asiel en grensbeheer niet openbaar gemaakt.

*11. Overige verplichtingen*

Naast bovenstaande zijn er nog een paar extra verplichtingen opgelegd aan aanbieders van AI-systemen met een hoog risico:
- Aanbieders zorgen dat hun naam, geregistreerde handelsnaam of geregistreerde merknaam en contactgegevens bij het AI-systeem, op de verpakking van het product waar het AI-systeem aan toebehoort, of in de bijgevoegde documentatie beschikbaar is.

- alle relevante documentatie wordt op een passende manier bewaard, inclusief de door het AI-systeem gegenereerde logs. Deze worden voor ten minste 10 jaren bewaard

- indien nodig worden corrigerende maatregelen genomen voor het AI-systeem

- indien hiernaar verzocht wordt door de nationale autoriteit kan aanbieder aantonen dat hij in overeenkomst met de wet handelt

<u>> 3.3 Plichten en voorwaarden voor systemen voor algemene doeleinden</u>

Wanneer een AI-systeem gezien wordt als een systeem voor algemene doeleinden, dient het aan een aantal verplichtingen te doen. Hoewel het er lang niet zoveel zijn als de verplichtingen bij een systeem met een hoog risico, dient alsnog zorgvuldig te worden nagegaan of aan al deze eisen voldaan is. Wanneer een AI-systeem voor algemene doeleinden een systeemrisico heeft, dient ook aan een paar bijkomende voorwaarden voldaan te zijn.

*1. Verplichtingen voor AI-systemen voor algemene doeleinden*

Alle AI-systemen voor algemene doeleinden dienen aan een aantal voorwaarden te doen, ongeacht of er een systeemrisico aanwezig is.

De eerste verplichting is dat technische documentatie van het model wordt opgesteld en bijgehouden. In de technische documentatie wordt ten minste opgenomen;
- het trainings- en testproces en een evaluatie van de resultaten daaruit
- De taken die het model uit dient te voeren, alsmede de type en aard van andere systemen waar het in geïntegreerd kan worden
- de “acceptable use policies” die van toepassing zijn
- de datum van uitgave en de wijze van verspreiding
- de architectuur en het aantal parameters
- de modaliteit en het formaat van de input en output
- de licentie
- De technische middelen die nodig zijn voor integratie in andere systemen
- De specificaties van het ontwerp van het model en het trainingsproces, met inbegrip van trainingsmethoden en -technieken
- Informatie over de gegevens die zijn gebruikt voor training, tests en validatie

- De rekenhulpmiddelen die zijn gebruikt om het model te trainen, alsmede de duur van de training en enige andere bijzonderheden
- Bekend of geschat energieverbruik van het model
- Naast bovenstaande wordt ook enige aanvullende informatie opgenomen, die redelijkerwijs nodig is om de technische documentatie volledig te maken. Hiermee wordt onder andere bedoeld 'een gedetailleerde beschrijving van evaluatiestrategieën', 'een gedetailleerde omschrijving van de maatregelen die zijn genomen' en 'een gedetailleerde omschrijving van de systeemarchitectuur'.

Informatie en documentatie moet opgesteld worden voor andere aanbieders die het AI-systeem voor algemene doeleinden in hun eigen AI-systeem willen integreren. Deze informatie moet andere aanbieders inzicht geven in de capaciteiten en beperkingen van het systeem. Deze moet ook omvattend genoeg zijn om andere aanbieders in staat te stellen aan hun verplichtingen te voldoen. De informatie die hierin opgenomen moet worden is grotendeels hetzelfde als bij de technische documentatie, met een paar extra toevoegingen:
- Hoe het model reageert of kan reageren op hardware of software waar het zelf geen onderdeel van is, indien van toepassing

- De versies van de relevante software met betrekking tot het gebruik van het model, indien van toepassing'.

Een volgende verplichting is dat er een beleid opgesteld moet worden, waarin duidelijk gemaakt wordt hoe wetgeving van de Europese Unie in het kader van auteursrechten nageleefd zal worden.

Ook wordt een gedetailleerde samenvatting opgesteld en openbaar gemaakt over het trainen van het AI-model en de inhoud die hierbij gebruikt werd.

Naast bovenstaande worden door het AI-bureau (de instantie van de EU die zich bezig houdt met AI en de naleving van de AI-verordening) praktijkcodes ontwikkeld. Hoewel de praktijkcodes niet verplicht zijn om te volgen, vormen deze wel een manier om aan alle relevante wetgeving te voldoen. Aanbieders kunnen zich dus baseren op deze praktijkcodes om aan te geven dat de wet goed nageleefd wordt.

Wanneer een aanbieder zich buiten de unie bevindt, dient hij een gemachtigde in de EU te hebben. Deze gemachtigde krijgt ten minste genoeg bevoegdheden om te zorgen dat het AI-systeem in overeenkomst is met alle relevante wetgeving.

*2. Bijkomende verplichtingen wanneer sprake is van een systeemrisico*

Wanneer een aanbieder een AI-systeem voor algemene doeleinden met een systeemrisico op de markt wil brengen, dient hij aan een aantal bijkomende verplichtingen de voldoen. Aan deze verplichtingen hoeft niet voldaan te zijn wanneer geen sprake is van een systeemrisico.

- De eerste van deze verplichtingen is het proces dat gevolgd dient te worden, om aan het AI-bureau duidelijk te maken dat er een AI-systeem met een systeemrisico is. Wanneer sprake is van een dergelijk systeem, wordt het AI-bureau daar zo snel mogelijk van op de hoogte gesteld, maar uiterlijk binnen 2 weken, door de aanbieder van het systeem. Bij de kennisgeving hiervan mag de aanbieder beargumenteren waarom hij van mening is dat zijn systeem niet als een Ai-systeem met een systeemrisico gezien moet worden. Deze argumentatie kan ook plaatsvinden in de vorm van een verzoek achteraf.

- Er wordt een modelevaluatie uitgevoerd. Enige tests gericht op het ontdekken van kwetsbaarheden in het systeem en alle gevonden systeemrisico's worden hier ook in opgenomen.

- Alle mogelijke systeemrisico's worden beoordeeld en zo goed mogelijk beperkt

- Ernstige incidenten en enige genomen corrigerende maatregelen worden gedocumenteerd. Deze documentatie wordt geactualiseerd en wordt zo snel mogelijk overgelegd aan het AI-bureau en de bevoegde nationale autoriteit

- Er wordt gezorgd voor een passend niveau van cyberbeveiliging op het AI-systeem

## > 3.4 Trainen en testen van AI-systemen

Ook voor het trainen en testen van AI worden specifieke regels van toepassing. Als eerste is van belang dat de lidstaten van de EU en het AI-bureau samenwerken om in iedere lidstaat ten minste 1 algemene AI-testgrond op te richten. De testomgeving dient uiterlijk binnen 24 maanden na ingang van de verordening operationeel te zijn, dus vanaf 02 April 2026. Ook zorgen de bevoegde autoriteiten zo nodig voor begeleiding, toezicht en ondersteuning binnen de testomgeving, met het oog op de vaststelling van risico's.

### *1. Regels m.b.t. het werken binnen de AI-testomgeving*

Er zijn een aantal belangrijke regels voor het werken in de AI-testomgeving. Als eerste is van belang dat aanbieders altijd verantwoordelijk blijven voor alles wat het AI-systeem doet binnen de testomgeving. Ook mogen testomgevingen maar voor een beperkte duur gebruikt worden voordat het AI-systeem op de markt gebracht wordt. Bevoegde autoriteiten zullen aanwezig zijn bij de AI-testomgeving. Indien nodig verstrekken bevoegde autoriteiten begeleiding, toezicht en ondersteuning aan iedere aanbieder die de testomgeving gebruikt. Deze ondersteuning is voornamelijk erop gericht dat ondernemers in overeenkomst zijn met alle relevante wetgeving, en op het vaststellen van risico's bij het AI-systeem. Als laatste is er ook nog een belangrijke voorwaarde in dat rechtmatig verkregen persoonsgegevens alleen onder strenge voorwaarden gebruikt mogen worden binnen de testomgeving, indien de persoonsgegevens origineel voor andere doeleinden bestemd waren.

Hoewel een paar algemene regels al in de AI-verordening verwerkt staan, is het grootste deel van de regelgeving m.b.t. de testomgeving op het moment van schrijven nog niet bekend. Dit wordt op latere datum door de Europese commissie verzorgt in de vorm van uitvoeringshandelingen.

*2. Testen van een AI-systeem **met een hoog risico** buiten de testomgeving*

Het is niet verboden om een AI-systeem met een hoog risico buiten de testomgeving in reële omstandigheden te testen. Echter, er zijn wel een aantal regels opgenomen om te verzorgen dat dit goed verloopt. De voorwaarden voor het testen onder reële omstandigheden zijn:

- Er wordt een plan voor tests onder reële omstandigheden opgesteld en ingediend bij de markttoezichtautoriteit

- Het plan voor tests is goedgekeurd. Wanneer de markttoezichtautoriteit niet binnen 30 dagen gereageerd heeft, wordt ervanuit gegaan dat goedkeuring verleend is

- de aanbieder heeft het testen onder reële omstandigheden geregistreerd in de Europese AI-databank. Hierbij is zoveel mogelijk relevante informatie verstrekt

- de aanbieder is in de EU gevestigd of heeft een wettelijke vertegenwoordiger binnen de unie

- verzamelde gegevens mogen alleen aan derde landen doorgegeven worden mits dit in het belang van de unie is

- het testen onder reële omstandigheden duurt niet langer dan nodig, en onder geen omstandigheid langer dan 6 maanden. Op deze uiterlijke termijn is wel een verlenging van 6 maanden mogelijk, indien dit tijdig bij de markttoezichtautoriteit aangegeven wordt, inclusief een uitleg waarom verlenging genoodzaakt is.

- proefpersonen die kwetsbaar zijn op basis van leeftijd of gebrek worden zo goed mogelijk beschermd

- indien het testen gebeurt in samenwerking met een of meer gebruikers, worden zij geïnformeerd over alle aspecten van het testen voordat het testen begint. Daarnaast ontvangen zij alle gebruiksinstructies voor het AI-systeem.

- iedere proefpersoon onder reële omstandigheden weet wat er aan de hand is en heeft toestemming gegeven. In het geval toestemming met kennis van zaken het testen onder reële omstandigheden niet mogelijk zou maken, mag de test geen negatieve gevolgen hebben voor de proefpersonen of hun persoonsgegevens.

- er wordt daadwerkelijk toezicht gehouden op het testen door aanbieder en eventuele exploitanten. Toezicht door exploitanten geschied door voldoende gekwalificeerd personen.

- enige voorspellingen, aanbevelingen of beslissingen van het AI-systeem tijdens de testperiode kunnen teruggedraaid en genegeerd worden.

- proefpersonen kunnen zich ten alle tijden zonder nadelige gevolgen of rechtvaardiging terugtrekken uit de tests. Hierop volgende kunnen zij onmiddellijke en permanente verwijdering van hun persoonsgegevens verzoeken.

- aanbieder is aansprakelijk namens het AI-systeem voor enige schade die tijdens het testen onder reële omstandigheden geleden wordt.

## 4. Gevolgen van overtreding en mogelijke rechtsmiddelen

> 4.1 Maatregelen en sancties

Er zijn 3 mogelijke maatregelen die het AI-bureau kan nemen, waardoor aanbieders tot bepaalde handelingen verplicht worden. Deze handelingen zijn:

- De aanbieder moet passende maatregelen nemen om te voldoen aan enige verplichtingen van AI-systemen voor algemene doeleinden waar nog niet aan voldaan is

- De aanbieder moet risicobeperkende maatregelen te treffen in geval van een (redelijk vermoeden van) systeemrisico op unieniveau.

- De aanbieder moet het op de interne markt beperken of het volledig uit de handel halen of terugroepen van een AI-model

Deze maatregelen mogen altijd toegepast worden voor zover het AI-bureau dit nodig en passend vindt. Enige besluiten tot maatregel dienen wel goed onderbouwd te worden. Daarnaast moet het AI-bureau altijd overleggen met de overtredende aanbieder, voordat zij een maatregel oplegt.

Naast maatregelen kan het AI-bureau ook boetes opleggen voor iedereen (niet alleen aanbieders) die de AI-verordening overtreedt. De mogelijke boetes zijn als volgt:

- Wanneer een volledig verboden AI-systeem op de markt gebracht wordt, dan wel op een andere manier in gebruik gesteld wordt, geld een boete van 35 miljoen euro, dan wel 7% van de totale wereldwijde omzet indien dit meer is.

- In een aantal gevallen geldt een boete van 15 miljoen euro, dan wel 3% van de wereldwijde omzet indien dit meer is:
-- een aanbieder schendt een verplichting m.b.t. AI-systemen met een hoog risico
-- een gemachtigde // importeur // gebruiker schendt een van zijn verplichtingen
-- een van de transparantieverplichtingen wordt geschonden

- in het geval er onjuiste, onvolledige of misleidende informatie aan een bevoegde instantie overgelegd wordt op basis van verzoek, wordt een boete opgelegd van maximaal 7,5 miljoen euro, dan wel 1% van de totale wereldwijde omzet van het bedrijf indien dit meer is.

- Ook in de volgende gevallen is sprake van een boete van maximaal 15 miljoen euro, dan wel 3% van de totale wereldwijde omzet indien dit meer is:
-- er wordt inbreuk gepleegd op een van de bepalingen uit de AI-verordening, waar nog geen boete op gesteld is
-- Er wordt niet voldaan aan een verzoek of document, dan wel onjuiste, onvolledige of misleidende informatie verstrekt heeft
-- Een opgelegde maatregel wordt niet nageleefd
-- De aanbieder geen toegang heeft verleend aan het AI-bureau tot het AI-model voor algemene doeleinden, op basis waarvan de commissie een evaluatie kan geven

Bij alle boetes die worden opgelegd wordt altijd rekening gehouden met de aard en ernst van de overtreding. Ook wordt goed gelet op overige omstandigheden en context. Daarnaast wordt een aanbieder ook altijd in de gelegenheid gesteld om zichzelf te verdedigen in het geval dat het AI-bureau een boete wil opleggen.

> 4.2 Rechtsmiddelen

Het kan voorkomen dat een instelling van de EU (b.v. het AI-bureau) of een lidstaat van de EU een besluit maakt waar een aanbieder het niet mee eens is, b.v. het opleggen van een maatregel of boete. In deze gevallen zijn er een aantal manieren om hier tegenop te komen. Het wordt sterk aangeraden om eerst met een jurist in overleg te gaan, voordat een van deze handelingen genomen wordt.

- standaard rechtsgang: Iedere persoon of onderneming die geraakt wordt door een handeling van een andere Europese instelling en het hier niet mee eens is, kan hier bezwaar tegen indienen. Dit gebeurt uiterlijk 2 maanden na het originele besluit bekend gemaakt is. Dit geldt niet alleen voor besluiten op basis van de AI-verordening. Tegen de meeste handelingen van de EU-instelling is het wel mogelijk om bezwaar in te dienen. Het bezwaar wordt ingediend bij de instelling die het originele besluit nam.

- een aangetekende klacht: Wanneer iemand redelijkerwijs denkt dat een marktautoriteit een bepaling uit deze verordening overschrijdt, kan deze ten alle tijden een aangetekende klacht indienen. De marktautoriteit in dit geval is degene die zich bezig houdt met de toepassing van de verordening namens het AI-bureau. Deze klacht wordt bij de marktautoriteit zelf ingediend.

- toelichting bij individuele besluitvorming: Wanneer een AI-systeem een besluit met rechtsgevolgen neemt, kan elke door dat besluit getroffen persoon een duidelijke inhoudelijke toelichting krijgen over de rol van het AI-systeem. Deze toelichting wordt verzocht bij de instelling die het besluit genomen heeft, vaak zal dit het AI-bureau zijn.

- melden overtredingen: Iedereen is bevoegd om een melding in te dienen bij de commissie, betreffende een overtreding van deze richtlijn. Wanneer iemand een dergelijke melding indienen, worden zij in overeenstemming met het unierecht beschermd.