



AI Verordening – Risicoclassificatie, Rol bepaling en overzicht Verplichtingen

Bezoekadres

Papendallaan 60, Arnhem

Postadres

Postbus 302, 6800 AH Arnhem

Telefoon

+31 (0)26 483 44 00

Email

info@nocnsf.nl

Web

nocnsf.nl

Partners: Nederlandse Loterij ○ Odido ○ AD ○ MissieH2 ○ Rabobank

Introductie

Dit document is opgesteld door de AI Officer van NOC*NSF en is bedoeld als hulpmiddel om binnen de kaders van de AI Verordening een inschatting te maken van de risicoclassificatie van de AI dat wordt ingezet binnen NOC*NSF, de rol waarin NOC*NSF de AI inzet en de bijlage geeft vervolgens aan welke verplichtingen er gelden voor NOC*NSF aan de hand van de rol en risico classificatie.

In Stap 0 wordt bepaald of er gebruik wordt gemaakt van AI, hetzij door NOC*NSF zelf of door de leveranciers die door NOC*NSF zijn gecontracteerd. In de daarop volgende stappen wordt bepaald of er uitzonderingen van toepassingen zijn, wat de risicoclassificatie is, wat de rolbepaling is van NOC*NSF en wat vervolgens de verplichtingen zijn.

*Let op: De onderhavige vragenlijst om de risico classificatie van het AI systeem en de rol van NOC*NSF daarin te duiden is met zorg opgesteld, maar doordat de AI Verordening nog nieuw is en er nog weinig richtlijnen en jurisprudentie zijn zal dit document regelmatig worden herzien.*

Stap 0: Is dit een AI tool?

Is dit een AI-tool?

Beantwoord de volgende vragen om dat te bepalen:

1. Maakt of vat de tool inhoud samen?

Bijvoorbeeld tekst, afbeeldingen, video's, enz.

Toelichting: Als de tool zelf inhoud kan maken of samenvatten (zoals tekst schrijven of beelden genereren), is dat een sterke aanwijzing dat het AI gebruikt.

- **Ja: Waarschijnlijk AI → AI-verordening van toepassing**
- **Nee: Ga naar vraag 2**

2. Is de tool getraind met machine learning?

Toelichting: Machine learning betekent dat de tool leert van data in plaats van alleen vaste regels te volgen. Een ML-model maakt gebruik van gegevens om patronen te herkennen en op basis daarvan voorspellingen of beslissingen te nemen.

- **Ja: Waarschijnlijk AI → AI-verordening van toepassing**
- **Nee: Ga naar vraag 3**

• **Gebruikt de tool inferentie, redenering, modellering of profilering?**

Bijvoorbeeld voorspellingen doen, aanbevelingen geven of beslissingen nemen.

Toelichting: Als de output gebaseerd is op complexe denkprocessen of analyses, is er waarschijnlijk AI in het spel.

- **Inferentie** betekent het afleiden van nieuwe informatie
- **Redenering** betekent logisch denken
- **Modellering** betekent een wiskundige representatie van gegevens
- **Profilering** betekent gedragsanalyse
- **Voorbeeld:** een tool zijn die aanbevelingen doet op basis van gebruikersgedrag of voorspellingen maakt op basis van historische gegevens.
- **Ja: Waarschijnlijk AI → AI-verordening van toepassing**
- **Nee: Ga naar vraag 4**

4. **Werkt de tool deels of helemaal zelfstandig?**

Toelichting: Als de tool dingen doet zonder dat je bij elke stap hoeft in te grijpen, is er sprake van autonomie. Dit kan betekenen dat de tool zelfstandig taken uitvoert (zoals een chatbot die automatisch klantenservice biedt) of zelf beslissingen neemt op basis van de gegevens die het ontvangt.

- **Ja: Waarschijnlijk AI → AI-verordening van toepassing**
- **Nee: Ga naar vraag 5**

5. **Leert de tool voortdurend van de input die het ontvangt?**

Toelichting: Als de tool zichzelf steeds verbetert door nieuwe data, noemen we dat zelflerend of adaptief. Bijvoorbeeld, een ML-model dat wordt gebruikt om klantvoorkeuren te voorspellen, kan zijn voorspellingen verbeteren naarmate het meer interacties met klanten krijgt

- **Ja: Waarschijnlijk AI → AI-verordening van toepassing**
- **Nee: Ga naar vraag 6**

6. **Wordt de tool door de leverancier gepresenteerd als 'AI' of 'ML'?**

Toelichting: Als de leverancier het een AI- of machine learning-tool noemt, is dat een duidelijke aanwijzing.

- **Ja: Waarschijnlijk AI → AI-verordening van toepassing**
- **Nee: Ga naar vraag 7**

7. **Voert de tool alleen vaste regels uit die door mensen zijn ingesteld?**

Toelichting: Als de tool alleen simpele, vooraf ingestelde regels volgt (zoals workflows of validatieregels), is het waarschijnlijk géén AI.

- **Ja: Waarschijnlijk géén AI → AI-verordening waarschijnlijk niet van toepassing**
- **Nee: Waarschijnlijk géén AI → AI-verordening waarschijnlijk niet van toepassing**

Stap 1: Is een (of meerdere) van onderstaande uitzonderingen op het AI systeem van toepassing?

☐ Wetenschappelijk onderzoek en ontwikkeling

Het AI-systeem, inclusief de gegenereerde output, is uitsluitend ontwikkeld en ingezet voor wetenschappelijk onderzoek en technologische ontwikkeling.

Voorbeeld: Een universiteit gebruikt een AI-model om patronen in klimaatdata te analyseren, zonder commerciële of operationele toepassingen.

☐ Onderzoek, test of ontwikkelfase (niet in reële omstandigheden)

Het AI-systeem bevindt zich nog in de onderzoeks-, test- of ontwikkelfase en wordt niet gebruikt in reële of productieve omgevingen.

Let op: Zodra het systeem daadwerkelijk in gebruik wordt genomen, valt het onder de AI-Verordening.

Voorbeeld: Een startup test een AI-chatbot intern om juridische vragen te beantwoorden, maar deze is nog niet beschikbaar voor klanten.

☐ Persoonlijk en niet-professioneel gebruik

Het AI-systeem wordt uitsluitend gebruikt voor persoonlijke, niet-commerciële en niet-professionele doeleinden.

Voorbeeld: Een hobbyist experimenteert met een AI-model om poëzie te genereren voor eigen gebruik, zonder deze te publiceren of te verkopen.

*Als je een van de bovenstaande vinkjes hebt aangevinkt, dan is de AI Verordening op het AI systeem niet van toepassing. **Je hoeft dan de vragenlijst niet verder in te vullen.***

[Zie voor meer informatie: artikel 2 AI Verordening]

Stap 2: Is het AI systeem bedoeld voor een of meerdere van de volgende verboden toepassingen?

- ☐ Het classificeren van mensen gebaseerd op hun kenmerken of gedrag met negatieve gevolgen, zoals 'social scoring' op basis van van bepaald sociaal gedrag of persoonlijke kenmerken.
- ☐ Het beoordelen of voorspellen van het risico dat natuurlijke personen strafbare feiten plegen, zoals 'predictive policing' om strafbare feiten bij mensen te beoordelen of te voorspellen.
- ☐ het creëren of (via scraping van internet of CCTV-beelden) uitbreiden van databanken voor gezichtsherkenning.
- ☐ manipuleren of misleiden van mensen, waarbij personen mogelijk fysieke of psychologische schade oplopen.
- ☐ emotieherkenning in de werkomgeving en het onderwijs, behalve wanneer het gebruik van het AI-systeem is bedoeld om uit medische of veiligheidsoverwegingen te worden ingevoerd.
- ☐ Het gebruikmaken van de kwetsbaarheden van een specifieke groep personen als gevolg van hun leeftijd of fysieke of geestelijke handicap. Bijvoorbeeld aan deze groep specifiek commerciële e-mails versturen om loterij kaartjes te kopen, omdat de kans groter is dat ze deze producten zullen afnemen.
- ☐ Biometrische categorisering die natuurlijke personen individueel in categorieën indeelt op basis van biometrische gegevens om hun ras, politieke opvattingen, lidmaatschap van een vakbond, religieuze of levensbeschouwelijke overtuigingen, seksleven of seksuele gerichtheid af te leiden, tenzij het gaat om het labelen of filteren van rechtmatig verkregen biometrische datasets, zoals afbeeldingen, op basis van biometrische gegevens of categorisering van biometrische gegevens op het gebied van rechtshandhaving.

*Als je een of meerdere van bovenstaande vinkjes hebt aangevinkt, dan is er **hoogstwaarschijnlijk sprake van een verboden praktijk. Neem zo snel mogelijk contact op met de AI Officer, want in het geval van een verboden praktijk moet je per direct stoppen met de activiteit.***

[Zie voor meer informatie: Artikel 5 AI Verordening]

Stap 3: Is het AI-systeem bedoeld als veiligheidscomponent van een product of is het zelf een product dat valt onder het volgende:

- ☐ Machinerichtlijn
- ☐ Veiligheid van speelgoed
- ☐ Pleziervaartuigen en waterscooters
- ☐ Liften en veiligheidscomponenten daarvan.
- ☐ Beveiliging van ontploffingsgevaar
- ☐ Radioapparatuur
- ☐ Drukapparatuur
- ☐ Kabelbaaninstallaties

- ☐ Persoonlijke beschermingsmiddelen
- ☐ Gasverbrandingstoestellen
- ☐ Medische hulpmiddelen
- ☐ Beveiliging burgerluchtvaart
- ☐ Goedkeuring van en het markttoezicht op twee- of driewielige voertuigen en vierwielers
- ☐ Goedkeuring van en het markttoezicht op landbouw- en bosbouwvoertuigen
- ☐ Uitrusting van zeeschepen
- ☐ Interoperabiliteit van het spoorwegsysteem in de Europese Unie
- ☐ Goedkeuring en markttoezicht op twee, drie en vierwielige voertuigen
- ☐ Systemen, onderdelen en technische eenheden die voor de algemene veiligheid van voertuigen en de bescherming van inzittenden en kwetsbare weggebruikers betreft
- ☐ Burgerluchtvaart

*Als je een of meerdere van bovenstaande vinkjes hebt aangevinkt, dan is er **mogelijk sprake van een hoog risico systeem**. Check dan ook of er een CE keuring door een derde partij moet worden uitgevoerd en overleg zo snel mogelijk met de AI Officer.*

[Zie voor meer informatie: artikel 6, lid 1 en Bijlage I AI Verordening]

Stap 4: Is het AI systeem bedoeld voor, of werkzaam in de volgende gebieden:

Werkgelegenheid, personeelsbeheer en toegang tot zelfstandige arbeid

- ☐ Werven of selecteren van natuurlijke personen, met name voor het plaatsen van gerichte vacatures, het analyseren en filteren van sollicitaties, en het beoordelen van kandidaten.
- ☐ Het nemen van besluiten die van invloed zijn op de voorwaarden van arbeid gerelateerde betrekkingen, de bevordering of beëindiging van arbeid gerelateerde contractuele betrekkingen, voor het toewijzen van taken op basis van individueel gedrag of persoonlijke eigenschappen of kenmerken, of voor het monitoren en evalueren van prestaties en gedrag van personen in dergelijke betrekkingen.

Biometrie:

- ☐ Identificatie op afstand, voor zover het systeem niet als enig doel heeft te bevestigen dat een specifiek natuurlijke persoon de persoon is die deze beweert te zijn.
- ☐ Categorisering op basis van gevoelige of beschermde eigenschappen of kenmerken, of op basis van wat uit die eigenschappen of kenmerken wordt afgeleid.
- ☐ Emotieherkenning.

De volgende categorieën zullen naar alle waarschijnlijkheid nooit van toepassing zijn binnen NOC*NSF, maar voor de volledigheid nemen we ze wel hieronder op.

Onderwijs en beroepsopleiding

- ☐ Het bepalen van toegang of toelating tot of het toewijzen van natuurlijke personen aan instellingen voor onderwijs.
- ☐ Beoordelen van het passende onderwijsniveau dat een persoon zal ontvangen of waartoe hij toegang zal hebben.
- ☐ Monitoren en detecteren van ongeoorloofd gedrag van studenten tijdens toetsen.

Essentiële particuliere en publieke diensten en uitkeringen

- ☐ Het door of namens overheidsinstanties gebruiken om te beoordelen of natuurlijke personen in aanmerking komen voor essentiële overheidsuitkeringen en -diensten, waaronder gezondheidsdiensten, of om dergelijke uitkeringen en diensten te verlenen, te beperken, in te trekken of terug te vorderen.
- ☐ Beoordelen van de kredietwaardigheid van natuurlijke personen of voor het vaststellen van hun krediet score, met uitzondering van AI-systemen die gebruikt worden om financiële fraude op te sporen.
- ☐ Risicobeoordeling en prijsstelling met betrekking tot natuurlijke personen in het geval van levens en ziektekostenverzekeringen.
- ☐ Systemen die bedoeld zijn om noodoproepen van natuurlijke personen te evalueren en te classificeren of om te worden gebruikt voor het inzetten of het bepalen van prioriteiten voor de inzet van hulpdiensten, onder meer van politie, brandweer en ambulance, alsook van systemen voor de triage van patiënten die dringend medische zorg behoeven.

Rechtshandhaving

- ☐ Risico beoordelen dat een natuurlijke persoon het slachtoffer wordt van strafbare feiten.
- ☐ Gebruik als leugendetector of soortgelijke instrumenten.
- ☐ Beoordelen van de betrouwbaarheid van bewijsmateriaal tijdens het onderzoek naar of de vervolging van strafbare feiten.
- ☐ Beoordelen hoe groot het risico is dat een natuurlijke persoon (opnieuw) een strafbaar feit zal plegen, of om persoonlijkheidskenmerken en eigenschappen of eerder crimineel gedrag van natuurlijke personen of groepen te beoordelen.
- ☐ Natuurlijke personen profileren tijdens het opsporen, onderzoeken of vervolgen van strafbare feiten.

Migratie-, asiel- en grenstoezicht

- ☐ Gebruik als leugendetector of soortgelijke instrumenten.
- ☐ Risico's beoordelen, waaronder een veiligheidsrisico, een risico op illegale migratie of een gezondheidsrisico, uitgaat van een natuurlijke persoon die voornemens is het grondgebied van een lidstaat te betreden of dat heeft gedaan.
- ☐ Behandeling van aanvragen voor asiel, visa of verblijfsvergunningen en bij de behandeling van aanverwante klachten in verband met het al dan niet in aanmerking komen van de natuurlijke personen die een aanvraag voor een status indienen, met inbegrip van hieraan gerelateerde beoordelingen van de betrouwbaarheid van bewijsmateriaal.
- ☐ Het opsporen, herkennen of identificeren van natuurlijke personen, met uitzondering van de verificatie van reisdocumenten.

Rechtsbedeling en democratische processen

- ☐ Ondersteunen bij het onderzoeken en uitleggen van feiten of de wet en bij de toepassing van het recht op een concrete reeks feiten of om te worden gebruikt op soortgelijke wijze in het kader van alternatieve geschillenbeslechting.
- ☐ Het beïnvloeden van de uitslag van een verkiezing of referendum of van het stemgedrag van natuurlijke personen bij de uitoefening van hun stemrecht bij verkiezingen of referenda. Dit geldt niet voor AI-systemen aan de output waarvan natuurlijke personen niet rechtstreeks worden blootgesteld, zoals instrumenten die worden gebruikt om politieke campagnes te organiseren, te optimaliseren of te structureren vanuit administratief of logistiek oogpunt

Kritieke infrastructuur:

☐ Veiligheidscomponent bij het beheer of de exploitatie van kritieke digitale infrastructuur, wegverkeer of bij de levering van water, gas, verwarming en elektriciteit.

Heb je ergens in stap 4 een vinkje aangekruist? → Het systeem is mogelijk een hoog risico systeem. Ga naar stappen 5 en 6. Zo niet, ga dan verder met invullen van stap 7.

[Voor meer informatie: Artikel 6, lid 2 en bijlage III AI Verordening]

Stap 5: Is een van de volgende uitzonderingen van toepassing op het hoog- risico AI systeem

☐ Het AI systeem is bedoeld om een beperkte procedurele taak uit te voeren. Een voorbeeld van een AI-systeem dat is bedoeld om een beperkte procedurele taak uit te voeren, is een factuurverwerkings-AI. Dit systeem is specifiek ontworpen om inkomende facturen automatisch te verwerken. Het herkent factuurgegevens zoals factuurnummer, bedrag en vervaldatum, vergelijkt deze met bestaande orders in het ERP-systeem en stuurt ze ter goedkeuring door naar de juiste afdeling. Dit AI-systeem heeft een duidelijke, afgebakende taak en opereert binnen vaste regels en parameters, zonder zelflerende of autonome besluitvorming buiten dit proces.

☐ Het AI-systeem is bedoeld om het resultaat van een eerder voltooide menselijke activiteit te verbeteren. Een voorbeeld van een AI-systeem dat bedoeld is om het resultaat van een eerder voltooide menselijke activiteit te verbeteren, is een AI-gestuurde beeldoptimalisatietool, zoals Adobe Enhance of Topaz AI. Dit systeem analyseert door mensen gemaakte foto's of video's en past verbeteringen toe, zoals ruisreductie, kleurcorrectie en verscherping van details. De AI verfijnt en optimaliseert de oorspronkelijke beelden zonder de creatieve intentie van de maker volledig te vervangen, waardoor de uiteindelijke visuele kwaliteit wordt verbeterd.

☐ Het AI-systeem is bedoeld om besluitvormingspatronen of afwijkingen van eerdere besluitvormingspatronen op te sporen en is niet bedoeld om de eerder voltooide menselijke beoordeling zonder behoorlijke menselijke toetsing te vervangen of te beïnvloeden.

☐ Het AI-systeem is bedoeld om een voorbereidende taak uit te voeren voor een relevante beoordeling. Een voorbeeld van een AI-systeem dat een voorbereidende taak uitvoert voor een relevante beoordeling, is een spellingscontrole in juridische documenten. Dit systeem scant juridische teksten op spel- en typefouten voordat een jurist of advocaat de definitieve beoordeling en goedkeuring doet. Het AI-systeem markeert mogelijke fouten of inconsistenties, zodat de jurist efficiënter kan werken en zich kan focussen op de inhoudelijke en juridische juistheid van het document.

Heb je bij deze stap géén vinkjes ingevuld, dan is er geen uitzondering van toepassing en is het AI-systeem hoogstwaarschijnlijk een hoog risico systeem. Neem zo spoedig mogelijk contact op met de AI Officer.

[Zie voor meer informatie: Artikel 6, lid 3 en 4 AI Verordening]

Stap 6: Voert het AI-systeem desalniettemin profilering uit?

☐ Het AI-systeem voert profilering van natuurlijke personen uit. Voorbeelden hiervan zijn als volgt:

- Een AI-recruitmenttool beoordeelt sollicitanten door hun CV, motivatiebrief en online gedrag te analyseren. Het systeem kan bijvoorbeeld patronen herkennen in eerdere werkervaringen en opleidingsachtergrond en deze gebruiken om kandidaten te rangschikken op geschiktheid voor een bepaalde functie.
- Een AI-marketingplatform segmenteert klanten op basis van hun online koopgedrag en interesses, waardoor bedrijven gerichte advertenties kunnen tonen. Door eerdere aankopen en zoekgedrag te analyseren, kan het systeem voorspellen welke producten of diensten iemand waarschijnlijk interessant vindt.
- Een fraude-detectiesysteem bij verzekeringen onderzoekt claimedrag en eerdere schademeldingen om risicoprofielen van klanten op te stellen. Op basis van afwijkende patronen in claims kan het systeem potentiële fraude identificeren en verzekeraars helpen om verdachte gevallen nader te onderzoeken.
- Een AI-gestuurd kredietwaardigheidssysteem analyseert financiële gegevens en de transactiesgeschiedenis van individuen om hun kredietscore te bepalen. Dit systeem beoordeelt het betalingsgedrag, openstaande schulden en andere financiële factoren om een risico-inschatting te maken voor kredietverstrekkers.

Heb je bij deze stap wel het vinkje ingevuld, dan is het AI-systeem hoogstwaarschijnlijk een hoog risico systeem. Neem zo spoedig mogelijk contact op met de AI Officer.

[Zie voor meer informatie: Artikel 6, lid 3 en 4 AI Verordening]

Stap 7: Beoordeel of jouw AI-systeem onder een van deze categorieën valt

1. Is het AI-systeem bedoeld voor interactie met natuurlijke personen?

☐ Ja, het AI-systeem is ontworpen om direct met mensen te communiceren.

- Voorbeelden:
 - Een virtuele assistent of chatbot zoals ChatGPT, Microsoft Copilot of Google Bard.
 - Een AI-gestuurd klantenservice-systeem dat vragen van gebruikers beantwoordt.
 - Een stemassistent zoals Alexa of Siri.

2. Wordt het AI-systeem gebruikt voor emotieherkenning of biometrische categorisatie?

☐ Ja, het AI-systeem analyseert emoties of categoriseert mensen op basis van biometrische kenmerken.

- Voorbeelden:
 - Een AI die gezichtsuitdrukkingen analyseert om emoties te detecteren.
 - Een wervingsplatform dat sollicitanten beoordeelt op basis van stem- of gezichtsherkenning.
 - Een marketingtool die de stemming van klanten analyseert op basis van hun spraak of gezichtsuitdrukking.

3. Genereert of bewerkt het AI-systeem beeld-, audio- of videomateriaal dat voor mensen als authentiek kan worden gezien ("deepfake")?

☐ Ja, het AI-systeem maakt of bewerkt media die sterk lijken op echte personen, objecten, plaatsen of gebeurtenissen.

- Voorbeelden:
 - Alle generatieve AI zoals ChatGPT, Microsoft Copilot of DALL·E die overtuigende afbeeldingen, teksten of audio kan genereren.

- Een AI die realistische nepvideo's maakt van bekende personen.
- Een stemkloner die iemands stem nabootst en kan laten zeggen wat de gebruiker invoert.

*Heb je ergens hierboven met ja geantwoord? → Het systeem vormt mogelijk een risico op misleiding. NOC*NSF moet dan voldoen aan transparantieplichtingen. Dit wordt ook wel aangeduid als systeem **met een beperkt risico**. Overleg met de AI Officer welke maatregelen er precies genomen dienen te worden.*

[Voor meer informatie: Artikel 50 AI Verordening]

Stap 8: Bepaal de rol van NOC*NSF tot het AI-systeem.

Welke rollen zijn er?

- Provider → Je ontwikkelt of laat een AI-systeem ontwikkelen en biedt het aan derden aan.
- Deployer → Je gebruikt een AI-systeem binnen jouw organisatie of integreert het zonder wijzigingen.
- Downstream Provider → Je integreert een bestaand AI-model in een nieuw AI-systeem en biedt het aan.
- Importer → Je brengt een AI-systeem op de EU-markt dat van buiten de EU afkomstig is.
- Distributor → Je verkoopt of verspreidt een AI-systeem binnen de EU zonder dat je het zelf importeert of ontwikkelt.

Selecteer hieronder één optie per vraag om je rol te bepalen.

1. Ontwikkel je zelf een AI-systeem of laat je het in jouw naam ontwikkelen?

☐ Ja, ik ontwikkel een AI-systeem of laat er een ontwikkelen in mijn naam (bijv. ik train een model, fine-tune een bestaand model of ontwikkel het vanaf nul).
☞ Provider → Je bent klaar.

☐ Nee, ik ontwikkel het niet zelf. → Ga door naar stap 2.

2. Gebruik je een AI-systeem dat je zelf hebt ontwikkeld of laten ontwikkelen?

☐ Ja, ik gebruik het AI-systeem dat ik (of iemand in mijn naam) heb ontwikkeld.
☞ Deployer → Je bent klaar.

☐ Nee, ik bied het alleen aan derden aan.

☞ Provider → Je bent klaar.

☐ Nee, ik heb het AI-systeem niet zelf ontwikkeld. → Ga door naar stap 3.

3. Gebruik je een AI-systeem zonder wijzigingen en bied je het niet aan derden aan?

☐ Ja, ik gebruik een kant-en-klaar AI-systeem zonder wijzigingen.

☞ Deployer → Je bent klaar.

☐ Nee, ik pas het AI-systeem wel aan voordat ik het gebruik. → Ga door naar stap 4.

Wat wordt bedoeld met een wijziging in deze stap?

Een wijziging betekent hier dat je de werking van het AI-systeem verandert, bijvoorbeeld door:

- Substantiële wijzigingen:
 - Aanpassen van de beslissingslogica van het systeem (bijv. veranderen hoe het systeem output genereert of hoe het keuzes maakt).
 - Toevoegen of wijzigen van risico-beperkende maatregelen (bijv. het inbouwen van extra validatiestappen of filters).
 - Veranderen van hoe het AI-systeem data verwerkt, waardoor de betrouwbaarheid of risico's veranderen.
- Niet-substantiële wijzigingen:
 - Veranderen van de gebruikersinterface (UI) zonder impact op de AI-functionaliteit.
 - Aanpassen van instellingen of drempelwaarden zonder impact op risico's of prestaties.

4. Gebruik je Retrieval-Augmented Generation (RAG) of integreer je een AI-systeem zonder het AI-model zelf te wijzigen?

☒ Ja, ik gebruik RAG of integreer een AI-systeem met externe bronnen, zonder het AI-model zelf te wijzigen.

 Deployer → Je bent klaar.

☐ Nee, ik pas het AI-model zelf aan. → Ga door naar stap 5.

Wat wordt bedoeld met een wijziging in deze stap?

- Geen wijziging (Deployer) → Je gebruikt een bestaand AI-systeem en combineert het met externe databronnen (zoals een database of kennisbank via RAG), zonder het onderliggende AI-model zelf te veranderen.
- Wel wijziging (door naar stap 5) → Je past het AI-model zelf aan, bijvoorbeeld door:
 - Het fine-tunen van een bestaand AI-model met extra trainingsdata.
 - Het hertrainen van een AI-model op nieuwe datasets.
 - Het direct aanpassen van de neurale netwerken of parameters van het model.

5. Pas je een bestaand AI-model aan voordat je het aanbiedt aan anderen?

☒ Ja, ik fine-tune of wijzig een bestaand AI-model en bied het aan derden aan. (bijv. ik pas een bestaand AI-model aan en breng het opnieuw op de markt binnen een AI-systeem).

 Downstream Provider → Je bent klaar.

☐ Nee, ik integreer een bestaand AI-model in een AI-systeem zonder het model zelf te wijzigen. → Je bent een Deployer.

Wat wordt bedoeld met een wijziging in deze stap?

- Elke wijziging, hoe klein ook, maakt je een Downstream Provider.
- Voorbeelden van wijzigingen:
 - Fine-tunen van een bestaand model met eigen bedrijfsdata.
 - Toevoegen van extra lagen aan een neuraal netwerk.

- Wijziging van de trainingsmethodiek of dataset.
- Substantiële wijzigingen:
 - Wijzigen van de architectuur van een AI-model.
 - Het opnieuw trainen van een model met een totaal andere dataset.

◆ Regulatorische impact? → Ook kleine wijzigingen kunnen extra nalevingsverplichtingen met zich meebrengen, zoals documentatie-eisen en risicobeoordelingen onder de AI Act.

6. Breng je een AI-systeem op de EU-markt dat van buiten de EU afkomstig is?

☐ Ja, ik importeer een AI-systeem uit een land buiten de EU en breng het op de markt binnen de EU.

📦 Importer → Je bent klaar.

☐ Nee, ik importeer geen AI-systemen van buiten de EU. → Ga door naar stap 7.

7. Verkoop of verspreid je AI-systemen binnen de EU zonder dat je ze zelf importeert of ontwikkelt?

☐ Ja, ik verkoop of verspreid een AI-systeem binnen de EU dat door een andere partij is ontwikkeld of geïmporteerd.

📦 Distributor → Je bent klaar.

☐ Nee, geen van bovenstaande opties is op mij van toepassing.

Stap 9. Concludeer of er laag/geen risico is.

1 Controleer de eerdere risico-inschatting

✓ Actie:

- Kijk terug naar de voorgaande stappen waarin werd bepaald of het AI-systeem onder verboden, hoog risico of beperkt risico valt.
- Als geen van deze categorieën van toepassing was, dan valt het AI-systeem onder laag/geen risico volgens de AI Verordening.

2 Bevestig dat het AI-systeem als laag risico wordt beschouwd onder de AI Verordening

✓ Actie:

- Als het AI-systeem geen transparantieplichtingen heeft en niet onder specifieke AI Verordening-regels valt, dan is het een laag/geen risico AI-systeem.

En als laatste een waarschuwing: Een laag risico onder de AI Verordening betekent niet dat er géén risico's zijn in andere wetgeving!

Bijlage 1. Overzicht Verplichtingen op grond van rol NOC*NSF en de classificatie van het door NOC*NSF ingezette AI systeem.

1. Transparantieverplichtingen voor limited risk.

Deze transparantieverplichtingen gaan gelden vanaf augustus 2026

1. Informeer gebruikers dat ze met een AI-systeem interageren

✎ Toepassing: AI-systemen zoals chatbots of virtuele assistenten.

✓ Actie:

Geef een duidelijke melding aan gebruikers dat ze met een AI-systeem communiceren.

Plaats deze melding op een zichtbare plek in de interface (bijv. boven het chatvenster of in de eerste AI-gegenereerde reactie).

◆ Voorbeeld van een melding:

"Let op: Dit gesprek wordt gevoerd met een AI-systeem, niet met een mens."

2. Zorg ervoor dat AI-gegenereerde content als zodanig herkenbaar is

✎ Toepassing: Alle AI-gegenereerde tekst, afbeeldingen, audio en video.

✓ Actie:

Label AI-gegenereerde content duidelijk als kunstmatig gegenereerd.

Dit geldt vooral als de content bedoeld is om het publiek te informeren over zaken van openbaar belang.

◆ Voorbeelden van correcte labeling:

Tekst: Voeg een disclaimer toe zoals "Deze tekst is gegenereerd door een AI-systeem."

Afbeeldingen: Voeg een watermerk of label toe zoals "AI-generated".

Audio/video: Geef in de metadata of in de video een melding zoals "Deze opname bevat AI-gegenereerde elementen."

3. Specifieke eisen voor deepfakes en gemanipuleerde media

✎ Toepassing: AI-gegenereerde of bewerkte audio en video die mensen kan misleiden.

✓ Actie:

Markeer en label deepfakes expliciet als AI-gegenereerd.

Zorg ervoor dat het voor de gebruiker direct duidelijk is dat het geen authentiek materiaal betreft.

◆ Voorbeeld van een melding:

"Deze video is gedeeltelijk/volledig AI-gegenereerd en mag niet als authentiek worden beschouwd."

4. Verantwoordelijkheid van de aanbieder (Provider)

✓ Actie:

Ontwikkelaars en aanbieders van AI-systemen moeten de juiste transparantie-instellingen implementeren.

Controleer of AI-content wordt voorzien van metadata, labels of disclaimers.

Zorg voor een mechanisme waarmee gebruikers eenvoudig feedback kunnen geven over mogelijk misleidende AI-content.

2. Verplichtingen voor high risk AI toepassingen

Artikel 8: Beoordeling en mitigatie van risico's

 Toepassing: AI-systemen met een hoog risico.

☒ Actie: Aanbieders moeten een systematische risicobeoordeling uitvoeren en passende maatregelen nemen om geïdentificeerde risico's te beperken.

 Voorbeeld van mitigatiemaatregelen:

- Het implementeren van veilige ontwerpprincipes.
- Continue monitoring van de AI-prestaties en bijsturing waar nodig.
- Aanpassingen aan datasets en modellen om systemische bias te verminderen.
- Voor aanbieders: Zij moeten de risicobeoordeling documenteren en regelmatig herzien.
- Voor gebruikers: Zij moeten de aanbevelingen van aanbieders opvolgen en de AI-systemen op verantwoorde wijze implementeren.

Artikel 9: Beheer van risico's

 Toepassing: AI-systemen met een hoog risico.

☒ Actie: Aanbieders moeten een continu risicobeheerproces implementeren gedurende de gehele levenscyclus van het AI-systeem.

 Voorbeelden van risicobeheeracties:

- Identificatie van potentiële schade aan gebruikers of derden.
- Opstellen van noodmaatregelen voor incidentrespons.
- Herziening en bijstelling van het AI-systeem op basis van nieuwe risicoanalyses.
- Voor aanbieders: Zij moeten een risicobeheersysteem opstellen en onderhouden.
- Voor gebruikers: Zij moeten toezicht houden op de werking en risico's van het AI-systeem en incidenten rapporteren.

Artikel 10: Data en datagovernance

 Toepassing: AI-systemen met een hoog risico die data gebruiken voor training, validatie en testen.

☒ Actie: Zorg voor representatieve, foutvrije en relevante datasets die voldoen aan strikte datakwaliteitsnormen.

 Belangrijke vereisten:

- Datasets moeten evenwichtig zijn en onnodige bias voorkomen.
- Transparantie in data-oorsprong en verwerkingsmethoden.
- Documenteren van alle datagerelateerde processen.
- Voor aanbieders: Verantwoordelijk voor de kwaliteit en traceerbaarheid van de data.
- Voor gebruikers: Moeten ervoor zorgen dat het systeem met juiste en legitieme data wordt gevoed en dat datasets up-to-date blijven.

Artikel 11: Technische documentatie

🔗 Toepassing: Alle AI-systemen met een hoog risico.

✅ Actie: Documenteer de technische kenmerken en werking van het AI-systeem in detail.

💎 Vereisten voor de documentatie:

- Specificaties van het AI-model en gebruikte algoritmen.
- Informatie over de training en testprocedures.
- Bewijsstukken van conformiteit met AI-regelgeving.
- Voor aanbieders: Verantwoordelijk voor het opstellen en bijhouden van technische documentatie. Voor gebruikers: Moeten zich informeren over de documentatie en zich houden aan de richtlijnen.

Artikel 12: Registratie in een EU-databank

🔗 Toepassing: AI-systemen met een hoog risico.

✅ Actie: AI-systemen met een hoog risico moeten worden geregistreerd in een door de EU beheerde databank.

💎 Belangrijke informatie die geregistreerd moet worden:

- Identiteit van de aanbieder en eventuele gemachtigde.
- Beschrijving van de werking van het AI-systeem.
- Eventuele beperkingen of risico's.
- Voor aanbieders: Moeten zorgen voor correcte en tijdige registratie.
- Voor gebruikers: Moeten controleren of het systeem is geregistreerd voordat ze het in gebruik nemen.

Artikel 13: Transparantie en informatieverstrekking aan gebruiksverantwoordelijken

🔗 Toepassing: AI-systemen met een hoog risico.

✅ Actie: Zorg voor voldoende transparantie in de werking van AI-systemen.

💎 Vereisten:

- Gebruik van begrijpelijke en toegankelijke documentatie.
- Gebruikers moeten de output van het AI-systeem correct kunnen interpreteren.
- Belangrijke beperkingen van het AI-systeem moeten expliciet worden vermeld.
- Voor aanbieders: Zorgen voor heldere en volledige gebruiksinstructies.
- Voor gebruikers: Zich informeren en correct gebruik maken van de AI-technologie.

Artikel 14: Menselijk toezicht

🔗 Toepassing: AI-systemen met een hoog risico.

✅ Actie: Zorg ervoor dat AI-systemen met een hoog risico onder menselijk toezicht staan om risico's voor de gezondheid, veiligheid en grondrechten te beperken.

💎 Belangrijke maatregelen:

- Ontwerp en ontwikkel AI-systemen zodat natuurlijke personen effectief toezicht kunnen houden.

- Voorkom situaties waarin de AI zelfstandig kritieke beslissingen neemt zonder menselijke controle.
- Gebruik van interfaces en tools die toezicht en correctie mogelijk maken.
- Voor aanbieders: Verplicht om menselijk toezicht te integreren in het ontwerp en gebruiksinstructies te voorzien.
- Voor gebruikers: Moeten de juiste menselijke controleprocessen implementeren bij het inzetten van het AI-systeem

Artikel 15: Nauwkeurigheid, robuustheid en cyberbeveiliging

 Toepassing: AI-systemen met een hoog risico.

Vereisten:

- AI-systemen moeten bestand zijn tegen fouten en manipulaties.
- Beveiligingsmaatregelen tegen cyberaanvallen en datavervuiling moeten worden ingebouwd.
- Zelflerende AI moet maatregelen nemen om vertekende output als input (feedback loops) te voorkomen.
- Voor aanbieders: Moeten technische en organisatorische maatregelen treffen om de prestaties en veiligheid te garanderen.
- Voor gebruikers: Moeten de betrouwbaarheid van het systeem verifiëren en zorgen voor veilig gebruik.

Artikel 16: Verplichtingen van aanbieders van AI-systemen met een hoog risico

 Toepassing: AI-systemen met een hoog risico.

 Actie: Aanbieders moeten ervoor zorgen dat hun AI-systemen voldoen aan alle wettelijke vereisten.

Verplichtingen:

- Vermelden van hun naam, handelsmerk en contactgegevens.
- Implementatie van een kwaliteitsbeheersysteem.
- Registratie en CE-markering van AI-systemen.
- Uitvoeren van een conformiteitsbeoordeling
- Voor aanbieders: Zij zijn verantwoordelijk voor naleving en documentatie.
- Voor gebruikers: Moeten zich informeren over conformiteit en registraties controleren.

Artikel 17: Systeem voor kwaliteitsbeheer

 Toepassing: AI-systemen met een hoog risico.

 Actie: Aanbieders moeten een kwaliteitsbeheersysteem implementeren dat de naleving van de AI-verordening waarborgt.

Elementen van het kwaliteitsbeheersysteem:

- Nalevingsstrategie en conformiteitsbeoordelingsprocedures.
- Beheer van wijzigingen aan het AI-systeem.
- Inspecties, tests en valideringsprocedures.
- Systemen en procedures voor databeheer
- Voor aanbieders: Moeten een kwaliteitsmanagementsysteem opstellen en onderhouden.
- Voor gebruikers: Moeten werken binnen de kwaliteitsnormen van de aanbieder.

Artikel 18: Bewaring van documentatie

✎ Toepassing: AI-systemen met een hoog risico.

✓ Actie: Aanbieders moeten bepaalde documentatie minstens 10 jaar bewaren na het op de markt brengen of in gebruik nemen van het AI-systeem.

◇ Documenten die bewaard moeten worden:

- Technische documentatie (artikel 11).
- Documentatie over het kwaliteitsbeheer (artikel 17).
- EU-conformiteitsverklaring (artikel 47)
- Voor aanbieders: Verplicht om deze documenten te bewaren en beschikbaar te stellen aan bevoegde autoriteiten.
- Voor gebruikers: Moeten toegang krijgen tot relevante documentatie indien nodig.

Artikel 19: Automatisch gegenereerde logs

✎ Toepassing: AI-systemen met een hoog risico.

✓ Actie: Aanbieders moeten automatisch gegenereerde logs opslaan en beheren.

◇ Vereisten:

- Logs moeten minstens 6 maanden worden bewaard.
- Financiële instellingen mogen de logs opnemen in hun bestaande documentatieplicht
- Voor aanbieders: Verplicht om loggingmechanismen in te bouwen en logs veilig op te slaan.
- Voor gebruikers: Moeten ervoor zorgen dat ze toegang hebben tot relevante loggegevens voor auditdoeleinden.

Artikel 20: Corrigerende maatregelen en mededelingsverplichting

✎ Toepassing: AI-systemen met een hoog risico.

✓ Actie: Aanbieders moeten onmiddellijk corrigerende maatregelen nemen als zij constateren dat hun AI-systeem niet voldoet aan de AI-verordening.

◇ Belangrijke verplichtingen:

- Als een AI-systeem niet in overeenstemming is, moet het worden aangepast, teruggeroepen of uit de handel worden genomen.
- De aanbieder moet distributeurs en gebruikers informeren over de genomen corrigerende maatregelen.
- Indien het AI-systeem een risico vormt, moeten ook de markttoezichtautoriteiten en, indien van toepassing, de aangemelde instanties worden geïnformeerd
- Voor aanbieders: Verplicht om corrigerende maatregelen onmiddellijk uit te voeren en rapporteren aan relevante partijen.
- Voor gebruikers: Moeten de correcties doorvoeren en, indien nodig, de AI-systemen tijdelijk of permanent stopzetten.

Artikel 21: Samenwerking met bevoegde autoriteiten

✎ Toepassing: AI-systemen met een hoog risico.

✓ Actie: Aanbieders moeten volledige medewerking verlenen aan bevoegde autoriteiten bij onderzoeken en toezicht.

◆ Vereisten:

- Aanbieders moeten op verzoek toegang geven tot technische documentatie en logs.
- Alle verstrekte informatie moet in een officiële EU-taal beschikbaar zijn.
- Bevoegde autoriteiten mogen vertrouwelijke informatie verwerken conform artikel 78
- Voor aanbieders: Moeten meewerken met autoriteiten en volledige documentatie beschikbaar stellen. Voor gebruikers: Moeten relevante informatie beschikbaar houden voor audits.

Artikel 22: Gemachtigden van aanbieders van AI-systemen met een hoog risico

✚ Toepassing: AI-aanbieders buiten de EU die hun AI-systemen in de EU op de markt willen brengen.

✓ Actie: Niet-EU-aanbieders moeten een gemachtigde in de EU aanwijzen.

◆ Taken van de gemachtigde:

- Controleren of de technische documentatie en conformiteitsverklaring aanwezig zijn.
- Contactgegevens van de aanbieder beschikbaar houden voor autoriteiten.
- Samenwerken met autoriteiten bij risicoanalyse en nalevingsprocedures
- Voor aanbieders buiten de EU: Verplicht om een gemachtigde in de EU aan te stellen.
- Voor gebruikers: Geen directe verplichtingen, maar moeten verifiëren of de aanbieder een gemachtigde heeft.

Artikel 23: Verplichtingen van importeurs

✚ Toepassing: Importeurs van AI-systemen met een hoog risico in de EU.

✓ Actie: Importeurs moeten nagaan of AI-systemen aan de wetgeving voldoen voordat ze deze op de markt brengen.

◆ Verplichtingen:

- Controleren of een conformiteitsbeoordeling is uitgevoerd.
- Zorgen dat het systeem een CE-markering heeft en de juiste documentatie bevat.
- Indien een product niet voldoet, de aanbieder op de hoogte stellen en de markttoezichtautoriteiten informeren indien een risico wordt vastgesteld
- Voor importeurs: Verplicht om naleving te controleren en documentatie beschikbaar te houden.
- Voor gebruikers: Moeten verifiëren of de geïmporteerde AI-systemen aan de eisen voldoen.

Artikel 24: Verplichtingen van distributeurs

✚ Toepassing: Distributeurs van AI-systemen met een hoog risico.

✓ Actie: Distributeurs mogen alleen AI-systemen op de markt brengen die voldoen aan de AI-verordening.

◆ Verplichtingen:

- Controleren of de CE-markering en conformiteitsverklaring aanwezig zijn.
- Indien het systeem niet voldoet, mag het niet op de markt worden gebracht totdat het in overeenstemming is gebracht.

- Zorgen dat opslag- en transportomstandigheden de conformiteit niet in gevaar brengen
- Voor distributeurs: Verplicht om naleving te controleren en geen niet-conforme producten te verkopen.
- Voor gebruikers: Moeten nagaan of het AI-systeem voldoet aan de regelgeving.

Artikel 25: Gevallen waarin distributeurs of importeurs als aanbieders worden beschouwd

 Toepassing: Distributeurs en importeurs die wijzigingen aanbrengen in AI-systemen.

 **Actie:** Indien een distributeur of importeur substantiële wijzigingen aanbrengt aan een AI-systeem, wordt deze als aanbieder beschouwd en krijgt hij dezelfde verplichtingen.

 Wat wordt als substantiële wijziging beschouwd?

- Aanpassingen die de prestaties of het beoogde doel van het AI-systeem veranderen.
- Wijzigingen die gevolgen hebben voor de naleving van de wetgeving
- Voor distributeurs en importeurs: Zij worden volledig verantwoordelijk als zij substantiële wijzigingen doorvoeren.
- Voor gebruikers: Moeten verifiëren of hun leverancier de juiste entiteit blijft.

Artikel 26: Verplichtingen van gebruiksverantwoordelijken

 Toepassing: Organisaties en individuen die AI-systemen met een hoog risico inzetten.

 **Actie:** Gebruikers moeten AI-systemen op een correcte en veilige manier gebruiken.

 Verplichtingen:

- AI-systemen alleen inzetten voor hun beoogde doel en volgens instructies van de aanbieder.
- Controleren of het systeem de juiste instellingen behoudt.
- Incidenten of non-conformiteiten melden aan de aanbieder of autoriteiten
- Voor gebruikers: Verplicht om het AI-systeem correct te implementeren en incidenten te melden.

Artikel 27: Register voor AI-systemen met een hoog risico

 Toepassing: AI-systemen met een hoog risico die in de EU worden gebruikt.

 **Actie:** AI-systemen moeten worden geregistreerd in een EU-database.

 Belangrijke vereisten:

- Aanbieders moeten informatie over hun AI-systemen aanleveren aan de EU-database.
- Autoriteiten moeten toegang krijgen tot de registraties om naleving te controleren
- Voor aanbieders: Verplicht om registratie correct en tijdig te voltooien.
- Voor gebruikers: Moeten nagaan of het systeem geregistreerd is alvorens het te gebruiken.

Artikel 40: Geharmoniseerde normen en normalisatieproducten

 Toepassing: AI-systemen met een hoog risico en AI-modellen voor algemene doeleinden.

 **Actie:** AI-systemen die voldoen aan geharmoniseerde normen worden geacht conform te zijn met de vereisten van de AI-verordening.

 Verplichtingen en voordelen:

- AI-systemen die voldoen aan normen die zijn gepubliceerd in het Publicatieblad van de EU, worden automatisch als conform beschouwd.
- De Commissie dient normalisatieverzoeken in en raadpleegt daarbij de AI-board en belanghebbenden.
- Focus op rapportering en documentatie om het energieverbruik en hulpbronnenverbruik te optimaliseren
- Voor aanbieders: Moeten streven naar conformiteit met geharmoniseerde normen voor eenvoudiger naleving.
- Voor gebruikers: Kunnen vertrouwen op normen als indicator van een veilig AI-systeem.

Artikel 41: Gemeenschappelijke specificaties

🔗 Toepassing: AI-systemen met een hoog risico.

✅ Actie: Als er geen geharmoniseerde normen zijn, kunnen AI-systemen voldoen aan door de Commissie vastgestelde gemeenschappelijke specificaties.

◆ Kernpunten:

- Gemeenschappelijke specificaties bieden een alternatieve route naar conformiteit.
- Lidstaten kunnen de Commissie verzoeken een specificatie aan te passen als deze niet aan de wettelijke eisen voldoet
- Voor aanbieders: Moeten voldoen aan deze specificaties als ze geen geharmoniseerde normen volgen.
- Voor gebruikers: Kunnen er zeker van zijn dat systemen die voldoen aan deze specificaties in lijn zijn met de AI-verordening.

Artikel 42: Vermoeden van conformiteit met bepaalde eisen

🔗 Toepassing: AI-systemen met een hoog risico.

✅ Actie: AI-systemen die zijn getest en gecertificeerd onder erkende normen of cyberbeveiligingsregelingen worden als conform beschouwd.

◆ Voordelen:

- Training en testen in een specifieke context verhogen de kans op conformiteit.
- Certificering onder Verordening (EU) 2019/881 biedt extra bewijs van cyberbeveiliging
- Voor aanbieders: Kunnen certificering gebruiken als bewijs van naleving.
- Voor gebruikers: Kunnen vertrouwen op AI-systemen met dergelijke certificaten.

Artikel 43: Conformiteitsbeoordeling

🔗 Toepassing: AI-systemen met een hoog risico.

✅ Actie: Aanbieders moeten een conformiteitsbeoordelingsprocedure doorlopen.

◆ Keuzemogelijkheden:

- Interne controle (bijlage VI).
- Beoordeling door een aangemelde instantie als geen geharmoniseerde normen beschikbaar zijn
- Voor aanbieders: Moeten een geschikte conformiteitsbeoordelingsroute kiezen.
- Voor gebruikers: Kunnen controleren of het AI-systeem correct is beoordeeld.

Artikel 44: Certificaten

🔗 Toepassing: AI-systemen met een hoog risico.

✅ Actie: AI-systemen kunnen certificaten ontvangen die maximaal vijf jaar geldig zijn.

◆ Belangrijke punten:

- Certificaten kunnen worden verlengd op basis van herbeoordeling.
- Niet-conforme systemen kunnen een schorsing of intrekking van hun certificaat krijgen
- Voor aanbieders: Verplicht om een certificaat te behouden voor naleving.
- Voor gebruikers: Kunnen nagaan of het systeem een geldig certificaat heeft.

Artikel 45: Informatieverplichtingen voor aangemelde instanties

🔗 Toepassing: Organisaties die conformiteitsbeoordelingen uitvoeren.

✅ Actie: Aangemelde instanties moeten autoriteiten informeren over certificeringen en niet-conforme systemen.

◆ Verplichtingen:

- Moeten details verstrekken over de uitgevoerde beoordelingen.
- Rapporteren van problemen met aanbieders aan autoriteiten
- Voor aanbieders: Moeten samenwerken met aangemelde instanties.
- Voor gebruikers: Kunnen vertrouwen op rapportages van aangemelde instanties.

Artikel 46: Verplichtingen van nationale autoriteiten en markttoezicht

🔗 Toepassing: Overheidsinstanties die toezicht houden op AI-systemen.

✅ Actie: Lidstaten moeten adequate structuren instellen voor toezicht en handhaving.

◆ Kernpunten:

- Nationale autoriteiten controleren de naleving en handhaven sancties.
- Bevoegde instanties moeten informatie delen met de Commissie en AI-Board
- Voor aanbieders: Moeten medewerking verlenen aan controles.
- Voor gebruikers: Moeten op de hoogte zijn van toezichtprocedures.

Artikel 47: EU-conformiteitsverklaring

🔗 Toepassing: AI-systemen met een hoog risico.

✅ Actie: Aanbieders moeten een EU-conformiteitsverklaring opstellen.

◆ Verplichtingen:

- Bevestigen dat hun AI-systeem voldoet aan de AI-verordening.
- Verklaring moet tien jaar bewaard blijven
- Voor aanbieders: Moeten een conformiteitsverklaring opstellen en bewaren.
- Voor gebruikers: Kunnen deze verklaring opvragen voor verificatie.

Artikel 48: CE-markering

🔗 Toepassing: AI-systemen met een hoog risico.

✓ Actie: AI-systemen moeten een CE-markering hebben voordat ze op de markt worden gebracht.

◆ Kernpunten:

- CE-markering toont aan dat het AI-systeem voldoet aan de regelgeving.
- Moet correct worden aangebracht en vergezeld gaan van de conformiteitsverklaring
- Voor aanbieders: Verplicht om CE-markering toe te passen.
- Voor gebruikers: Moeten de CE-markering controleren voor naleving.

Artikel 49: Registratie van AI-systemen met een hoog risico

✚ Toepassing: AI-systemen met een hoog risico.

✓ Actie: AI-systemen moeten geregistreerd worden in een centrale EU-database.

◆ Verplichtingen:

- Aanbieders moeten registraties uitvoeren vóór het in gebruik nemen.
- Informatie over het AI-systeem moet beschikbaar zijn voor autoriteiten
- Voor aanbieders: Verplicht om AI-systemen correct te registreren.
- Voor gebruikers: Moeten nagaan of een AI-systeem geregistreerd is alvorens het te gebruiken.

Artikel 72: Monitoring na het in de handel brengen

✚ Toepassing: AI-systemen met een hoog risico.

✓ Actie: Aanbieders moeten een systeem voor monitoring na het in de handel brengen vaststellen en documenteren.

◆ Belangrijke verplichtingen:

- Continue verzameling, documentatie en analyse van relevante gegevens over prestaties en risico's van het AI-systeem.
- Plan voor monitoring na het in de handel brengen als onderdeel van de technische documentatie.
- In sommige gevallen monitoring van de interactie met andere AI-systemen
- Voor aanbieders: Verplicht om monitoring na marktintroductie uit te voeren.
- Voor gebruikers: Moeten relevante gegevens verstrekken voor monitoringdoeleinden.

Artikel 73: Melding van ernstige incidenten

✚ Toepassing: AI-systemen met een hoog risico die in de EU op de markt zijn gebracht.

✓ Actie: Aanbieders en gebruikers moeten ernstige incidenten rapporteren aan de bevoegde markttoezichtautoriteiten.

◆ Verplichtingen:

- Melding binnen 15 dagen na het vaststellen van een verband tussen het AI-systeem en een ernstig incident.
- Directe melding bij een wijdverspreide inbreuk of een incident met dodelijke afloop.

Colofon

Samenstelling

Rol	Naam	Functie	E-mail
Opdrachtgever	Jan-Joost Reyn	Informatiemanager	jan-joost.reyn@nocnsf.nl
Auteur	Marianne de Feijter	Privacy Officer	Marianne.defeijter@nocnsf.nl

Arnhem, 26-03-2025