Implementatie
AI-verordening

Veelgestelde vragen Generatieve AI compliance

Wat is dit document?

Dit document heeft als doel antwoord te geven op de meest gestelde vragen rond Generatieve AI compliance in de zin van de AI-verordening. Dit document geeft geen volledig overzicht van alle vereisten uit de AI-verordening.

De vragen zijn opgehaald in de interdepartementale werkgroep 'Rijksbrede Implementatie AI-verordening' en een workshop met Rijksoverheidsorganisaties. Er is gekozen om geen uitgebreid document te schrijven waarin de hele AI-verordening wordt uitgelegd. In plaats daarvan beantwoordt dit document alleen de vragen die leven bij organisaties die al bezig zijn met het implementeren of ontwikkelen van Generatieve AI toepassingen.

Kan ik 100% op dit document vertrouwen?

Hoewel deze informatie zorgvuldig is opgesteld kunnen er bepaalde nuances zijn verloren, gebruik deze handreiking daarom altijd samen met de officiële tekst van de AI-verordening.

De interpretatie van definities en bepalingen in de AI-verordening ontwikkelt zich nog, het is daarom waarschijnlijk dat een deel van de in dit document gegeven informatie in de loop van de tijd niet meer volledig of actueel is. De Europese Commissie heeft een richtsnoer gepubliceerd over de toepassing van het concept AI-systeem.

De informatie in dit document dient als leidraad. Andere wet- en regelgeving is ook van kracht. Zoals de BIO 2.0. en de AVG. De AVG is van toepassing als (bij ontwikkelen van) het AI-systeem de persoonsgegevens worden verwerkt. Neem altijd contact op met een juridisch adviseur om belangrijke informatie of besluiten op basis van deze informatie te controleren.

CIO Rijk zal eventuele hiaten, voortschrijdend inzicht, guidance van toezichthouders verwerken in een geüpdatete versie en deze via dezelfde kanalen verspreiden.

Wie heeft dit document gemaakt?

Dit document is ontwikkeld door CIO Rijk met adviseurs van het RijksICT Gilde en de interdepartementale werkgroep 'Rijksbrede implementatie AI-verordening' in opdracht van de CDO-raad.

- Joas van Ham (RijksICT Gilde)
- Nout van Deijck (RijksICT Gilde)
- Isabel van Vledder (RijksICT Gilde)
- Lynda la Paine (Privacy team CIO Rijk BZK)
- Martha Romkes (voormalig CIO Rijk BZK)
- Ouren Kuiper (CIO Rijk en digitaliseringsbeleid BZK)

Speciale dank aan Maria Craane (Considerati) de leden van de CDO-raad, de interdepartementale werkgroep, en collega's die hebben bijgedragen aan de totstandkoming van dit document.

Waar kan ik terecht met vragen of feedback?

Voor feedback, vragen of opmerkingen mail: ai-verordening@minbzk.nl

Versie: 1.0 (maart 2026)
Cover: Jamillah Knowles & Digit / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

Inhoudsopgave

Leeswijzer

De vragen in dit document zijn ingedeeld in zes thematische delen:

1. 1. Introductie AI-verordening;
2. 2. De risico-classificatie van Generatieve AI-systemen;
3. 3. De rollen en verantwoordelijkheden van actoren betrokken bij die systemen;
4. 4. De vereisten die voor Generatieve AI gelden;
5. 5. De inkoop en ontwikkeling; en
6. 6. De vraagstukken rond use cases en eindgebruikers.

Omdat gepoogd is de vragen individueel leesbaar te maken, is er hier en daar wat overlap in de beantwoording. Voor meer informatie raadpleeg het algoritmekader.

Informatie uit de AI-verordening is in dit document zo simpel mogelijk beschreven. Betrek altijd een jurist of expert voordat je start met het gebruik van een AI-systeem.

Per onderdeel wordt verwezen naar hulpmiddelen en meer informatie. Soms is dit ander beleid of wetgeving, maar kunnen ook informatieproducten van derden zijn.

We verwijzen naar de artikelen uit de AI-verordening. Dit doen we in de vorm (Art. x(x)). In die gevallen gaat het om de AI-verordening tenzij anders aangegeven.[1]

Introductie AI-verordening

De AI-verordening beschrijft de vereisten die worden gesteld aan AI-systemen en de regels die aanbieders en gebruikers moeten volgen wanneer zij deze systemen ontwikkelen en/of gebruiken (Art. 3(1)). De AI-verordening hanteert hiertoe een risico-gebaseerde benadering waarbij een onderscheid wordt gemaakt tussen verboden AI-systemen (Art. 5), hoog-risico AI-systemen (Art. 6) en overige AI-systemen (Art. 50).

! Let op: Ga je een AI-systeem implementeren in jouw organisatie? Vraag altijd juridisch advies aan een expert.

Wat is een AI-systeem?

Een AI-systeem is een op een machine gebaseerd systeem. Handmatige beslisbomen vallen er dus buiten. Het systeem werkt met een zekere mate van autonomie: de output komt deels tot stand door factoren waar de gebruiker geen directe invloed op heeft. Die output valt doorgaans in drie categorieën: voorspellingen, aanbevelingen of beslissingen. Beslissingen zijn het meest autonoom, voorspellingen het minst.

Een AI-systeem kán aanpassingsvermogen vertonen, bijvoorbeeld door te blijven leren na de inzet, maar dit is geen harde vereiste. Wat een AI-systeem echt onderscheidt van andere systemen is het inferentievermogen: het vermogen om uit ontvangen input zelf af te leiden hoe output gegenereerd moet worden. Dit gaat verder dan het simpelweg verwerken van data; het systeem leert, redeneert of modelleert.

Het systeem werkt naar expliciete of impliciete doelstellingen, en de output kan invloed hebben op zowel fysieke als virtuele omgevingen. Systemen die puur op door mensen vastgestelde regels draaien, vallen buiten de definitie.

Wat is Generatieve AI?

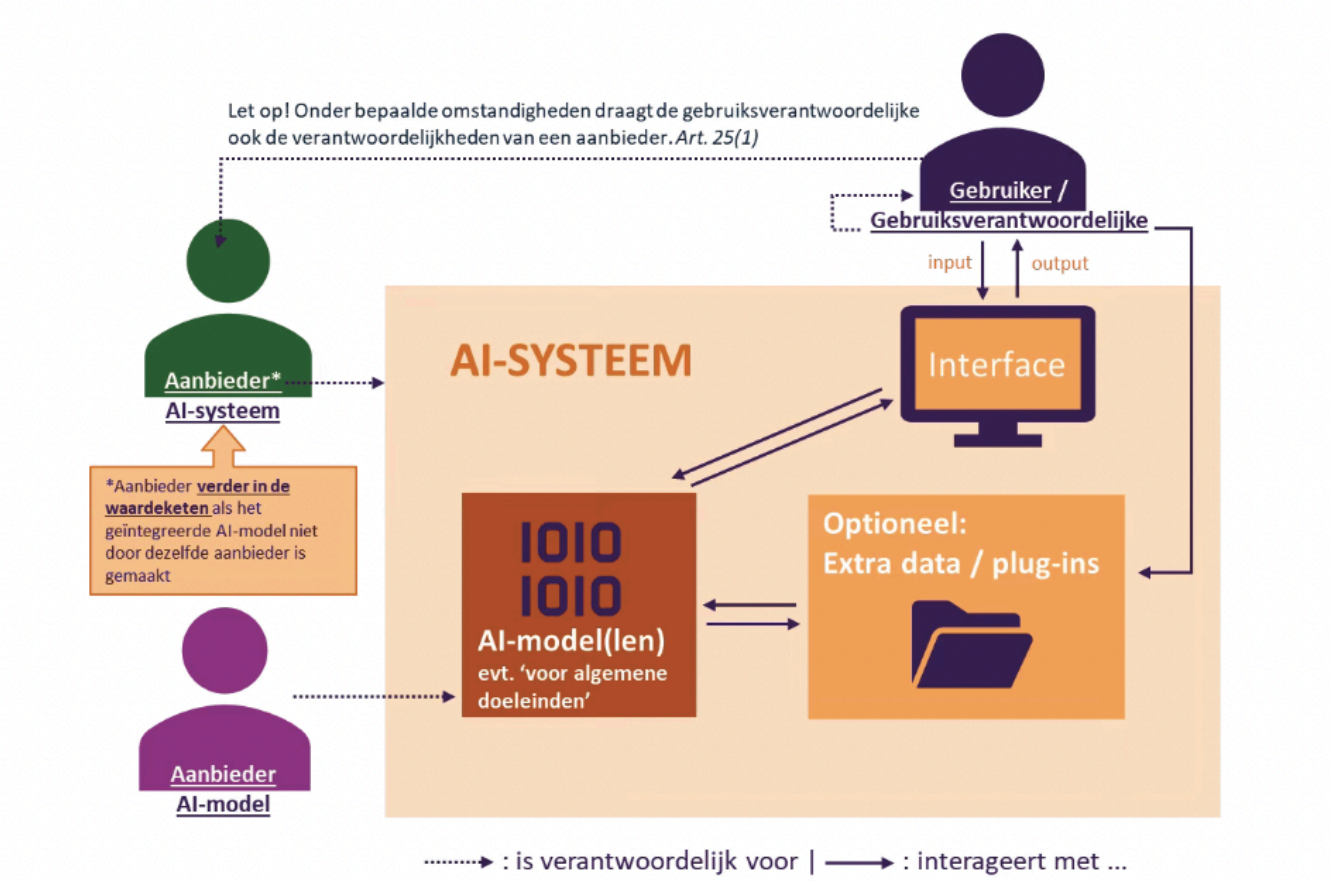
Generatieve AI heeft als voornaamste kenmerk dat ze nieuwe inhoud kunnen produceren. Denk aan tekst, afbeeldingen, audio, video of code. De systemen zijn getraind op grote hoeveelheden data en hebben op basis daarvan een model opgebouwd. Op basis van dat model genereren ze output die statistisch plausibel is gegeven de invoer.

In het perspectief van de AI-verordening is het soms verwarrend om over Generatieve AI te spreken omdat een onderscheid gemaakt wordt tussen het model (model voor algemene doeleinden) en het AI-systeem. Bijvoorbeeld: het AI-systeem ChatGPT, kan gebruik maken van verschillende modellen (gpt-5.4, gpt-5.4-mini, etc.). De verordening stelt eisen op voor zowel de aanbieder van modellen en systemen, als de gebruiksverantwoordelijken daarvan.

[1] De AI-verordening is te raadplegen via: https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=OJ:L_202401689.

Welke rollen kent de AI-verordening?

De AI-verordening stelt andere verplichtingen afhankelijk van de rol die een organisatie heeft bij het AI-systeem. Onderstaande afbeelding en tabel geven een overzicht van de meest voorkomende rollen en hoe deze zich tot elkaar en (onderdelen van) het AI-systeem verhouden.



Aanbieder: een natuurlijke of rechtspersoon, overheidsinstantie, agentschap of ander orgaan die/dat een AI-systeem of een AI-model voor algemene doeleinden ontwikkelt of laat ontwikkelen en dat systeem of model in de handel brengt of het AI-systeem in gebruik stelt onder de eigen naam of merk, al dan niet tegen betaling (Art. 3(3)).

Gebruiksverantwoordelijke: een natuurlijke of rechtspersoon, overheidsinstantie, agentschap of ander orgaan die/dat een AI-systeem onder eigen verantwoordelijkheid gebruikt, tenzij het AI-systeem wordt gebruikt in het kader van een persoonlijke niet-beroepsactiviteit (Art. 3(4))

AI-systeem: een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan aanpassingsvermogen kan vertonen, en dat, voor expliciete of impliciete doelstellingen, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen. (Art. 3(1))

Aanbieder verder in de AI-waardeketen: een aanbieder van een AI-systeem, met inbegrip van een AI-systeem voor algemene doeleinden, waarin een AI-model is geïntegreerd, ongeacht of het AI-model door hemzelf wordt verstrekt en verticaal geïntegreerd is of door een andere entiteit wordt aangeboden op basis van contractuele betrekkingen. (Art. 3(68))

AI-model voor algemene doeleinden: een AI-model, ook wanneer het is getraind met een grote hoeveelheid data met behulp van self-supervision op grote schaal, dat een aanzienlijk algemeen karakter vertoont en in staat is op competente wijze een breed scala aan verschillende taken uit te voeren, ongeacht de wijze waarop het model in de handel wordt gebracht, en dat kan worden geïntegreerd in een verscheidenheid aan systemen verder in de AI-waardeketen of toepassingen verder in de AI-waardeketen, met uitzondering van AI-modellen die worden gebruikt voor onderzoek, ontwikkeling of prototypingactiviteiten alvorens zij in de handel worden gebracht (Art 3(63))

Wanneer is een AI-systeem 'hoog-risico'?

De AI-verordening bepaalt dat een AI-systeem een hoog-risico heeft als:

- Het AI-systeem een product of een veiligheidscomponent van een product is. Voorbeelden hiervan zijn speelgoed, machines, liften en voertuigen. Denk aan een lift die bediend wordt met behulp van een chatbot waar je tegen praat om aan tegen naar welke verdieping je wil gaan.[1]
- Het AI-systeem wordt ingezet voor onder andere het selecteren en beoordelen van kandidaten in een sollicitatieprocedure, emotie herkenning, beoordelen of personen in aanmerking komen voor essentiële overheidsdiensten. Deze toepassingen zijn opgenomen in 7 specifieke use cases beschreven in Annex III van de AI-verordening (Art. 6(2)).

Voor een aanbieder van een AI-systeem met een hoog-risico gelden aanvullende verplichtingen. Waaronder het beoogde doel van het systeem te bepalen en documentatie (onder andere gebruiksinstructies) mee te leveren aan gebruikers.

Gelden er uitzonderingen voor 'hoog-risico' AI-systemen?

De AI-verordening kent uitzonderingen voor AI-systemen die in een hoog-risico toepassingsgebied vallen. Daarmee worden de systemen toch niet als hoog-risico worden aangemerkt (Art. 6(3)). Een AI-systeem valt onder deze uitzondering als het:

- Een beperkte procedurele taak uitvoert, zoals het detecteren van duplicaten in grote datasets.
- Een resultaat van een eerder voltooide menselijke activiteit verbetert, bijvoorbeeld het verbeteren van taalgebruik in een door een mens geschreven tekst.
- Besluitvormingspatronen of afwijkingen in eerdere patronen controleert zonder het besluit te vervangen of te beïnvloeden.
- Een voorbereidende taak uitvoert voor een beoordeling die relevant is voor een van de hoog-risico toepassingsgebieden uit Annex III, zoals het vertalen van documenten of het koppelen van gegevens uit verschillende bronnen.

Het gaat dus om AI-systemen die puur ondersteunend zijn en geen invloed hebben op de uiteindelijke uitkomsten. Denk aan het pseudonimiseren van Cv's in een selectieprocedure.

Aanbieders van AI-systemen die een beroep willen doen op een uitzonderingsgrond voor AI-systemen met een hoog-risico, moeten deze keuze rechtvaardigen voor het systeem op de markt gebracht kan worden (Art. 6(3-4)). Deze aanbieder moet documenteren waarom het AI-systeem niet als hoog-risico geclassificeerd wordt. Ook moet de aanbieder zichzelf en het systeem registreren in een EU-databank.[2]

Hoog-risico generatieve AI door onbedoeld en/of ongewenst gebruik

Generatieve AI-systemen zijn uniek omdat ze in de praktijk eenvoudiger gebruikt *kunnen* worden voor use cases die niet zijn bedoeld door de aanbieder en gebruiksverantwoordelijke. Bijvoorbeeld, een eindgebruiker kan een systeem dat bedoeld is om reacties op sollicitanten op te stellen (geen hoog-risico toepassingsgebied) (on)bedoeld gebruiken om ook een oordeel over de kandidaat te laten genereren (hoog-risico toepassingsgebied).

Als een Generatieve AI-systeem onbedoeld wordt ingezet in een hoog-risico situatie, en er geldt geen uitzondering, dan kan de betrokken partij op grond van Art. 25(1) als aanbieder van het systeem worden aangemerkt. Dat kan gaan om de gebruiksverantwoordelijke, maar ook om een distributeur, importeur of een andere partij die betrokken is. Dit is belangrijk, omdat een aanbieder meer wettelijke verplichtingen heeft. Voor gebruiksverantwoordelijke kan dit extra risico's met zich meebrengen. In het hoofdstuk over Rollen en verantwoordelijkheden pagina 10 gaan we hier verder op in.

Er zijn verschillende maatregelen die genomen kunne worden om te voorkomen of te herkennen het Generatieve AI-systeem niet wordt toegepast voor een onbedoeld en/of ongewenst doel. Zoals duidelijke instructies en training van eindgebruikers van het AI-systeem. Meer maatregelen worden toegelicht in het hoofdstuk Use cases en gebruik op pagina 21

Is de inzet van Generatieve AI bij programmeren een hoog-risico toepassing?

Het gebruik van Generatieve AI bij coderen is niet per definitie hoog-risico. Het hangt vooral af van waardoor de gemaakte code wordt gebruikt. Gaat de code gebruikt worden in een toepassing die onder een van de hoog-risico categorieën valt? Dan valt deze functie onder de hoog-risico verplichtingen zodra de gegenereerde code operationeel is in een systeem met hoog-risico.

De uitzonderingsgronden kunnen van toepassing zijn bij het gebruik voor het schrijven van code. Het gebruik voor het reviewen of testen van code kan bijvoorbeeld vallen onder het verbeteren van bestaande menselijke output of het uitvoeren van een voorbereidende taak.

Het is dus belangrijk om na te gaan hoe en waar de geschreven code gebruikt gaat worden en of dit in een van de hoog-risico categorieën valt zoals hierboven beschreven. Belangrijk is om te bepalen welke rol Generatieve AI precies heeft gespeeld bij het creëren van de code. Dit helpt bij het bepalen of het AI-systeem onder een van de uitzonderingen valt.

Hoe bepaal ik of een AI-systeem een hoog-risico systeem is?

Er zijn verschillende hulpmiddelen die kunnen helpen om te bepalen of een AI-systeem een hoog-risico systeem is. Bijvoorbeeld de Beslishulp van het Algoritmekader en de Compliance Checker van de AI Act Service Desk van de Europese Commissie (zie ook het kopje hulpmiddelen).

[1] Deze AI-systemen volgen uit Art. 6(1) en Annex I.
[2] De EU-databank is beschreven in Annex VIII afdeling B (Art. 49(2)).

Let wel, deze hulpmiddelen bieden geen juridische zekerheid. Het wordt aangeraden om altijd juridisch advies in te winnen van een expert. Op het moment van het schrijven van deze antwoorden op veelgestelde vragen zijn er voor de AI-verordening nog geen verplichte interne procedures binnen de Rijksoverheid. Deze zal dus je als organisatie zelf moeten bedenken en inrichten. In 2026 zal de Europese Commissie richtlijnen publiceren over de praktische uitvoering van de classificatie van AI-systemen met een hoog-risico (Art. 6(5)). Dit zal helpen met het bepalen of jouw AI-systeem onder de hoog-risico categorie valt.

Sinds de zomer van 2025 is het al wel mogelijk om vragen over de implementatie van de AI-verordening in te dienen bij het AI-bureau via de eerdergenoemde AI Act Service Desk. Het is ook mogelijk om vragen hierover te sturen naar de AI-verordening inbox van de Rijksoverheid via AI-verordening@minbzk.nl.

Voor aanbieders van AI-systemen zijn de AI-testomgevingen (*regulatory sandboxes*) ook nog interessant die vanaf augustus 2026 operationeel moeten zijn (Art. 57). Binnen deze omgevingen bieden toezichthouders ondersteuning aan aanbieders van AI-systemen die tijdens de ontwikkeling vragen hebben over hoe zij aan de AI-verordening kunnen voldoen, zodat zij hun product in overeenstemming met de regels op de markt kunnen brengen. Hieronder worden de vormvoorstellen van de AP en RDI hierover gelinkt.

Is VLAM-chat een hoog- of laag-risico systeem?

VLAM-chat is een chatbot ontwikkeld door SSC-ICT voor algemeen gebruik in niet hoog-risico use cases. In principe is VLAM-chat dus niet bedoeld als hoog-risico AI-systeem. Maar dit is afhankelijk van hoe de organisaties VLAM-chat gaan inzetten.

VLAM-chat is niet ontworpen voor hoog-risico use cases en niet geschikt voor een van de uitzonderingen voor hoog-risico systemen.[1] De ministeries die VLAM-chat van SSC-ICT afnemen zijn verantwoordelijkheid om voorkomen dat eindgebruikers het systeem voor een hoog-risico situatie gaan gebruiken. Wordt het systeem wel in hoog-risico situatie gebruikt, dan gelden er aanvullende wettelijke verplichtingen voor dat afnemende ministerie. Deze wordt dan namelijk gezien als aanbieder van het systeem.

Bestaande hulpmiddelen

- De handleiding identificatie en classificatie AI-systemen geeft een uitgebreide instructie voor de classificatie van AI-systemen.
- De Beslishulp AI-verordening helpt bij het bepalen of jouw systeem onder de AI-verordening valt en welke risicoclassificatie het heeft.
- EU AI Act Compliance Checker is een tool om de verplichtingen van de AI-verordening in relatie tot jouw systeem of model te verhelderen.
- De AI Act Service Desk, hier kan je vragen stellen aan het AI-bureau over de implementatie van de AI-verordening.
- De Gids AI-Verordening (EZK) geeft op pagina 6-7 een duidelijk overzicht van hoog-risico use cases, op pagina 8 de uitzonderingen.
- Het Algoritmekader, geeft een overzicht van vereisten voor aanbieders en gebruiksverantwoordelijken (overzicht vereisten).

Meer informatie en gerelateerd

- De Autoriteit Persoonsgegevens over de regulatory sandbox.
- De Rijksdienst voor Digitale Infrastructuur over de regulatory sandbox.

[1] De uitzonderingen uit Art. 6(3) en toegelicht in Wanneer is een AI-systeem 'hoog-risico'?

Risicoclassificatie Generatieve AI

In de voorgaande vragen hebben we gekeken naar wanneer een systeem als hoog-risico AI-systeem classificeert. In deze vragen passen we dit toe op Generatieve AI.

Welke eisen zijn er voor een Generatief AI-systeem met een hoog-risico in de AI-verordening?

Generatieve AI-systemen waar AI-modellen voor algemene doeleinden (zoals generatieve AI-modellen) in zijn verwerkt kunnen ook onder de hoog-risico categorie AI-systemen vallen wanneer deze voldoen aan de criteria voor hoog-risico systemen. (Art. 6). Bijvoorbeeld: een organisatie die inkomende documenten analyseert om risico-indicatoren te genereren, automatisch risicoscores toekent aan burgers, en deze gebruikt om extra te controleren of aanvragen af te wijzen of te vertragen. Dan gelden voor zowel aanbieders als gebruiksverantwoordelijken de algemene verplichtingen voor AI-systemen met een hoog-risico. Hieronder wordt een overzicht hiervan gegeven per rol.

De Gids AI-verordening van EZK geeft op pagina 13 t/m 19 extra toelichting per vereiste voor hoog-risico systemen. Het Algoritmekader geeft ook een overzicht van de vereisten met mogelijke maatregelen die getroffen kunnen worden (zie Hulpmiddelen).

In het hoofdstuk Rollen en verantwoordelijkheden op pagina 10 gaan we verder in op de bepaling van rollen, de informatieverplichtingen die aanbieders naar gebruiksverantwoordelijken hebben en wanneer je als gebruiksverantwoordelijke óók de aanbieder van een AI-systeem met een hoog-risico wordt. Voor de algemene vereisten voor Generatieve AI-systemen, zie ook: 'Welke eisen gelden voor niet-hoog-risico Generatieve AI-systemen?'.

Vereisten AI-systemen met een hoog-risico

Aanbieders van hoog-risico AI-systemen moeten voldoen aan eisen uit de AI-verordening (Art. 8-15). Dit zijn:

- Het vaststellen, uitvoeren, documenteren en in stand houden van een systeem voor risicobeheer.
- Maatregelen op het gebied van data en data-governance. Zoals het gebruiken van voldoende representatieve datasets voor training, validatie en testen.
- Het opstellen van technische documentatie.
- Registratie ('logs') bijhouden. Dit is het dusdanig vormgeven van AI-systemen dat gebeurtenissen gedurende de levenscyclus van het systeem automatisch worden geregistreerd.
- Transparantie en informatieverstrekking aan gebruiksverantwoordelijken. Zoals het opstellen van gebruiksinstructies.
- Maatregelen nemen voor menselijk toezicht. Bijvoorbeeld een duidelijke mens-machine interface.
- Het bieden van een passend niveau van nauwkeurigheid, robuustheid en cyberbeveiliging.
- Verdere verplichtingen voor aanbieders volgen uit Art. 16:
- Het laten uitvoeren van een conformiteitsbeoordeling (Art. 43) en het opstellen van een conformiteitsverklaring (Art. 47).
- Kwaliteitsmanagementsysteem (Art. 17) opstellen dat alle aspecten van ontwerp, ontwikkeling, testen en op de markt brengen omvat.
- Zichzelf en het AI-systeem registreren in de EU-databank die in Art. 71 wordt beschreven.

De verplichtingen voor gebruiksverantwoordelijken van AI-systemen met een hoog-risico moeten ervoor zorgen dat de betreffende AI-systemen correct in gebruik worden genomen (zie ook: 'Welke gebruiksinstructie moeten we meegeven bij Generatieve AI-assistenten?'). De gebruiksverantwoordelijken moeten zich aan het volgende houden eisen (Art. 26):

- Het nemen van technische en organisatorische maatregelen om ervoor te zorgen dat het hoog-risico AI-systeem volgens de gebruiksinstructies gebruikt wordt.
- Het aanwijzen van personen die het menselijk toezicht uitvoeren die over de juiste kennis, bekwaamheid en autoriteit beschikken (Art. 14).
- Waarborgen dat de inputdata van het AI-systeem voldoende relevant en representatief is voor het beoogde doel van het systeem, voor zover de gebruiksverantwoordelijke hier controle over heeft.
- De werking van het AI-systeem monitoren op basis van de gebruiksinstructies. Als een gebruiksverantwoordelijke vaststelt dat het AI-systeem een risico vormt volgens Art. 79(1) en daarmee niet voldoet aan de AI-verordening, moeten zij de aanbieder hiervan op de hoogte stellen en onderbreken zij het gebruik van het systeem. Bij incidenten wordt ook eerst de aanbieder op de hoogte gesteld en de betreffende toezichthouders.
- De automatische logs worden voor ten minste zes maanden bewaard.
- De werknemersvertegenwoordiging (OR) en betrokken werknemers informeren voor het AI-systeem op de werkvloer wordt ingezet.
- Als een hoog-risico AI-systeem beslissingen over mensen neemt of als deze met behulp het AI-systeem worden gemaakt, dan moeten deze mensen hierover proactief worden geïnformeerd (Art. 26(11)).
- Als er sprake is van biometrische identificatie achteraf wordt er vooraf een bindende machtiging gevraagd aan een gerechtelijke of administratieve autoriteit.

Overheidsinstanties als gebruiksverantwoordelijken

Overheidsorganen die een AI-systeem met een hoog-risico als gebruikersverantwoordelijken in gebruik willen nemen, hebben een aantal extra verplichtingen:

- De overheidsorganisatie moet zichzelf registreren in de EU-databank (Art. 49 & 71). .Als een hoog-risico AI-systeem niet in deze EU-databank is geregistreerd, mag dit systeem niet in gebruik worden genomen te worden. Ook moet de aanbieder of distributeur hiervan op de hoogte worden gesteld (Art. 26(8).
- De overheidsorganisatie moet voordat het hoog-risico AI-systeem in gebruik wordt genomen, een Fundamental Rights Impact Assessment (FRIA) uit. Een FRIA is een beoordeling van de gevolgen voor grondrechten die het gebruik van het AI-systeem kan opleveren. Bij deze beoordeling wordt bijvoorbeeld gekeken naar de duur van het gebruik en binnen welke processen het systeem gaat worden gebruikt. Je beoordeelt de impact die het gebruik op de grondrechten van mensen of groepen, zoals privacy, gelijke behandeling of vrijheid van meningsuiting. Uit een FRIA kunnen risico's voor de grondrechten volgen. Hierna moeten de overheidsorganisatie maatregelen nemen voor menselijk toezicht en voor het omgaan met de geïdentificeerde risico's. Daarnaast moet de overheidsorganisatie na afronding van de FRIA een melding bij de markttoezichthouder. Deze verplichting geldt niet als er een beroep gedaan kan worden op een uitzondering op basis van openbare veiligheid of bescherming van de gezondheid van personen (Art. 27).

Daarnaast zijn de procedures die in algemeenheid gelden voor IT en IV zaken onverminderd van toepassing. Denk aan de toepassing van het CIO-stelsel (oordelen bij grote projecten, e.d.), maar ook DPIA's en quickscan informatiebeveiliging.

Standaarden

Om te helpen voldoen aan bepaalde verplichtingen uit de AI-verordening wordt er op Europees niveau gewerkt aan technische standaarden waar concrete acties aan verbonden zijn. Deze zijn momenteel nog in ontwikkeling. Zie voor meer informatie: 'Wat kunnen we doen als de standaarden er nog niet zijn?'.

Bestaande hulpmiddelen

- De Gids AI-Verordening (EZK) geeft op pagina 13-19 een overzicht met uitleg van de verplichtingen voor gebruiksverantwoordelijken en aanbieders van zowel hoog-risico AI-systemen als AI-modellen en -systemen voor algemene doeleinden.
- Het Algoritmekader geeft een overzicht van vereisten voor aanbieders en gebruiksverantwoordelijken. Door een AI-verordening profiel te kiezen, wordt er gefilterd op de vereisten die relevant zijn voor jouw rol en type systeem.

Rollen en verantwoordelijkheden

Hoe zijn de verantwoordelijkheden verdeeld bij het ontwikkelen van een Generatieve AI toepassing?

Kort overzicht belangrijke rollen AI-verordening

Voor de overheid zijn de rollen *aanbieder* en *gebruiksverantwoordelijke* uit de AI-verordening het meest relevant.

- Een aanbieder is de organisatie die een AI-systeem of een AI-model voor algemene doeleinden zelf ontwikkelt of laat ontwikkelen en dit onder eigen naam in handel brengt of zelf gebruikt (Art. 3(3)).
- De gebruiksverantwoordelijke is de organisatie die een AI-systeem onder eigen verantwoordelijkheid in gebruik neemt (Art. 3(4)).

De AI-verordening definieert ook de rol *aanbieder verder in de AI-waardeketen*. Dit is een aanbieder van een AI-systeem waar een AI-model in is geïntegreerd dat niet door henzelf is ontwikkeld (Art. 3(68)). Een voorbeeld hiervan is als een organisatie een chatbot voor intern gebruik bouwt en hiervoor een bestaand large language model (LLM) (zoals ChatGPT) van een externe partij als basis neemt.

Voor dit type aanbieder gelden dezelfde verplichtingen als voor een algemene aanbieder van een AI-systeem. De aanbieder van het AI-model dient technische documentatie op te maken (Art. 53(1)(b)) en te delen om goede integratie van het model en naleving van de AI-verordening mogelijk te maken (overweging 101). De aanbieder verder in de waardeketen vult deze aan met informatie over mogelijke wijzigingen of verfijningen die zijn aangebracht.

Hoog-risico AI-systemen en verschuiving van rollen

Een gebruikersverantwoordelijken kan onder omstandigheden ook de rol van aanbieder aannemen Dat betekent ook dat deze partij zich aan de verplichtingen van een aanbieder moeten houden (Art. 25(1)).

De AI-verordening beschrijft drie scenario's waarin dit mogelijk is. Deze scenario's spelen zich af in de context van AI-systemen die al door een andere partij op de markt zijn gebracht. Een gebruikersverantwoordelijke wordt een aanbieder als deze:

1. Een eigen naam of merk op een AI-systeem met een hoog-risico plaatst. Het maakt hierbij niet uit of de partijen contractuele afspraken hebben gemaakt over de verdeling van de juridische verplichtingen.
2. Een substantiële wijziging aanbrengt aan een AI-systeem met een hoog-risico op zo'n manier dat het systeem een hoog-risico blijft. Een substantiële wijziging is een wijziging die door de oorspronkelijke aanbieder niet vooraf is meegenomen in de conformiteitsbeoordeling[1] (Art. 3(23)). Dat betekent dus dat de nieuwe aanbieder die de wijziging heeft gemaakt ook verantwoordelijk is voor naleving op dit vlak. Een verandering van het beoogde doel van een AI-systeem, dat is vastgelegd in de technische documentatie, kan ook een gevolg zijn van een substantiële wijziging.
3. Het beoogde doel van een niet-hoog risico AI-systeem zodanig verandert dat het AI-systeem als hoog-risico wordt geclassificeerd. Bijvoorbeeld met technische wijzigingen, het aanpassen van de context waarin de toepassing wordt gebruikt, of de output anders toepassen. Een voorbeeld is als een werkgever een applicatie voor persoonlijke zelfevaluaties verplicht stelt om zijn werknemers te monitoren, wat een hoog-risico toepassing is (Annex III(4)(b)).

In geval van een van de drie bovenstaande scenario's is de oorspronkelijke aanbieder geen aanbieder meer voor het nieuwe systeem. De oorspronkelijke aanbieder moet wel nauw samenwerken met de nieuwe aanbieder en helpen met de naleving van de AI-verordening, onder andere door relevantie technische documentatie te delen (Art. 25(2)).

! Let op: De verplichting om documentatie te verstrekken geldt niet als de oorspronkelijke aanbieder heeft aangegeven dat het AI-systeem niet mag worden gewijzigd in een AI-systeem met een hoog-risico (Art. 25(2)) of is beperkt als het intellectuele eigendomsrechten of bedrijfsgeheimen in gevaar zou kunnen brengen (Art. 25(5)).

De rol als een aanbieder van een hoog-risico AI-systeem brengt veel verplichtingen en extra werk met zich mee. Zeker in het geval waarbij modellen voor algemene doeleinden onderdeel vormen van het systeem, dan is documentatie benodigd is van de aanbieder van het model die mogelijk niet (voldoende) beschikbaar is. Het is belangrijk om hierover een goed afgewogen keuze te maken.

Is SSC-ICT aanbieder als mijn organisatie vlam-chat afneemt?

SSC-ICT is de aanbieder van vlam-chat. VLAM-chat is niet ontworpen voor hoog-risico use cases. Als een organisatie vlam-chat desondanks toch inzet in een hoog-risico toepassingsgebied, of als veiligheidscomponent (in een nieuw 'systeem') dat niet voorzien is door de aanbieder (zie scenario 3), dan is de organisatie die deze wijzigingen aanbrengt, en hiermee dus een nieuw systeem in werking stelt, de aanbieder voor de AI-verordening (inclusief de plichten en vereisten die daarbij horen).

[1] Een conformiteitsbeoordeling wordt uitgevoerd door de aanbieder van een hoog-risico AI-systeem (en soms door een onafhankelijke notified body) voordat het systeem op de markt wordt gebracht of in gebruik wordt genomen. Hiermee wordt vastgesteld dat het systeem voldoet aan alle eisen van de AI Act, zoals risicobeheersing, datakwaliteit en menselijke controle.

Bestaande hulpmiddelen

- De Beslishulp AI-verordening helpt bij het bepalen of jouw systeem onder de AI-verordening valt en welke rol jouw organisatie hierbij aanneemt.
- Het overzicht rollen en verantwoordelijkheden, geeft een kort overzicht van de rollen in de AI-verordening en wanneer welke van toepassing is (vindbaar op dezelfde plek als dit document).

Hoe kunnen we binnen onze organisatie/keten/domein AI-governance het beste organiseren?

De AI-verordening schrijft geen specifiek governancekader voor. Dit zal per organisatie ingericht moeten worden om te helpen bij de juiste implementatie van AI-toepassingen. Voor het gebruik van generatieve AI kan mogelijkerwijs aangesloten worden op al bestaande AI- of data-governance van de organisatie.

De AI-verordening stelt wel de verplichting voor hoog-risico AI-systemen een systeem voor risicobeheersing (Art. 9) en kwaliteitsbeheer (Art. 17) op te zetten. De stappen die voor deze verplichtingen worden beschreven zijn ook breder toepasbaar en kunnen worden gebruikt voor het inrichten van een goede governance-structuur.

In de onderstaande hulpmiddelen wordt verwezen naar verschillende bronnen die extra uitleg en inspiratie geven voor het inrichten van AI-governance. De governance pagina op het Algoritmekader gaat over de governance van algoritmen binnen je organisatie en geeft maatregelen mee die kunnen helpen bij de inrichting hiervan. Hoofdstuk 4 van de 'Overheidsbrede handreiking op Verantwoorde inzet van generatieve AI' beschrijft een stappenplan voor een effectieve AI-governance. De visie op generatieve AI van de Autoriteit Persoonsgegevens heeft ter inspiratie een tabel in figuur 7 die op model-, systeem- en toepassingsniveau mogelijke beheersmaatregelen geeft voor de ontwikkeling, inzet en het gebruik van generatieve AI.

Bestaande hulpmiddelen

- De Overheidsbrede handreiking voor verantwoorde inzet van generatieve AI beschrijft in hoofdstuk 4 een stappenplan voor het inzetten van generatieve AI met onder andere hoe een effectieve AI-governance opgezet kan worden.
- Het Algoritmekader geeft op deze pagina uitleg over het inrichten van governance binnen je organisatie en welke maatregelen daarbij kunnen horen.
- Op het Algoritmekader vind je hier ook meer informatie over generatieve AI en wat het gebruik ervan met zich meebrengt voor de overheid.
- De AP-visie op generatieve AI bevat op pagina 22 een figuur die als inspiratiebron dient voor de beheersing van de ontwikkeling, inzet en het gebruik van generatieve AI.

Vereisten

Wat zijn transparantieverplichtingen bij Generatieve AI?

Transparantieverplichtingen m.b.t. door AI gegenereerde/ gemanipuleerde inhoud

De AI-verordening kent een aantal transparantieverplichtingen. Het moet voor mensen duidelijk zijn dat ze in contact zijn/komen met een AI-systeem. Art. 50 maakt onderscheid in transparantie-verplichtingen voor aanbieders en gebruiksverantwoordelijken en voor 4 soorten AI-systemen.

Aanbieders moeten ervoor zorgen dat zij de AI-systemen zo ontwerpen en ontwikkelen dat mensen geïnformeerd kunnen worden dat ze met (de output) van een AI-system te maken hebben (Art. 50).

- I**nteractie met een AI-systeem**
  Sommige AI-systemen zijn bedoeld voor directe interactie met mensen. Denk bijvoorbeeld aan chatbots of spraakassistenten. Voor deze systemen geldt dat mensen door de gebruiksverantwoordelijke geïnformeerd moeten worden dat zij communiceren met een AI-systeem. De informatie moet expliciet en aan het begin van de interactie duidelijk worden gemaakt (Art. 50(5) en overweging 132). Alleen als het overduidelijk is dat er geen sprake is van interactie met een mens, maar met een AI-systeem, is geen expliciete kennisgeving nodig.
- **Content gemaakt met een AI-systeem**
  Een AI-systeem kan synthetische audio-, beeld-, video- of tekstinhoud genereren. In dat geval moet de output van dat systeem worden gemarkeerd als kunstmatig gegenereerd of gemanipuleerd (Art. 50(2) en (4)). Op deze verplichting is een uitzondering mogelijk als het gebruik van het AI-systeem wettelijk is toegestaan voor wetshandhaving. Daarnaast zijn er beperkte transparantieverplichtingen zijn er voor kunst en fictie dat met behulp van AI is gegenereerd. Aanbieders moeten een technische oplossing zoeken voor de markering van synthetische data gemaakt met Generatieve AI. Bijvoorbeeld 'SynthID' van Google waarbij een digitaal watermerk wordt toegevoegd aan beeldmateriaal wat door een Generatieve AI-systeem wordt gegenereerd en later kan worden herkend.[1]
- **AI-systemen voor emotieherkenning of biometrische categorisering**
  Voor AI-systemen voor het herkennen van emotie (Art. 3(39)) en biometrische categorisatie (Art. 3(40)) geldt dat gebruiksverantwoordelijken de gebruikers expliciet moeten informeren over de werking (Art. 50(3)). Let op dat de AVG hier volledig van toepassing is en er een rechtsgrond voor de verwerking moet zijn (overweging 63).
- **Informeren publiek met AI gegenereerde of bewerkte tekst**
  Gebruiksverantwoordelijken kunnen met behulp van een AI-systeem gegenereerde of bewerkte tekst aanbieden om het publiek te informeren over zaken van algemeen belang. Bijvoorbeeld bij het automatisch genereren van nieuwsberichten over een noodsituatie. De gebruikersverantwoordelijke moeten dan bekend maken dat deze tekst kunstmatig is gegenereerd of bewerkt (Art. 50(4)). Hierop zijn 2 uitzonderingen mogelijk:
  - Het gebruik van het AI-systeem is bij wet toegestaan om strafbare feiten op te sporen, te voorkomen, te onderzoeken of te vervolgen; of
  - De door AI gegenereerde content is onderworpen aan menselijke toetsing of er heeft redactionele controle plaatsgevonden. Deze uitzondering geldt als een natuurlijke of rechtspersoon de redactionele verantwoordelijkheid draagt voor de bekendmaking van de content. AI is dan een hulpmiddel om concepten op te stellen. Een mens controleert de content op juistheid voordat deze wordt vastgesteld en gepubliceerd.

Uitzonderingen op de transparantieverplichtingen gelden voor AI-systemen die ingezet worden voor rechtshandhaving: opsporen, voorkomen, onderzoeken of vervolgen van strafbare feiten (Art.50(1)). Behalve voor AI-systemen die meldingen van strafbare feiten door het publiek afhandelen, zoals chatbots van de politie.

Transparantie bij AI-systemen met hoog-risico

Art. 13 bevat de verplichtingen t.a.v. transparantie en informatieverstrekking bij AI-systemen met een hoog-risico. Aanbieders moeten deze systemen zo ontwerpen en ontwikkelen dat de werking voldoende transparant is. Dit moet gebruiksverantwoordelijken in staat stellen de output kunnen te interpreteren en het systeem op de passende wijze kunnen gebruiken.

De aanbieder moet zorgen dat de gebruikersinstructies bij het AI-systeem met een hoog-risico onder andere duidelijk zijn en begrijpelijk voor de gebruiksverantwoordelijken.

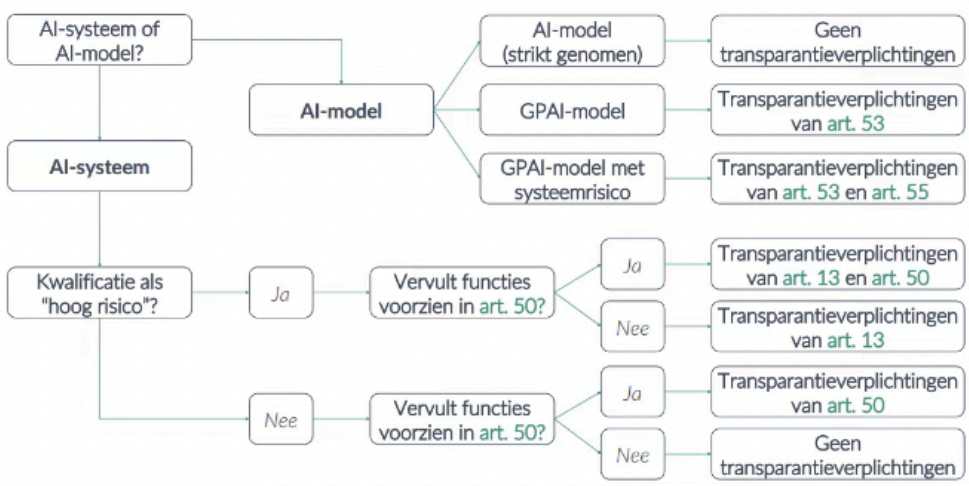
Transparantie bij beslissingen door AI-systeem

Gebruiksverantwoordelijken voor een AI-systeem met een hoog-risico (bijlage III) moeten mensen informeren als zij dit systeem inzetten om beslissingen over hen te nemen of om daarbij te helpen (Art. 26(11)).

[1] Lees meer over de werking op: https://deepmind.google/models/synthid/

Transparantie bij AI-modellen voor algemene doeleinden

Aanbieders hebben verplichtingen ten aanzien van het opstellen en up-to-date houden van (technische) documentatie en informatie. De verplichtingen zijn uitgewerkt in Art. 53.



Figuur 1 KU Leuven. 'Een visueel overzicht van de transparantie-verplichtingen; (KU Leuven: transparantieverplichtingen en AI wet)

Informatieplicht vanuit de AVG

Uit Art. 13 en 14 van de AVG volgt een informatieplicht over de verwerking van persoonsgegevens. Deze plicht geldt zowel wanneer persoonsgegevens direct bij de betrokkene worden verzameld (Art. 13 AVG) als wanneer de persoonsgegevens niet van de betrokkene zijn verkregen (Art. 14 AVG).

Deze informatieplicht geldt ook voor werkgevers richting hun medewerkers. Een werkgever moet informatie geven over onder andere welke persoonsgegevens door hen worden verzameld, met welk doel deze worden verzameld en op basis van welke grondslag. Dit kan door een duidelijke link naar de privacyverklaring op te nemen waarin deze informatie wordt gegeven.

Daarnaast moeten gebruiksverantwoordelijken in hun rol van werkgever hun OR en betrokken medewerkers informeren over het gebruik van AI-systemen met een hoog-risico.

Ook vanuit andere wetgeving gelden transparantieverplichtingen, zoals het consumentenrecht en de Digital Services Act. Vraag juridische ondersteuning om helder te krijgen aan welke andere wetgeving moet worden voldaan.

Bestaande hulpmiddelen

- Algoritmekader (selecteer [onderwerp] 'transparantie').
- Code of Practice for General-Purpose AI models, KU Leuven

Meer informatie en gerelateerd

- Er komt een code of practice aan over het labelen van gegenereerde content.

Toekomstige hulpmiddelen

- In de zomer van 2026 presenteert het AI-bureau (Europese Commissie) leidraad en *code of* practice over de transparantieverplichtingen uit Art. 50.

Wat kunnen we al doen als geharmoniseerde standaarden (nog) niet beschikbaar zijn?

Productstandaarden zijn volop in ontwikkeling en zullen op termijn verdere en concretere invulling geven aan de vereisten uit de AI-verordening.

Als er (nog) geen geharmoniseerde standaarden zijn, blijven de regels uit de AI-verordening gelden. Het ontbreken van standaarden betekent dat er geen sprake is van een *vermoeden van conformiteit*[1] en dat aanbieders en gebruiksverantwoordelijken zelf moeten aantonen dat hun AI-systemen voldoen aan de geldende vereisten. Dit vraagt om een alternatieve invulling van compliance, via uitgebreidere en meer gedetailleerde technische documentatie.

In de praktijk kunnen organisaties in deze situatie gebruikmaken van bestaande internationale standaarden en concept-standaarden die betrokken worden bij toekomstige geharmoniseerde standaarden, zoals ISO- en IEC-normen (zie hieronder). Deze standaarden geven geen vermoeden van conformiteit, maar zijn wel relevant voor de deugdelijke ontwikkeling, het beheer en het gebruik van AI-systemen en worden bovendien expliciet betrokken bij de Europese standaardisatietrajecten. Het is daardoor niet nodig om te wachten tot alle geharmoniseerde standaarden formeel zijn vastgesteld.

Daarnaast kunnen organisaties eigen oplossingen hanteren om conformiteit met de vereisten uit de AI-verordening aan te tonen. Dit betekent dat zij zelf invulling moeten geven aan vereisten op het gebied van risicomanagement, datagovernance, transparantie, menselijk toezicht, logging, nauwkeurigheid, robuustheid en cybersecurity. Deze invulling moet goed worden vastgelegd in de technische documentatie van het AI-systeem. Aansluiten bij bestaande governancestructuren in het privacy en informatiebeveiligingsdomein is hier ook om redenen van efficiency zinvol.

Belangrijk is dat deze inspanningen niet losstaan van de bredere implementatie van de AI-verordening. Ook zonder standaarden blijft verankering in beleid en processen, inrichting van governance, bewustwording binnen de organisatie en afstemming met gerelateerde domeinen noodzakelijk. Standaarden kunnen werk uit handen nemen, maar zijn geen voorwaarde voor het starten met implementatie.

Tot slot kunnen organisaties, op basis van hun AI-portfolio en roadmap, vooruitlopen op laat beschikbare standaarden door nu al te bepalen hoe zij met deze standaarden zullen omgaan zodra zij beschikbaar komen. Daarbij is ook het perspectief relevant van externe aanbieders van AI-systemen die zelf (nog) geen gebruik kunnen maken van geharmoniseerde standaarden.

Status harmonisatietrajecten AI-standaarden (update 12/2025)

Reeds in publieke consultatie:

- *prEN 18286 Quality management system for EU AI Act regulatory purposes*

Half februari in publieke consultatie

- prEN 18228: AI Risk Management
- prEN 18229-1: AI trustworthiness framework - Part 1: Logging, transparency and human oversight
- prEN 18229-2: AI trustworthiness framework - Part 2: Accuracy and robustness
- prEN 18282: Cybersecurity specifications for AI systems

Half juni in publieke consultatie

- prEN 18283: Concepts, measures and requirements for managing bias in AI systems

[1] Het vermoeden van conformiteit betekent dat een AI-systeem geacht wordt te voldoen aan de AI Act als het is ontwikkeld volgens geharmoniseerde normen of erkende specificaties. De toezichthouder gaat er dan in principe vanuit dat aan de wettelijke eisen is voldaan, tenzij het tegendeel wordt aangetoond.

Gepubliceerde standaarden die betrokken worden bij harmonisatietrajecten

Stand. verzoek	Referentie	Traject
Accuracy specifications for AI systems	FprCEN/CLC, ISO/IEC/TS 12791	Information technology - Artificial intelligence - Treatment of unwanted bias in classification and regression machine learning tasks
	ISO/IEC TS 4213	Accuracy of classification systems
	ISO/IEC TS 4213 (update)	Accuracy of AI systems for regression, recommendation and clustering
Governance and quality of datasets used to build AI systems	CEN/CLC/TR 18115	Data Governance and quality for AI in the European context
	FprCEN/CLC ISO/IEC/TS 12791	Information technology - Artificial intelligence - Treatment of unwanted bias in classification and regression machine learning tasks
	prEN ISO/IEC 8183	Information technology – Artificial intelligence – Data life cycle framework
	ISO/IEC 5259 part 1-4	Data quality for analytics and machine learning (ML) - Part 1: Overview, terminology, and examples - Part 2: Data quality measures - Part 3: Data quality management requirements and guidelines - Part 4: Data quality process framework
Supporting standard	EN ISO/IEC 22989:2023	Information technology - Artificial intelligence – Artificial intelligence concepts and terminology (ISO/IEC 22989:2022)
	EN ISO/IEC 23053:2023	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) (ISO/IEC 23053:2022)

Meer informatie en gerelateerd

- Zie, naast bovenstaand schema, de website van de Autoriteit Persoonsgegevens voor de meest recente informatie.
- De Autoriteit Persoonsgegevens over de rol van productstandaarden voor AI-systemen.
- Overzicht van de status van de standaardisatietrajecten.

Welke impact assessments (bijv. IAMA, DPIA) zijn verplicht voor AI-systemen?

DPIA (Art. 35 AVG)

Een DPIA moet worden uitgevoerd bij een verwerking van persoonsgegevens die waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Deze verplichting geldt in het bijzonder voor een verwerking waarbij nieuwe technologieën worden gebruikt. Om te bepalen of je een DPIA moet uitvoeren, kan de Pre-scan DPIA gebruikt worden (zie 'bestaande hulpmiddelen).

Deze verplichting geldt ook voor een AI-systeem als in het AI-systeem persoonsgegevens verwerkt worden en dit waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van natuurlijke personen. Bijvoorbeeld als een AI-systeem wordt gebruikt om fraude te bestrijden.

Een DPIA is een hulpmiddel om risico's voor de rechten en vrijheden van mensen in beeld te brengen. Ook helpt het om te beoordelen of de huidige maatregelen voldoende zijn en welke extra maatregelen nodig zijn om de risico's zo veel mogelijk te beperken. Het gaat bij een DPIA dus niet om de risico's voor de organisatie. Verwerken is alles wat er met persoonsgegevens gedaan wordt, bijvoorbeeld verzamelen, invoeren, bewaren en archiveren van persoonsgegevens.

Het is belangrijk om de DPIA zo vroeg mogelijk in het proces uit te voeren. Op dat moment is het namelijk nog mogelijk om met open vizier na te denken over de effecten en bestaat er nog voldoende gelegenheid om de uitgangspunten van het voorstel zonder grote nadelige consequenties te herzien.

Bij hoog-risico AI-systemen gebruik je de gebruikersinstructies verstrekt door de aanbieder (Art. 13) bij de verplichting om een DPIA uit te voeren (Art. 26(9)).

Mensenrechten impact assessment

Overheidsorganisaties en aanbieders van publieke diensten, zoals onderwijs- en zorginstellingen, wordt sterk aangeraden een mensenrechten-impactbeoordeling (FRIA) uit te voeren bij het gebruik van hoog-risico AI-systemen in de zin van Art. 6(2).

Een voorbeeld van een mensenrechten impact assessment is het Universiteit Utrecht ontwikkelde IAMA. Een ander voorbeeld is het AI impact assessment (AIIA) ontwikkeld door het Ministerie van IenW. Dit laatste heeft in bijlage 3 specifiek aandacht voor Generatieve AI.

De handreiking samenhang IAMA, AIIA en AI-geletterdheid kan behulpzaam zijn bij het maken van keuze voor een instrument en de uitvoering van een gekozen assessment. Deze is op te vragen via privacy-ciorijk@minbzk.nl.

Vanaf 2 augustus 2026 moeten gebruikers van AI-systemen met een hoog-risico voor de start van het gebruik een Fundamental Rights Impact Assessment (FRIA) uitvoeren (Art 27). Een FRIA richt zich op risico's van AI-systemen voor fundamentele rechten. Dat zijn grondrechten zoals privacy, maar bijvoorbeeld ook discriminatie, vrijheid van meningsuiting, milieu en andere maatschappelijke effecten. Door deze effecten in kaart vooraf in kaart te brengen kunnen mitigerende maatregelen genomen worden om de risico's te verminderen. Op het moment van schrijven is er nog geen standaard aanpak voor FRIA's.

Er is (mogelijk) een dubbele verplichting voor het uitvoeren van risico assessments, waarbij er overlap is tussen elementen van een DPIA, FRIA en andere (risico)afwegingen. Dit wordt ook in de AI-verordening erkend en organisaties kunnen kiezen voor twee aparte assessments of een geïntegreerd assessment. Voor het gezamenlijk uitvoeren van een IAMA en een DPIA is een handreiking beschikbaar, zie hieronder.

Bestaande hulpmiddelen

- De invulhulp pre-scan DPIA kan ingevuld worden om te zien welke assessments (nog meer) gedaan moeten worden. De invulhulp Rijksmodel DPIA om de initiële DPIA in te vullen.
- Handreiking gezamenlijk uitvoeren IAMA en DPIA. De overeenkomsten en verschillen tussen het IAMA en de DPIA zijn opgenomen in een handreiking. Hierin is ook uitgelegd hoe deze instrumenten gecombineerd kunnen worden. Het doel is om zo deze instrumenten op een efficiënte en gebruikersvriendelijke manier samen te kunnen gebruiken. Dit document wordt herzien in verband met de nieuwe versie van de IAMA.
- De impact assessment mensenrechten en algoritmes (v2)
- Het AI Impact Assessment (AIIA) van IenW, bijlage 3 gaat specifiek in op Generatieve AI.
- Het Rijksmodel DPIA op Beleidskompas.

Meer informatie en gerelateerd

- Art. 26(9) & 27, Art. 35 AVG.
- AVG Regels bij het gebruik van algoritmes.
- DPIA in het Algoritmekader.
- IAMA in het Algoritmekader.

Welke impact assessments zijn verplicht voor een leverancier?

Voor leveranciers (aanbieders) geldt dat zij aan veel eisen moeten voldoen, met name bij het ontwerp en ontwikkelen van AI-systemen met een hoog-risico (Art. 16). Eisen zijn onder andere een risicobeheersysteem (Art. 9) en een kwaliteitsbeheersysteem (Art. 17). Een impact assessment als een DPIA of een mensenrechten impact assessment hoeven zij echter niet te doen. Dat is aan de gebruiksverantwoordelijken.

Een risicomanagementsysteem moet worden ingericht om bekende risico's en risico's die redelijkerwijs te voorzien zijn te identificeren en analyseren. De focus moet bij risico's liggen op gezondheid, veiligheid en grondrechten. De AI-verordening stelt eisen aan het risicomanagementsysteem (Art. 9). Een kwaliteitsbeheersysteem helpt bij de naleving van de AI-verordening. Hiervoor worden standaarden ontwikkeld die naar verwachting in 2026 worden vastgesteld en gepubliceerd.

Voor Generatieve AI modellen met systeemrisico zijn modelevaluaties verplicht en moeten risico's gemitigeerd worden.

Meer informatie en gerelateerd

- Art. 9 & 72 voor post-market monitoring.
- Art. 55 voor Generatieve AI *modellen* met systeemrisico.

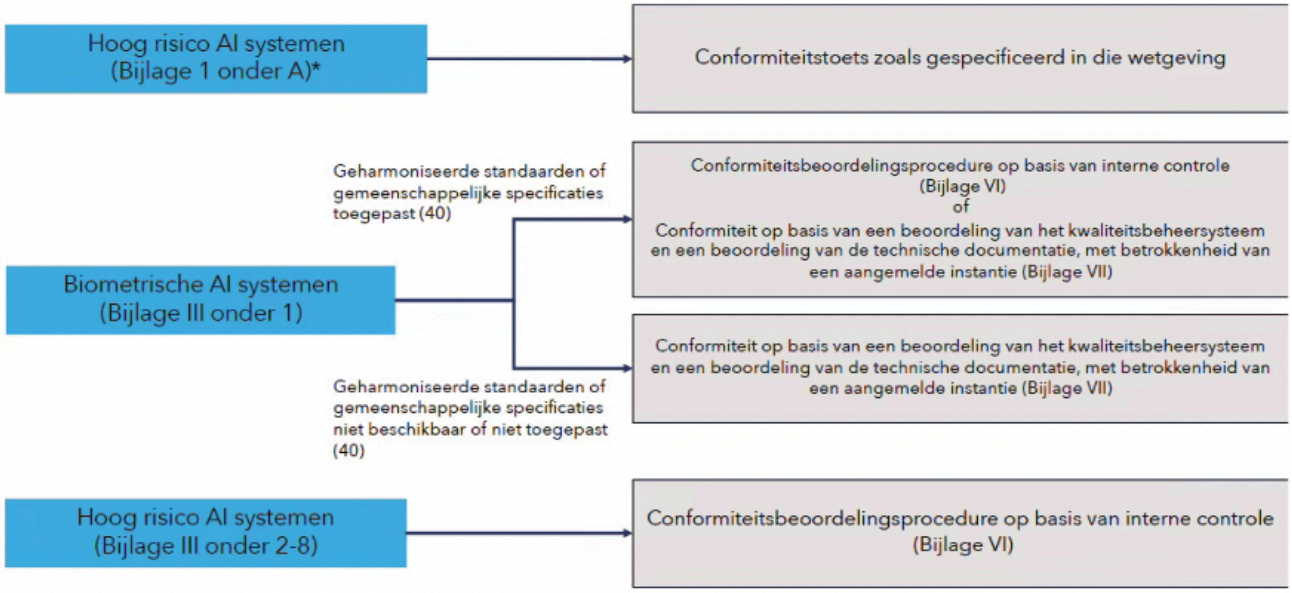
Wanneer en hoe doen we een conformiteitsbeoordeling?

Aanbieders van AI-systemen met een hoog-risico moeten zorgen dat een conformiteitsbeoordeling (Art. 43) wordt uitgevoerd, voordat zij hun hoog-risico AI-systeem op de markt brengen of in gebruik nemen (Art.16).

Het soort hoog-risico AI-systeem bepaalt welke conformiteitsbeoordeling moet worden uitgevoerd. Expertise van juristen en kwaliteitsmedewerkers helpt om te bepalen welke toets op welke wijze uitgevoerd moet worden. Hieronder is in schema kort weergegeven welke conformiteitstoets er wanneer uitgevoerd moeten worden.

Meer informatie en gerelateerd

- Het Algoritmekader biedt aanvullende informatie over de conformiteitsbeoordelingsprocedure.



Figuur 2 Considerati: welke conformiteitstoets?

Welke eisen gelden voor niet-hoog-risico Generatieve AI-systemen?

Er moet worden vastgesteld dat er sprake is van een AI-systeem (Art. 3.1) en wat de risicoclassificatie van het AI-systeem is. Documenteer deze beoordeling.

Aanbieders en gebruiksverantwoordelijken moeten zorgen voor een toereikend niveau van AI-geletterdheid bij hun medewerkers en andere personen die namens hen AI-systemen exploiteren en gebruiken (Art. 4). Daarbij moet, zoals bij ook andere scholing, rekening worden gehouden met technische kennis, ervaring, onderwijs en opleiding en de context waarin de AI-systemen gebruikt gaan worden en ook met de personen ten aanzien van wie de AI-systemen zullen worden gebruikt.

Er zijn transparantieverplichtingen voor AI-systemen die bedoeld zijn voor directe interactie met natuurlijke personen (Art. 50) (zie ook de 1e vraag over transparantieverplichtingen.

Andere wetgeving dan de AI-verordening blijft gelden, bijvoorbeeld de AVG, Auteurswet en de Woo.

Meer informatie en gerelateerd

- Het Algoritmekader geeft maatregelen voor de documentatie van de beoordeling 'geen hoog-risico-AI-systeem'.

Wat is de relatie met andere wetgeving en beleid?

Soms overlapt andere wet- of regelgeving met de AI-verordening. In die gevallen gelden beide wetten. Voorbeelden van overlap:

- De **Cybersecuritywet** stelt eisen aan de beveiliging van AI-systemen, kent een meldplicht voor het melden van incidenten en vereist een vorm van risicobeoordeling.
- De **AVG** en de AI-verordening gaan uit van een verantwoord gebruik van AI en persoonsgegevens om fundamentele rechten en vrijheden van mensen te beschermen. Beide wetten grotendeels risico gebaseerd. Dit betekent hoe hoger de risico's, hoe strenger de regels en eisen. Het is essentieel om vast te stellen welke rol je hebt binnen de wetgeving. Hierdoor weet je aan welke verplichtingen voldaan moet worden.
- Naast de AVG kan er specifieke wetgeving zijn voor de omgang met persoonsgegevens. Bijvoorbeeld de **Wet politiegegevens (Wpg)**. Deze wet regelt het verwerken van politiegegevens. Dit zijn persoonsgegevens die voor het uitvoeren van de politietaak worden verwerkt.
- De **Wet open overheid (Woo)** moet zorgen dat voor burgers duidelijk wordt wat de overheid doet en waarom. Er zijn regels voor openbaarheid van overheidsinformatie en uitzonderingen (bijvoorbeeld persoonsgegevens) hierop. Bij een verzoek om openbaarheid van een algoritme moet dit dus ook langs de regels van de Woo worden gelegd.
- De **Wet hergebruik overheidsinformatie (Who)** verplicht overheden om op verzoek openbare (ongevoelige) overheidsinformatie beschikbaar te stellen voor hergebruik op een manier dat deze gegevens vindbaar, toegankelijk en ook daadwerkelijk technisch herbruikbaar zijn, bijvoorbeeld met open bestandsformaten en open licenties. Daar hoort ook broncode van (AI-)systemen bij. Deze informatie kan dan ook voor andere doeleinden worden gebruikt dan waarvoor zij verzameld of geproduceerd zijn, zoals het oplossen van maatschappelijke problemen als de energiecrisis, en voor innovatie en economische groei.[1]
- De **BIO2 (Baseline Informatiebeveiliging Overheid)** stelt eisen aan de informatiebeveiliging van systemen binnen de overheid, waaronder AI-systemen. De BIO2 hanteert net als de AI-verordening een risico gebaseerde aanpak en verplicht overheidsorganisaties tot het inrichten van een beheersysteem voor informatiebeveiliging (ISMS). De Quickscan Informatiebeveiliging (QIS) is een instrument dat daarbij helpt: hiermee bepaalt een organisatie het benodigde beveiligingsniveau van een proces of systeem. Omdat de AI-verordening ook eisen stelt aan risicobeheer en beveiliging van AI-systemen, liggen deze kaders inhoudelijk dicht bij elkaar en is afstemming tussen beide trajecten aan te raden.
-

! Let op: Vraag bij een jurist na welke aanvullende wetgeving van kracht is.

Meer informatie en gerelateerd

- Informatie over de doorwerking van internationaal recht in de nationale rechtsorde.
- Basisinformatie AVG van de Autoriteit Persoonsgegevens.

[1] Vernieuwde Handleiding herziene Wet hergebruik van overheidsinformatie

Inkoop en ontwikkeling

Wat zijn vereisten voor (generatieve) AI-systemen en hoe kunnen deze in het inkoop- of leveranciersproces worden opgenomen?

De vereisten voor Generatieve AI-systemen die van belang zijn in het inkoopproces zijn afhankelijk van allerlei technische en organisatorische aspecten. Omdat de inkopende organisatie en/of leveranciers nog relatief weinig ervaring hebben met de inkoop van dergelijke systemen is het van belang het inkoopproces zorgvuldig in te richten.

In het Algoritmekader, op de websites van PIANOo en de Europese Commissie is informatie te vinden over het veilig kopen of laten ontwikkelen van algoritmes en AI. Deze informatie zal zowel in bij interne als Rijksbrede inkoop- en leveranciersprocessen moeten worden verwerkt. Er zijn standaard clausules ontwikkeld door de EU. Ook zijn er andere standaarden, bijvoorbeeld de algemene voorwaarden inkoop Rijksoverheid. Het CIP heeft een wizard voor veilig aanbesteden. Hierin zijn cybersecurity- en privacy-eisen verwerkt.

Weten inkopers genoeg van de AI-verordening?

Inkopers spelen een belangrijke rol voor de compliance van Generatieve AI-systemen. Het naleven van sommige vereisten uit de AI-verordening worden al bij de keuze voor een bepaald systeem of leverancier bepaald. Er is een factsheet over de AI-verordening voor inkopers beschikbaar (zie 'bestaande hulpmiddelen') in het Algoritmekader en de website van PIANOo geeft een leidraad voor het inkopen en ontwikkelen van AI.

Zoals bij elke nieuwe wetgeving is nog niet alles uitgekristalliseerd in de praktijk. Vraagstukken rond de inkoop van AI-systemen zullen in de komende tijd meer in samenhang beantwoord worden, onder andere door de prioriteit vanuit de NDS.

Hoe werkt de inkoop van VLAM-chat?

SSC-ICT een interne dienstverlener. Daarom is er geen sprake van aanbesteding, maar van inbesteding. Om een VLAM dienst af te nemen heeft SSC-ICT een samenwerkruimte ingericht met documentatie. Voor meer informatie en toegang, neem contact op met: SSCICTAI@minbzk.nl.

Vlam kan het beste worden gezien als AI-as-a-Service (AIaaS). AI-as-a-Service bij SSC-ICT betekent dat geavanceerde AI-modellen beschikbaar worden gesteld en gehost vanuit een eigen GPU-cluster. Dit betekent dat de modellen draaien op eigen systemen van het Rijk, en niet bij commerciële aanbieders zoals grote clouddiensten. SSC-ICT ontwikkeld in dit kader een aantal diensten:

- vlam-API: brengt veilig eigen AI-apps naar productie voor de Rijksoverheid
- vlam-chat: chat veilig met generatieve AI zonder gevoelige data te lekken
- vlam-search: doorzoek snel openbare overheidsinformatie met krachtige AI
- vlam-transcribe: Maakt automatisch notulen of samenvattingen van vergaderingen.

Bestaande hulpmiddelen

- Inkoopvoorwaarden uit het Algoritmekader.
- De factsheet AI-geletterdheid voor inkopers.
- De PIANOo Leidraad kopen en ontwikkelen algoritmes en AI (PIANOO).
- EU AI model contractual clauses (Public Buyers Community):
- Algemene inkoopvoorwaarden voor het Rijk.
- De ICO-Wizard (CIP).

Hoe gaan we om met (nieuwe) generatieve AI-componenten in een bestaande dienst?

Wanneer aan een bestaande dienst (nieuwe) generatieve-AI-componenten worden toegevoegd, is het noodzakelijk hierover vooraf afspraken te maken met de leverancier en deze contractueel vast te leggen. Onderdeel van deze afspraken moet zijn dat de leverancier tijdig meldt wanneer AI-functionaliteit wordt geïntroduceerd of wordt gewijzigd en dat dergelijke wijzigingen uitsluitend na akkoord van de opdrachtgever worden doorgevoerd.

De inzet van generatieve AI kan gevolgen hebben voor het doel, het gebruik en de risicoclassificatie van de dienst. Daarom is het belangrijk om bij wijzigingen te beoordelen of het gebruik van een AI-component binnen het oorspronkelijke doel blijft of dat een herbeoordeling van de risicoclassificatie onder de AI-verordening nodig is. Als de inzet leidt tot een andere of bredere toepassing kunnen aanvullende verplichtingen gelden. Zoals verplichtingen voor hoog-risico AI-systemen of een wijziging in rollen en verantwoordelijkheden.

Naast de AI-verordening blijven andere juridische kaders van toepassing, zoals regelgeving op het gebied van intellectueel eigendom, gegevensbescherming en informatiebeveiliging. Deze aspecten moeten worden meegenomen bij zowel de ontwikkeling als de inkoop en het gebruik van AI-functionaliteit binnen bestaande diensten.

Door wijzigingsafspraken en verantwoordelijkheden vooraf vast te leggen, kan de inzet van generatieve AI binnen bestaande diensten op een beheerste en conforme manier plaatsvinden.

Bestaande hulpmiddelen

- Factsheet AI-geletterdheid voor inkopers in het Algoritmekader.
- Voorwaarden voor inkoop bij Rijksopdrachten.

- Contractvoorwaarden voor het inkopen van artificiële intelligentie.
- Leidraad 'Het kopen of laten ontwikkelen van algoritmes en AI': (PIANOO).

Meer informatie en gerelateerd
- Beschrijving het van het inkoopproces.

Hoe kunnen we nagaan of ons beoogde doel geschikt is voor het AI-systeem van een aanbieder?

Er zijn twee verschillende soorten afwegingen die nodig zijn om na te gaan of een doel geschikt is om met inzet van een AI-systeem te behalen:

- Juridische afweging: Mogen we dit systeem voor ons doel gebruiken? Om deze afweging te maken moet het doel duidelijk zijn en worden nagegaan of de AI-verordening het AI-systeem of de beoogde inzet als hoog-risico heeft geclassificeerd. Niet alleen het door de aanbieder bepaalde beoogde doel is dan relevant, maar ook hoe de gebruikersverantwoordelijke het AI-systeem in de concrete context feitelijk gaat gebruiken. Is er sprake van een hoog-risico use case, dan moet het systeem door de aanbieder ontwikkeld zijn met een beoogd doel dat aansluit bij het doel van de gebruiksverantwoordelijke. Dit blijkt uit de documentatie van de aanbieder. Een systeem kan dus gebruikt worden als het ontworpen is voor een hoog-risico use case en zo ook ingezet wordt, of als een systeem wordt ingezet voor een use case die niet hoog-risico is.
- Functionele afweging: Is het systeem goed genoeg voor ons doel? Deze afweging is complex en contextafhankelijk. De mogelijkheden van AI-systemen veranderen snel maar worden ook overschat. Daarnaast is de kwaliteit van een AI-systeem niet alleen afhankelijk van technische aspecten, maar ook van de inbedding in het IT-landschap, beheersing, vaardigheden van gebruikers, enzovoort. Een organisatie zal dus vooralsnog zelf moeten testen en valideren of (en onder welke voorwaarden) een AI-systeem geschikt is.

Voor generatieve AI-systemen die uiteenlopende taken (lijken te) kunnen uitvoeren, is het lastig te beoordelen of het systeem geschikt is voor een specifieke taak. Of een samenvatting van een tekst goed genoeg is, hangt bijvoorbeeld af van: de complexiteit van de tekst, hoe de prompt is geformuleerd, de capaciteiten van het model, de kennis van de gebruiker, het doel waarvoor de samenvatting wordt gemaakt, en wat de gebruiker met de uitkomst doet. Bij de geschiktheidsbeoordeling is het daarom belangrijk om goed in beeld te hebben welke factoren de kwaliteit beïnvloeden en hoe die per situatie verschillen.

Bestaande hulpmiddelen
- De handleiding identificatie en classificatie AI-systemen geeft een uitgebreide instructie voor de classificatie van AI-systemen.

Meer informatie en gerelateerd
- Voor inzicht in ontwikkelingen van Generatieve AI gebruik (incl. use cases) bij de overheid zie het TNO-rapport 'Overheidsbrede Monitor Generatieve AI'.

Use cases en gebruik

Welke gebruiksinstructie moeten we meegeven bij Generatieve AI-assistenten?

AI-assistenten in de vorm van chatbots kunnen ingezet worden voor allerlei taken, ook taken die ongewenst zijn of waarvoor het systeem ongeschikt is. Omdat de eisen van de AI-verordening afhangen van hoe een AI-systeem wordt gebruikt in de praktijk, is het belangrijk om bij generatieve AI-systemen het gebruik te bewaken.

Er zijn twee scenario's waarvoor beheersing van het gebruik van een AI-systeem het belangrijkst is:

1. Een door de aanbieder geleverd hoog-risico AI-systeem *moet* ingezet worden voor het beoogde doel en in lijn met de gebruiksinstructies door de gebruiksverantwoordelijke.
2. Een hoog-risico AI-systeem dat door de aanbieder niet bedoeld is voor een hoog-risico toepassing, mag ook niet voor zo'n toepassing worden gebruikt. Doe je dat toch, dan word je als gebruiker zelf beschouwd als aanbieder onder de AI-verordening, met alle extra verplichtingen die daarbij horen.

Vereisten voor gebruik en geletterdheid

Een gebruikersverantwoordelijke heeft bij AI-systemen met een hoog-risico verschillende verantwoordelijkheden. Bij een AI-systeem die gebruikt worden voor het door de aanbieder beoogde doel gelden rond het thema 'gebruik' de volgende verantwoordelijkheden:

- Passende technische en organisatorische maatregelen nemen om te waarborgen dat de gebruiksaanwijzingen van de aanbieder worden opgevolgd (Art.26(1)).
- Menselijk toezicht opdragen aan personen die de nodige bekwaamheid, opleiding, en autoriteit hebben en de ondersteuning krijgen die zij nodig hebben (Art.26(2)).
- Controle houden over de inputdata en zorgen dat dit relevant en voldoende representatief is (Art.26(4)).
- Monitoren van de werking van het systeem inrichten (Art.26(5))
- Logs bewaren (voor zover die onder controle van de gebruiksverantwoordelijke vallen) voor ten minste 6 maanden (of langer als dat passend is voor het doel van het systeem) (Art.26(6)).
- Maatregelen nemen om voor een toereikend niveau van AI-geletterdheid te zorgen bij medewerkers en andere betrokkenen die de systemen exploiteren en gebruiken (Art.4).

Voor systemen die door de aanbieder niet bedoeld zijn voor hoog-risico toepassingen moet de gebruiksverantwoordelijke, als hij wil voorkomen als aanbieder aangemerkt te worden, maatregelen nemen om te voorkomen dat gebruikers het systeem voor hoog-risico use cases gebruiken. Daarnaast moet de gebruiksverantwoordelijke bij alle AI-systemen voldoen aan de AI-geletterdheidsvereiste, zijn er mogelijk transparantievereisten (zie: Wat zijn transparantieverplichtingen bij Generatieve AI?), en moeten Rijksoverheidsorganisaties voldoen aan het standpunt generatieve AI.

Maatregelen beheersing eindgebruiker

In alle scenario's is het dus gewenst om maatregelen te nemen die het gebruik van een Generatieve AI-systeem in goede banen leidt. Hieronder volgt een overzicht van maatregelen die hierbij helpen.

Het overzicht overzicht op de volgende pagina dient ter inspiratie. Bij het nemen van maatregelen moet rekening worden gehouden met de specifieke omstandigheden van een organisatie, het AI-systeem en het bedoeld gebruik van het systeem. Let op dat deze maatregelen gericht op *eindgebruikers* niet genoeg zijn om te voldoen aan alle vereisten van de verordening (Zie voor meer informatie over vereisten de vraag: Welke eisen zijn er voor een Generatief AI-systeem met een hoog-risico in de AI-verordening?).

Beleid	• Stel een visie en doelbinding voor Generatieve AI gebruik vast • Ontwerp afgebakende en goedgekeurde use cases • Stel een Privacy-/Gegevensbeschermingsbeleid vast • Maak afspraken over IP en auteursrecht van output • Voorkom invoer van vertrouwelijke of strategische informatie • Weeg de proportionaliteit van de inzet • Leg beperkingen op voor gevoelige toepassingen • Ontwerp expliciete schadepreventie • Sluit aan bij organisatie brede waarden • Sluit aan bij toepasselijk beleid (zoals Woo, archiefwet, etc.)
Governance & Organisatie	• Bepaal eigenaarschap per use case (business owner + AI owner) • Verplicht human-in-the-loop-momenten • Leg validatieplicht van output vast • Ontwerp escalatiepad bij twijfel, fouten of ethische bezwaren • Leg aansprakelijkheden en verantwoordelijkheden vast • Evalueer periodiek en evt. benodigde besluitvorming • Toets aan relevante AI- en privacywetgeving • Zorg voor contractuele borging (dataretentie, training, logging) • Registreer use cases en keuzes daaromtrent • Documenteer aannames en risicoafwegingen • Ontwerp beslislogica rond inzet van Generatieve AI • Regel interne en externe auditbaarheid • Rapporteer periodiek over gebruik en impact
Technische maatregelen	• Bepaal eigenaarschap per use case (business owner + AI owner) • Verplicht human-in-the-loop-momenten • Leg validatieplicht van output vast • Ontwerp escalatiepad bij twijfel, fouten of ethische bezwaren • Leg aansprakelijkheden en verantwoordelijkheden vast • Evalueer periodiek en evt. benodigde besluitvorming • Toets aan relevante AI- en privacywetgeving • Zorg voor contractuele borging (dataretentie, training, logging) • Registreer use cases en keuzes daaromtrent • Documenteer aannames en risicoafwegingen • Ontwerp beslislogica rond inzet van Generatieve AI • Regel interne en externe auditbaarheid • Rapporteer periodiek over gebruik en impact
Geletterdheid & Training	• Geef een basistraining Generatieve AI: werking en beperkingen • Train gebruikers in kritische beoordeling en validatie van output • Bevorder bewustwording van bias, hallucinaties en risico's • Train gebruikers in het herkennen van ongeschikte of risicovolle toepassingen • Maak contextspecifieke training per rol of use case • Herhaal en actualiseer periodiek het bovenstaande • Wijs een aanspreekpunt aan voor vragen en ethische dilemma's

Welke eisen zijn er rond geletterdheid?

Wat moeten we doen, monitoren en rapporteren?

AI-geletterdheid moet betrokkenen in staat stellen om onderbouwde beslissingen te maken met betrekking tot AI-systemen. Afhankelijk van iemands rol en het toepassingsgebied van het AI-systeem, bestaat een toereikend niveau van AI-geletterdheid uit inzicht in:

- De correcte toepassing van technische elementen tijdens de ontwikkeling van AI-systemen;
- De maatregelen die genomen moeten worden tijdens het gebruik van een AI-systeem;
- De juiste interpretatie van de output van AI-systemen;
- De impact van AI-besluiten op natuurlijke personen; en
- De kennis die nodig is om naleving en handhaving van de AI-verordening mogelijk te maken.

Dit betekent dat eenmalige trainingen over de 'kansen en risico's' van AI of een prompttraining niet voldoende zullen zijn. Het gaat om een doorlopend programma gericht op de AI-systemen die in de organisatie worden gebruikt én geldt voor iedereen die te maken heeft met deze systemen. Ook moet regelmatig worden nagegaan of veranderingen in de inzet, context, gebruikers, enzovoort zijn verander en wat dat betekent voor het doel een 'adequaat niveau' van geletterdheid te bereiken bij de verschillende doelgroepen.

Bestaande hulpmiddelen

- In het 'verzameldocument AI-geletterdheid' is meer informatie te vinden (vindbaar op dezelfde plek als dit document):
  - Overzicht vereisten AI-geletterdheid
  - Blauwdruk AI-geletterdheidsprogramma
  - Niveaus, rollen en leerdoelen AI-geletterdheid
  - Overzicht AI-geletterdheidstrainingen
  - Factsheet Inkoop & AI-verordening
  - Factsheet AI-geletterdheid voor bestuurders

Meer informatie en gerelateerd

- De Autoriteit Persoonsgegevens over AI-geletterdheid:
- Het NDS-competentiecentrum dat wordt onderzocht om AI bij de overheid te versnellen zal op termijn mogelijk kunnen ondersteunen bij AI-geletterdheidsvraagstukken.

Veelgestelde vragen Generatieve AI Compliance

2026

ai-verordening@minbzk.nl