Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1233

LIJST VAN VRAGEN EN ANTWOORDEN

Vastgesteld 8 november 2024

De vaste commissie voor Digitale Zaken heeft een aantal vragen voorgelegd aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over het rapport van de Algemene Rekenkamer van 17 oktober 2024 inzake «Publicatie Focus op AI bij de Rijksoverheid» (Kamerstuk 26 643, nr. 1226).

De Staatssecretaris heeft deze vragen beantwoord bij brief van 8 november 2024. Vragen en antwoorden, voorzien van een inleiding, zijn hierna afgedrukt.

De voorzitter van de commissie,
Palmen

Adjunct-griffier van de commissie,
Muller

kst-26643-1233
ISSN 0921 - 7371
's-Gravenhage 2024

Inleiding

Hierbij stuur ik u de beantwoording van de vragen die de vaste commissie voor Digitale Zaken op 25 oktober jl. heeft gesteld naar aanleiding van de bestuurlijke reactie op het Algemene Rekenkamer rapport «Focus op AI bij de Rijksoverheid» mede namens de Minister van Economische Zaken en de Minister van Justitie en Veiligheid.

Het rapport van de Algemene Rekenkamer laat zien dat er veel rondom het gebruik van AI gebeurt. Dit kwam ook naar voren als een belangrijk onderwerp in een bijeenkomst die ik op 4 november jl. had met vertegenwoordigers van gemeenten, waterschappen, publieke dienstverleners, andere departementen, de politiek, het bedrijfsleven en de wetenschap over de totstandkoming van de Nederlandse Digitaliseringsstrategie. Het zou mijns inziens goed zijn om met de leden van de commissie door te praten over de thema's die in deze Kamervragen worden aangesneden. Ik bied dan ook graag aan om daarover een werksessie te organiseren.

Vragen en antwoorden

Vraag 1: Kunt u alle interne protocollen en kaders voor het gebruik van kunstmatige intelligentie (AI-gebruik) die nu gebruikt worden binnen departementen en uitvoerders met de Kamer delen?

Alle protocollen en kaders die relevant zijn voor het gebruik van AI worden samengebracht in het algoritmekader, zodat de hele overheid er gebruik van kan maken. Er is al een versie van dit algoritmekader met uw Kamer gedeeld[1].

Het doel van dit algoritmekader is om wetten en regels beter toepasbaar te maken in de context waarin AI en algoritmes door overheden worden ontwikkeld en/of gebruikt. Het algoritmekader heeft zowel betrekking op algoritmes, als op AI-systemen. De eisen aan AI-systemen die voortvloeien uit de Europese AI-verordening worden momenteel ook in het algoritmekader verwerkt. Dit zal uiterlijk in het eerste kwartaal van 2025 gereed zijn.

Vraag 2: Hoe vult u concreet uw coördinerende taak in bij het toezien op ethisch en wenselijk gebruik van AI-systemen door alle ministeries en uitvoerders?

Mijn taak als Staatssecretaris is hierbij zowel kaderstellend, ondersteunend, en waar nodig aanjagend naar alle overheidslagen. Met onze overheden streven we vooral naar uniformiteit van de aanpak binnen de overheid en zorgen we voor optimale afstemming tussen de overheidslagen. Hiermee kunnen we echt werken als één overheid. En dat is waar ik mij sterk voor maak.

De inzet van AI-systemen door ministeries en uitvoerders dient te voldoen aan geldende wet- en regelgeving. Bij de inzet van AI-systemen dienen daarnaast ethische vragen over de wenselijkheid ervan te worden gesteld.

Als het gaat om ethisch en wenselijk gebruik van AI-systemen, speelt de AI-verordening een belangrijke rol. Daarom focus ik mij op het in lijn brengen van het algoritmekader met de AI-verordening, zodat we als overheid een uniform en integraal kader hebben waarop we ons kunnen inrichten.

---

[1] https://minbzk.github.io/algoritmekader/

In deze aanpak is elk vakdepartement zelf verantwoordelijk voor de verantwoorde inzet van AI-systemen. Vanuit het Besluit CIO-stelsel kan er gemonitord en gecoördineerd worden op deze verantwoorde inzet. Zo worden er via de CIO Rijk bijvoorbeeld uitvragen gedaan naar verboden AI-praktijken en de registratie van hoog-risico AI-systemen door departementen. Eind januari 2025 verwachten we reactie over de verboden AI-praktijken, en februari 2025 over de hoog-risico AI-systemen.

Vraag 3: Kunt u departementen en organisaties dwingen om AI-systemen buiten werking te stellen als deze niet wenselijk zijn?

Binnen de AI-verordening worden AI-systemen in bepaalde risicocategorieën geclassificeerd. Op het voldoen aan de AI-verordening (en daarmee ook de juiste classificatie van AI-systemen) zal toezicht worden gehouden. Momenteel wordt aan de inrichting van het toezicht op de AI-verordening gewerkt. Voor uitgebreider antwoord over de inrichting van het toezicht op de AI-verordening verwijs ik u door naar het antwoord op vraag 12.

Vanuit mijn coördinerende rol als Staatssecretaris voor digitalisering kan ik (zoals uit het Besluit CIO stelsel volgt) monitoren en coördineren op de verantwoorde inzet van AI-systemen.

Vraag 4: Wie is er binnen departementen en uitvoeringsorganisaties verantwoordelijk voor het toezien op het acceptabele gebruik van AI-systemen?

De verantwoordelijkheden op het gebied van digitalisering en daarmee ook van AI zijn bij diverse functionarissen belegd. De functies van de Chief Information Officer (CIO) zijn vastgelegd in het CIO-stelsel. Bij veel ministeries en uitvoeringsorganisaties valt onder de CIO de verantwoordelijkheid voor de verantwoorde inzet van AI-systemen. Specifiek heeft de functionaris gegevensbescherming een rol als het gaat om de bescherming van persoonsgegevens en het toezicht op AI-systemen volgens de Algemene Verordening Gegevensbescherming (AVG).

Vraag 5: Mede gelet op het feit dat er in dit onderzoek geen AI-systemen zijn ontdekt met onaanvaardbare risico's in de zin van de Europese AI-verordening: zijn er concrete gevallen bekend waarbij het gebruik van AI als ondersteuning direct heeft geleid tot onaanvaardbare verwezenlijking van risico's?

Tot op heden zijn mij geen gevallen bekend van AI-systemen waarbij het gebruik van AI als ondersteuning direct heeft geleid tot onaanvaardbare verwezenlijking van risico's.

Vraag 6: In het rapport is niets terug te lezen over de inzet van optische tekenherkenning (OCR). Wat maakt dat OCR ontbreekt of niet in beeld is?

De Algemene Rekenkamer (AR) heeft dit onderzoek uitgevoerd op basis van een zelfassessment door ministeries met een korte doorlooptijd. Voor het ontbreken van bepaalde AI-systemen in het rapport verwijs ik naar de AR. Dat OCR niet genoemd wordt in het rapport, betekent niet dat de OCR niet in beeld is.

Vraag 7: Hoe gaat u waarborgen dat alle overheidsdepartementen zich er vóór 2 februari 2025 volledig van bewust zijn welke gebruikte algoritmen onder de AI-verordening vallen, welke

daarvan een onaanvaardbaar risico teweegbrengen en aan welke compliancy vereisten elk algoritme moet voldoen?

Vraag 8: Hoe gaat u waarborgen dat de AI-systemen met een nog onbekend risiconiveau juist geclassificeerd zijn vóór 2 februari 2025 en daarnaast tijdig aan de juiste compliancyvereisten voldoen?

Vraag 9: Hoe gaat u waarborgen dat alle onrechtmatige AI-systemen die binnen de overheid gebruikt worden, tijdig rechtmatig zijn dan wel buiten gebruik gesteld worden?

(Gecombineerd antwoord op vragen 7, 8 en 9)

Zoals in het antwoord op vraag 3 benoemd, worden per 2 februari 2025 de eerste bepalingen van de AI-verordening van kracht. Deze gaan over verboden AI-praktijken. De verantwoordelijkheid voor de juiste classificatie ligt bij de desbetreffende overheidsorganisatie. Aan overheden wordt door middel van handreikingen, een interdepartementale werkgroep, een spreekuur, en webinars hulp geboden bij het inventariseren en classificeren van AI-systemen die nu al of in de toekomst worden ingezet, zodat deze indien nodig tijdig kunnen worden aangepast of gestopt.

Vraag 10: Hoe gaat u waarborgen dat alle hoog-risico-AI-systemen tijdig geregistreerd staan in het openbare Algoritmeregister?

Ik stimuleer overheden, zowel binnen de Rijksoverheid als medeoverheden, om te publiceren. Daarvoor neem ik proactief contact op met overheden en help ik hen met verschillende instrumenten, zoals de handreiking algoritmeregister, templates van leveranciers, ondersteuning van een implementatieteam, zogenaamde aansluitsessies, een regiotour, een nieuwsbrief en artikelen met tips van organisaties die al gepubliceerd hebben. Verder hebben de departementen uw Kamer toegezegd ten minste hun hoog-risico AI-systemen voor eind 2025 in het Algoritmeregister te registreren. In de Jaarrapportage Rijk (JBR) 2024 zullen departementen inzicht verschaffen in de precieze voortgang. De uitvraag hiervoor gaat binnenkort via de CIO Rijk naar de departementen.

De JBR 2024 verschijnt in het voorjaar van 2025. Naast een terugblik op 2024 zal deze een vooruitblik bevatten voor de registraties door de Rijksoverheid die zullen volgen in 2025.

Vraag 11: Hoe gaat u waarborgen dat overheidsdepartementen het risico van AI-systemen niet te laag classificeren?

Zie hiervoor ook het antwoord onder vraag 9.

Op het voldoen aan de AI-verordening (en daarmee ook de juiste classificatie van AI-systemen) zal verder ook toezicht worden gehouden. Momenteel wordt aan de inrichting van het toezicht op de AI-verordening gewerkt. Voor een uitgebreider antwoord over de inrichting van het toezicht op de AI-verordening verwijs ik u door naar het antwoord op vraag 12.

Vraag 12: Heeft u, op basis van gesprekken met de relevante toezichthouders, het idee dat het toezicht op de AI-verordening per 2 februari 2025 op orde is? Kunt u dit onderbouwen?

De AI-verordening schrijft voor dat lidstaten op 2 augustus 2025 de toezichthouders moeten hebben aangewezen en moeten voorzien in passende sancties en handhavingsmaatregelen. Volgens de AI-verordening moeten toezichthouders dus uiterlijk 6 maanden na het ingaan van de bepalingen inzake verboden AI-praktijken (2 februari 2025) aangewezen worden. Op 2 augustus 2025 gaan ook de bepalingen rondom de AI-modellen voor algemene doeleinden in, waar het AI-bureau *(AI Office)* van de Europese Unie toezicht op houdt. Een jaar later, op 2 augustus 2026, gaan de eisen voor hoog-risico toepassingen en transparantie-verplichtingen in. Op 2 augustus 2027 gaan de eisen in voor hoog-risico AI als veiligheidscomponent van producten die reeds onder bestaande productregelgeving (onder andere medische apparatuur en machines) vallen en hoog-risico AI die op zichzelf een dergelijk product is. Voor hoog-risico AI-systemen die bij de overheid voor 2 augustus 2026 in gebruik zijn en geen significante wijziging ondergaan, geldt dat deze systemen uiterlijk 31 december 2030 in lijn met de AI-verordening moeten zijn gebracht.

Het aanwijzen van toezichthouders vereist formele uitvoeringswetgeving. AI wordt in veel sectoren gebruikt en de AI-verordening raakt aan diverse bestaande wetten. Dit betekent dat veel ministeries en toezichthouders betrokken zijn bij de inrichting van het toezicht op de AI-verordening en de uitvoeringswetgeving. Momenteel werken de betrokken ministeries onder leiding van EZ, BZK en JenV uit hoe het toezicht het beste kan worden ingericht. Daarbij wordt het advies van de toezichthouders over deze inrichting betrokken.

Naar verwachting is afronding van het wetgevingstraject voor 2 augustus 2025 niet mogelijk. Er is extra tijd nodig om tot zorgvuldige besluitvorming over de inrichting van het toezicht in afstemming met alle betrokkenen te komen en voor het doorlopen van alle stappen van het wetgevingsproces, waaronder alle verplichte raadplegingen en toetsen. Om deze reden heeft het kabinet tijdens de onderhandeling van de AI-verordening, helaas onsuccesvol, gepleit voor langere implementatietermijnen.

Dit betekent dat er op 2 augustus 2025 nog geen aangewezen toezichthouder voor de verboden AI is. Het betekent niet dat er niks gedaan kan worden tegen verboden AI-praktijken. De verboden zijn rechtstreeks van toepassing vanaf 2 februari 2025 en een overtreding van de AI-verordening op dit punt kwalificeert daardoor als een onrechtmatige daad. Burgers of ondernemingen die daardoor schade leiden, kunnen een procedure starten bij de burgerlijke rechter.

De ambitie van het kabinet is om zo snel mogelijk een besluit te nemen over de inrichting van het toezicht op de AI-verordening zodat de beoogde toezichthouders zich daarop kunnen voorbereiden. Toezichthouders kunnen hun toezichts- en handhavingsbevoegdheden echter pas uitoefenen nadat de benodigde uitvoeringswetgeving in werking is getreden.

Uiteraard voelen wij de urgentie om te komen tot een effectieve uitvoering van de AI-verordening in Nederland en zullen uw Kamer op de hoogte houden van de voortgang ervan

Vraag 13: Heeft u het idee dat het aan u verleende mandaat op bepaalde gebieden mogelijk tekort om uw coördinerende en kaderstellende taak op AI-gebruik binnen de Rijksoverheid effectief en krachtig uit te voeren?

Het uitvoeren van mijn coördinerende en kaderstellende taak omtrent AI-gebruik binnen de Rijksoverheid vergt meer dan alleen een bepaald mandaat. Om deze taak uit te voeren, dienen budget, capaciteit, stelselverantwoordelijkheid en mandaat in lijn te zijn met het benodigde beleid en kaders. Om dit te bereiken wordt gewerkt aan een herijking van het CIO-stelsel. Tegelijkertijd ligt de uiteindelijke verantwoordelijkheid voor AI-gebruik binnen de Rijksoverheid bij de Ministers van de betreffende departementen.

Verder geldt dat het gehele stelsel van partijen/instrumenten als de Auditdienst Rijk, de Algemene Rekenkamer, de Jaarrapportage Bedrijfsvoering Rijk, de werking van de CIO-offices, de controlerende taak van de Tweede Kamer en het nog in te richten toezicht op de AI-verordening, ertoe moeten leiden dat we met elkaar onze taken goed vervullen. Mijn coördinerende en kaderstellende taken voer ik daarbij uit op de manier zoals verwoord in het antwoord op vraag 2.

Vraag 14: Hoe verklaart u het zeer geringe aantal AI-systemen die zijn geregistreerd in het Algoritmeregister?

Zoals de AR opmerkt in het rapport, hoeven niet alle AI-systemen die zij opgevraagd heeft in het Algoritmeregister te worden geregistreerd. Bijvoorbeeld als het gaat om een experiment dat geen impact heeft (gehad) op burgers of bedrijven, of als de impact van een AI-systeem met name indirect is. Op basis van het rapport is het daarom lastig in te schatten welk percentage te registreren AI-systemen ontbreekt.

Mij is bekend dat veel overheden bezig zijn met de vulling van het register, maar dat het inventariseren, beoordelen en registreren van AI-systemen tijd en capaciteit vraagt. Zoals in vraag 10 toegelicht, hebben alle departementen toegezegd ten minste de hoogrisico AI-systemen eind 2025 geregistreerd te hebben. In de JBR zullen departementen inzicht verschaffen in de precieze voortgang.

Vraag 15: Kunt u de verwachting dat per eind 2025 alle impactvolle AI-systemen geregistreerd zijn onderbouwen? Is het huidige tempo waarop systemen geregistreerd worden daartoe toereikend?

Zoals aangegeven bij het antwoord op vraag 10, hebben alle departementen toegezegd uiterlijk eind 2025 hun hoogrisico AI-systemen in de zin van de AI-verordening in het algoritmeregister te publiceren.

Vraag 16: Hoe verklaart u het relatief hoge gebruik van AI-toepassingen bij de Ministeries van Justitie en Veiligheid en Asiel en Migratie?

Er is geen eenduidige verklaring voor het feit dat organisaties binnen de Ministeries van Justitie en Veiligheid (JenV) en Asiel en Migratie (AenM) relatief veel AI-systemen hebben doorgegeven aan de Algemene Rekenkamer. Een mogelijke verklaring kan zijn dat binnen het domein van JenV en AenM een grote hoeveelheid aan uitvoeringsorganisaties bestaat, met een omvangrijke taakuitvoering.

Vraag 17: Hoe verklaart u het relatief hoge gebruik van AI-toepassingen bij de Ministeries van Economische Zaken, Klimaat & Groene Groei, en Landbouw, Visserij, Voedselzekerheid en Natuur?

Bij de Ministeries van Economische Zaken, Klimaat en Groene Groei en Landbouw, Visserij, Voedselzekerheid en Natuur lijken er relatief meer AI-systemen te zijn, omdat deze departementen onder hetzelfde CIO-Office vallen. Hierdoor kan de indruk ontstaan dat er meer AI-systemen worden gebruikt, terwijl de aangegeven hoeveelheid betrekking heeft op drie ministeries. Het merendeel van de genoemde toepassingen binnen LVVN zijn experimenten of verkenningen zonder dat er uitvoerende stappen zijn ondernomen. Deze experimenten zijn door de Algemene Rekenkamer als lopend aangemerkt, maar het aantal feitelijk gebruikte AI-systemen binnen LVVN ligt lager dan in het rapport staat. Er zijn op basis hiervan geen indicaties dat er per departement meer AI-systemen worden gebruikt dan gemiddeld.

Vraag 18: Hoe verklaart u het relatief hoge gebruik van AI-toepassingen bij het Ministerie van Infrastructuur en Waterstaat?

Het Ministerie van IenW is een proactieve en innovatieve speler op het gebied van data- en informatiegestuurd werken en digitale innovaties, waaronder AI. Voor IenW zijn de kansen die AI biedt voor de aanpak van de maatschappelijke opgaven belangrijk. Zeker ook omdat IenW een ministerie is met een belangrijke en grote uitvoeringskant en inspectie waar AI mogelijkheden biedt om slimmer te werken en effectiever uit te voeren. Daarbij moet worden opgemerkt dat voorafgaand aan de huidige grote aandacht voor AI onderdelen van IenW, zoals KNMI en RWS, AI al jaren gebruikten.

Vraag 19: Hoe verklaart u het relatief hoge gebruik van AI-toepassingen bij het Ministerie van Sociale Zaken en Werkgelegenheid?

De sociale zekerheid omvat onder andere twee grote uitvoerders (de ZBO's UWV en SVB) en een inspectie (NLA). Binnen de sociale zekerheid werkt UWV aan relatief veel AI-toepassingen. Voor UWV speelt daarbij een rol dat het een grote uitvoeringsorganisatie is, die veel belang heeft bij optimale automatisering van uitvoeringstaken vanwege de grote hoeveelheid administratieve taken, en dat UWV al vanaf het begin betrokken is bij transparantie-initiatieven zoals het Algoritmeregister.

Verder maakt de ARK in zijn rapportage geen onderscheid tussen hoog risico-AI-toepassingen en AI-toepassingen met beperkt risico die worden ingezet voor de interne bedrijfsvoering. Het aantal AI-toepassingen dat op dit moment bij UWV daadwerkelijk wordt ingezet bij de dienstverlening aan cliënten is vier.

Vraag 20: Wat zegt het geringe aantal geregistreerde AI-systemen over de werkbaarheid van het Algoritmeregister?

Mij zijn geen signalen bekend dat er problemen zijn met de werkbaarheid van het algoritmeregister. Zoals aangegeven bij het antwoord op vraag 10, doen we veel om overheden hierbij te ondersteunen. Graag verwijs ik hier ook naar het antwoord bij vraag 14.

Vraag 21: Kunt u alle AI-systemen in gebruik van de politie uiteenzetten, inclusief lopende en beëindigde experimenten? Kunt u hierbij aangeven wat het doel is van deze systemen?

Voor wat betreft de publicatie van algoritmes maakt de Rijksoverheid gebruik van het Algoritmeregister. Met uw Kamer is afgesproken dat voor zover het de Rijksoverheid betreft, ten minste alle hoog-risico AI-systemen

eind 2025 in het Algoritmeregister worden gepubliceerd. Dat geldt ook voor de politie. In algemene zin wordt gebruik gemaakt van AI-toepassingen die het werk van politiemedewerkers ondersteunen. Het gaat bijvoorbeeld om het doorzoekbaar maken van beeld- en audiomateriaal, zoals het zoeken naar objecten in afbeeldingen of het omzetten van audiobestanden naar tekst.

Vraag 22: Kunt u alle AI-systemen in gebruik bij het Uitvoeringsinstituut Werknemersverzekeringen (UWV) uiteenzetten, inclusief lopende en beëindigde experimenten? Kunt u hierbij aangeven wat het doel is van deze systemen?

UWV heeft een actuele lijst voor AI-toepassingen die continu wordt bijgewerkt. Uit deze lijst zijn inmiddels drie van de tien aan de Rekenkamer gemelde AI-toepassingen geschrapt, omdat de daarin opgenomen AI-componenten buiten gebruik zijn gesteld – in alle gevallen ging het om AI-componenten van veel gebruikte software van derden, zoals JIRA, Confluence en Trello. Sindsdien zijn er wel weer twee nieuwe toepassingen met een AI-component in gebruik genomen.

De vier AI-toepassingen die UWV inzet bij de dienstverlening aan cliënten zijn opgenomen in het Algoritmeregister van de Nederlandse Overheid. De overige toepassingen worden gebruikt voor de interne bedrijfsvoering, denk aan het anonimiseren van documenten bij Woo-verzoeken. In de meeste gevallen gaat het dan om AI-componenten van veelgebruikte software als Microsoft Defender.

AI biedt voortdurend nieuwe mogelijkheden om zowel onze dienstverlening als onze bedrijfsvoering te verbeteren. Experimenten leren ons hoe we AI op een verantwoorde manier kunnen inzetten en worden gedaan in beveiligde omgevingen. Op dit moment loopt er een vijftiental experimenten. In de meeste gevallen gaat het om toepassingen om interne documentatie om eigen kennisbanken beter toegankelijk te maken, maar in twee gevallen ook om het matchen van vacatures en cv's op basis van skills.

Een tiental experimenten heeft UWV, deels al langer geleden, beëindigd, omdat deze niet blijvend kunnen voldoen aan de strenge voorwaarden die we stellen, of de beoogde resultaten niet behaald worden. Het gaat daarbij om zeer verschillende toepassingen, variërend van het herkennen van medische termen in dossiers tot het beter doorzoekbaar maken van het elektronisch archief.

Vraag 23: Vindt u het gebruik van sommige categorieën AI-systemen meer of minder wenselijk dan andere categorieën? Kunt u aangeven welke van de negen categorieën u het meest en het minst wenselijk vindt?

Of het gebruik van een bepaalde categorie AI-systemen wenselijk is hangt af van de specifieke toepassing, de context, de tijdelijkheid en of de juiste afwegingen zijn gemaakt. Voor het maken van de juiste afwegingen wordt in het Algoritmekader een basis gelegd. Daarnaast worden AI-systemen binnen de AI-verordening in bepaalde risicocategorieën geclassificeerd. Daar staan we als kabinet achter.

Vraag 24: Aan welke categorieën AI-systemen kleven de meeste risico's? Gaat u de meer risicovolle categorieën versneld toevoegen aan het Algoritmeregister?

Het is lastig te zeggen aan welke categorie de meeste risico's kleven, omdat de context en risicoafweging bepalend zijn en niet alleen het systeem. De afspraak is dat eind 2025 ten minste alle hoog-risico AI-systemen (in de zin van de AI-verordening) die in gebruik zijn bij de Rijksoverheid geregistreerd zijn in het Algoritmeregister. Deze hoog-risico AI-systemen worden dus inderdaad met prioriteit toegevoegd aan het Algoritmeregister.

Vraag 25: In het rapport valt op bladzijde 17 bij figuur 8 onder de toepassingscategorie «Kennisverwerking» te lezen «Gesproken tekst omzetten naar geschreven tekst» en onder de toepassingscategorie «Democratisch Proces» staat «Kamerdebatten transcriberen». Transcriptie is het een op een omzetten van gesproken tekst naar geschreven tekst. Vanwaar deze splitsing?

Voor vragen over de keuzes in de categorisering verwijs ik u naar de Algemene Rekenkamer. De splitsing is niet door mij gekozen.

Vraag 26: Bent u bekend met de 82 toepassingen van AI op het gebied van inspectie en handhaving? Op welke termijn worden deze volledig opgenomen in het Algoritmeregister?

Ik ben bekend met het feit dat AI wordt ingezet op het gebied van inspectie. Indien het hoog-risico AI-systemen binnen de Rijksoverheid betreft, worden deze systemen uiterlijk eind 2025 in het Algoritmeregister opgenomen. Indien het geen hoog-risico AI-systemen betreft, raad ik Rijksorganisaties nog steeds aan deze te registreren.

Vraag 27: Kunt u uitleggen waarom de Dienst Justitiële Inrichtingen (DJI) een robothond nodig heeft? Hoe duur was de robothond?

DJI verkent de mogelijkheden van innovaties om de maatschappelijke opgave van DJI verder te kunnen verbeteren. In het geval van de robothond onderzoekt DJI in hoeverre een robothond de effectiviteit en efficiëntie van een celinspectie kan vergroten. De innovatiepilot loopt nog en duurt waarschijnlijk nog 2 jaar. DJI heeft de robothond niet zelf aangeschaft, maar heeft de robot ingezet voor de innovatiepilot. De verhuur van de robothond loopt via onderzoeksorganisatie TNO. De huur van de robothond kost € 7.500 per jaar.

Vraag 28: Kunt u uitleggen welke AI-systemen worden gebruikt voor opsporing?

Ik verwijs naar mijn antwoord op vraag 21.

Vraag 29: Op welke termijn worden alle AI-systemen met directe impact in het Algoritmeregister opgenomen om de transparantie van de inzet te vergroten?

Voor zover het hoog-risico AI-systemen binnen de Rijksoverheid betreft, is er de afspraak dat deze eind 2025 geregistreerd dienen te zijn. Voor meer informatie verwijs ik u naar de beantwoording van vraag 10.

Vraag 30: Worden burgers actief geïnformeerd over AI-systemen met directe impact die gebruikt worden in processen die hen aangaan? Welke regels zijn er over proactieve transparantie over het gebruik van AI?

De AI-verordening verplicht gebruikers bij het gebruik van hoog-risico AI-systemen voor besluitvorming, de daardoor geraakte natuurlijke persoon hierover te informeren. Daarnaast heeft de natuurlijke persoon een recht op uitleg bij de inzet van bepaalde hoog-risico AI-toepassingen.

In het regeerprogramma staat verder dat het kabinet werk maakt van transparantie over het gebruik van AI en algoritmes. Het gaat hier om transparantie, zodat burgers kunnen weten hoe een besluit met algoritmes tot stand is gekomen. Momenteel wordt nader bezien hoe hier invulling aan kan worden gegeven.

Vraag 31: Is er in alle 140 AI-systemen met directe impact sprake van menselijke tussenkomst? Hoe wordt hier toezicht op gehouden?

Als coördinerend bewindspersoon heb ik geen inzicht in alle specifieke AI-toepassingen en op welke wijze deze worden ingezet. Door het algoritmeregister en het algoritmekader, ondersteun ik overheden wel bij de verantwoorde inzet van AI. Als het gaat om hoogrisico AI-systemen, schrijft de AI-verordening voor dat door mensen wordt toegezien op de juiste werking van het systeem.

Ook de Algemene Verordening Gegevensbescherming (AVG) kent in artikel 22 rechten toe aan betrokkenen met betrekking tot menselijke tussenkomst. In dat kader ligt het toezicht bij de Autoriteit Persoonsgegevens (AP). Voor wat betreft het toezicht op AI-verordening, verwijs ik u naar het antwoord onder vraag 12.

Vraag 32: Is het juridisch houdbaar om als overheid generatieve AI te gebruiken als deze getraind is op data die verkregen is op illegale wijze, zoals door het schenden van privacy- of auteursrechten via «scraping»?

In reactie op eerdere Kamervragen heeft het (vorige) kabinet aangegeven dat de veronderstelling niet zondermeer klopt, dat het trainen van generatieve AI met van het internet gescrapete[2] data niet is toegestaan.[3] De Auteurswet bevat een uitzondering voor tekst- en datamining (artikel 15o), zoals bepaald in artikel 4 van Richtlijn (EU) 2019/790 inzake auteursrechten in de digitale eengemaakte markt. Onder «tekst- en datamining» wordt verstaan: een geautomatiseerde analysetechniek die gericht is op de ontleding van tekst en gegevens in digitale vorm om informatie te genereren, zoals, maar niet uitsluitend, patronen, trends en onderlinge verbanden. Naar de letter kan daaronder ook het trainen van generatieve AI vallen. Het maken van een reproductie van een werk van letterkunde, wetenschap of kunst is toegestaan voor tekst- en datamining. Dit geldt indien er rechtmatige toegang tot het werk is en de makers of hun rechtverkrijgenden dit niet uitdrukkelijk hebben verboden. Dit verbod kan bijvoorbeeld via machinaal leesbare middelen bij een online beschikbaar werk worden aangegeven. Scrapen is toegestaan, wanneer de voornoemde voorwaarden worden gerespecteerd. Anders levert scrapen een inbreuk op het auteursrecht op. Dat is echter niet zonder meer het geval.

Daarnaast bestaan er zorgen over de naleving van gegevensbeschermingswetgeving bij de totstandkoming van AI-systemen.

---

[2] Onder scrapen wordt verstaan het automatisch verzamelen en opslaan van informatie van het internet door middel van software.

[3] *Kamerstuk* 26 643, nr. 1202.

De situatie is complex vanwege de nieuwe en snel ontwikkelende aard van AI-technologie. Daarom herzie ik momenteel het voorlopig standpunt over generatieve AI bij de (Rijks)overheid[4].

Vraag 33: Kunt u garanderen dat de overheid geen AI-systemen gebruikt die getraind zijn op illegaal verkregen data?

Als overheid willen wij op een verantwoorde manier omgaan met data. Illegaal verkregen data voldoen niet aan onze voorwaarden. Desondanks bestaan er, ook bij de Autoriteit Persoonsgegevens, zorgen over de naleving van privacywetgeving en auteursrecht bij de totstandkoming van AI-systemen. De nieuwe en zich snel ontwikkelende aard van AI-technologie maakt dit tot een complex vraagstuk. Daarom herzie ik momenteel het voorlopige standpunt over generatieve AI.[5]

Vraag 34: Hoe toetst u de kwaliteit van de trainingsdata voor AI-systemen van de overheid? Onder welke voorwaarden acht u de kwaliteit acceptabel?

Voor AI-systemen met een hoog risico bevat de AI-verordening specifieke vereisten met betrekking tot onder meer de kwaliteit van de gebruikte data, technische documentatie, transparantie en menselijk toezicht. In dat geval moet worden aangegeven wat de herkomst, reikwijdte en belangrijkste kenmerken van de betreffende dataset zijn en hoe de data is verkregen en geselecteerd. De aangewezen toezichthouder heeft de bevoegdheid om deze documentatie in te zien.

Daarnaast bevat de AI-verordening eisen voor AI-modellen die in staat zijn om veel verschillende taken uit te voeren en die in diverse AI-systemen kunnen worden geïntegreerd. Dit wordt aangeduid als «AI-modellen voor algemene doeleinden». Op deze vorm van AI zal Europees toezicht plaatsvinden. Aanbieders van deze modellen zijn verplicht om informatie over de werking van het model te delen met ontwikkelaars die op dit model voortbouwen. Ook moet duidelijk worden gemaakt hoe het auteursrecht wordt gerespecteerd en dat alle door AI gegenereerde content als zodanig wordt gemarkeerd. Deze eisen dragen eraan bij dat beter inzichtelijk wordt welke content tot stand is gekomen met AI en mogelijk onzeker, fout of ongeverifieerd is[6].

Vraag 35: Gebruikt de overheid generatieve AI-systemen die getraind zijn op illegaal verkregen data? Met hoeveel zekerheid kunt u dit zeggen?

Ik verwijs u naar mijn antwoord op vraag 33.

Vraag 36: Kunt u in brede zin uitleggen waarom de zestien beëindigde experimenten met generatieve AI geen doorgang vonden?

Experimenten kunnen om verschillende redenen worden stopgezet. Redenen om een dergelijk experiment stop te zetten kunnen bijvoorbeeld zijn een gebrek aan effectiviteit, minimale kennis en ervaring bij de inzet of het niet in lijn zijn met het voorlopig Rijksbrede standpunt op generatieve AI.

---

[4] Kamerstuk 26 643, nr. 1098.
[5] Kamerstuk 26 643, nr. 1098.
[6] Kamerstuk 26 643, nr. 1202

Vraag 37: In hoeveel van de bij u bekende generatieve AI-toepassingen is het doel om beelden of video's te genereren?

Het is bij mij bekend dat communicatieafdelingen het potentieel van generatieve AI zien en hier graag mee experimenteren. Deze experimenten bevinden zich bij mijn weten nog niet in de toepassingsfase. Een juiste risicoanalyse vind ik daarbij van groot belang.

Vraag 38: Kunnen burgers er op vertrouwen dat teksten, beelden en video's in openbare uitingen van de overheid altijd door een mens zijn gemaakt en geen auteursrechten schenden?

Het is van belang dat wanneer de overheid op generatieve AI inzet, dit op een verantwoorde manier gebeurt. Daar hoort ook het voldoen aan wettelijke regels, waaronder het auteursrecht, toe. De overheid streeft altijd naar het zorgvuldig omgaan met deze regels. Daarnaast geldt het voorlopig standpunt generatieve AI, dat ik momenteel herzie. Ook geldt het Beeldkompas, dat inhoudt dat beelden en video's van de Rijksoverheid een realistische kijk op de Nederlandse samenleving moeten bieden, waarbij de kenmerken geloofwaardigheid en herkenbaarheid gelden.

Vraag 39: Is er een plicht om burgers te informeren als de overheid gegenereerde inhoud gebruikt in openbare uitingen? Ziet u hier noodzaak toe?

In het geval dat de overheid gegenereerde inhoud gebruikt in openbare uitingen, volgt uit artikel 50 van de AI-verordening voor aanbieders van dergelijke AI-systemen de verplichting dat door AI gegenereerde inhoud wordt gemarkeerd (in een machineleesbaar formaat) en op die manier detecteerbaar is als kunstmatig gegenereerd of gemanipuleerd. Daarnaast geldt voor gebruiksverantwoordelijken die een AI-systeem gebruiken om content zoals deep fakes te genereren de verplichting om duidelijk kenbaar te maken dat de content kunstmatig is gecreëerd of gemanipuleerd.

Vraag 40: Kunt u garanderen dat alle lopende experimenten en in gebruik genomen generatie AI-toepassingen strikt intern gebruikt worden?

Op dit moment bestaat er geen beleid dat generatieve AI alleen intern gebruikt mag worden. Wel bestaat er het voorlopig standpunt voor Rijksorganisaties bij het gebruik van generatieve AI, welke op dit moment wordt herzien. Dit punt kan daarin mee worden genomen. Daarnaast wordt er gewerkt aan een overheidsbrede handreiking, waarin richtlijnen staan over verantwoord gebruik van generatieve AI.

Vraag 41: Is er beleid voor het gebruik van AI in het schrijven of maken van publieke uitingen door de Rijksoverheid? Zo ja, hoe wordt dit beleid gehandhaafd?

Op dit moment is er het voorlopig standpunt voor Rijksorganisaties bij het gebruik van generatieve AI, welke op dit moment wordt herzien. Ook wordt er gewerkt aan een overheidsbrede handreiking, waarin richtlijnen staan over verantwoord gebruik van generatieve AI. Daarnaast gelden vanuit de AI-verordening transparantieverplichtingen. Zie ook het antwoord bij vraag 39.

Vraag 42: Kunt u de meerwaarde uitleggen van AI-systemen waarvan de gebruikers zelf niet kunnen beoordelen of ze naar behoren presteren?

Het is net als bij ieder IT-systeem de verantwoordelijkheid van de organisatie om een proces in te richten om de kwaliteit van het systeem te blijven controleren. Op grond van de AI-verordening heeft de gebruiksverantwoordelijke van een hoog-risico AI-systeem bovendien de verplichting om na ingebruikname te beoordelen of het AI-systeem naar behoren functioneert. Dat kan de gebruiker zelf doen, maar ook laten doen.

Vraag 43: Is het verplicht dat AI-systemen in gebruik van de overheid aantoonbaar goed functioneren?

Ja. Afhankelijk van de risicocategorie waarin een AI-systeem volgens de AI-verordening is onverdeeld, gelden zwaardere of minder zware regels. Voor hoog-risico AI-systemen moet een conformiteitsbeoordeling zijn uitgevoerd voordat deze systemen op de markt zijn gebracht of in gebruik zijn genomen. Hierbij horen strikte eisen, waarvan de aanbieder moet zorgen dat het systeem daaraan voldoet. Denk bijvoorbeeld aan het uitvoeren van een risicoanalyse, zorgen voor menselijk toezicht en het opstellen van technische documentatie. Het doel van deze eisen is om ervoor te zorgen dat een hoog-risico AI-systeem betrouwbaar is en goed functioneert in de context van de toepassing waarvoor het is ontwikkeld. In de openbare EU databank moeten aanbieders vervolgens bepaalde informatie over het hoog-risico AI-systeem opnemen, waaronder een EU-conformiteitsverklaring en een elektronische gebruiksaanwijzing. Op verzoek van markttoezichtautoriteiten geven aanbieders toegang tot de documentatie en de datasets.

Vraag 44: Kunt u het smaldeel in gebruik genomen AI-systemen die slechter presteren dan verwacht toelichten?

Nee. Ik heb geen inzicht in de informatie die door de ARK is verzameld.

Vraag 45: Is het uw intentie om AI-systemen die slechter functioneren dan verwacht met meer urgentie op te nemen in het Algoritmeregister?

Ik zet mij ervoor in dat AI-systemen die als hoog-risico volgens de AI-verordening kunnen worden getypeerd of anderszins impact hebben op burgers of bedrijven, of ze nu wel of niet goed functioneren, in het algoritmeregister worden opgenomen.

Vraag 46: s er een standaard methodiek voor het beoordelen van wenselijk AI-gebruik door afdelingen Juridische Zaken?

Nee, die is er niet. De afweging van wenselijkheid van AI-gebruik vindt bij verschillende Rijksorganisaties plaats op een contextafhankelijke wijze. Deze afweging moet vanuit verschillende perspectieven worden gemaakt, waaronder het juridisch perspectief. Als er juridische vragen zijn bij de inzet van AI, dan worden juridische afdelingen hierbij betrokken.

Vraag 47: Is het advies van een afdeling Juridische Zaken over de inzet van AI bindend?

Eventuele adviezen vanuit juridische afdelingen over de juridische implicaties van AI worden altijd serieus behandeld. Uiteindelijk komen alle adviezen over de inzet van AI-systemen samen op de bestuurstafel. Hier wordt vervolgens een besluit over genomen.

Vraag 48: Binnen welke kaders moeten experimenten met AI plaatsvinden? Is dat standaard in een beveiligde omgeving en buiten primaire processen om?

Ook tijdens het experimenteren met AI moet worden voldaan aan geldende wet- en regelgeving. Het Algoritmekader voorziet in een handzaam overzicht van alle protocollen en kaders voor zover die relevant zijn voor het AI-gebruik (en ook het experimenteren met AI-systemen).

Vraag 49: Kunt u nader toelichten waarom wet- en regelgeving genoemd wordt als belemmerende factor in het toepassen van en experimenteren met AI?

Vraag 50: Kunt u nader toelichten waarom verantwoording afleggen over de systemen die de overheid gebruikt wordt gezien als belemmerend?

(Gecombineerd antwoord op vragen 49 en 50)

Bij de inzet van AI dient vanzelfsprekend te worden voldaan aan de wet- en regelgeving. Daarbij valt te denken aan, naast sectorale wetgeving, aan de AI-verordening, de Algemene Verordening Gegevensbescherming, de Auteurswet, de Baseline Informatiebeveiliging Overheid en de Archiefwet. Het voldoen aan alle geldende wet- en regelgeving vereist kennis, expertise, transparantie en verantwoording, hetgeen in de uitvoering als een behoorlijke last kan worden ervaren, omdat bij de systeemtechnologie van AI al deze disciplines voor het eerst bij elkaar komen.

Deze last staat tegenover een rap veranderende samenleving die steeds directer en sneller vraagt om resultaten, en waar AI op kan inspelen. Deze verhouding wordt als belemmerend ervaren omdat een zware verantwoordingslast en snel resultaat contrair aan elkaar kunnen zijn.

Vraag 51: In het rapport staat op bladzijde 23: «In een eerdere brief aan de Tweede Kamer wezen wij al op obstakels die overheidsorganisaties ervaren door de interpretatie van privacyregels.» Welke stappen zijn er genomen inzake dit probleem, waarvoor de Autoriteit Persoonsgegevens (AP) al met enige regelmaat door de Europese Commissie (EC) op de vingers werd getikt?

In de brief van de ARK waarnaar op p. 23 wordt verwezen, wijst de ARK op het belang van een goede omgang met de AVG door uitvoeringsorganisaties, omdat in de dagelijkse praktijk er momenteel niet altijd voldoende kennis aanwezig is om de ruimte te benutten die de AVG biedt.

Door het vorige kabinet is dit onderkend. In de beleidsreactie d.d. 28 juni 2024 op het WODC-rapport naar de naleving van de AVG door overheden[7], worden verschillende, veelal reeds lopende maatregelen genoemd om de toepassing van de AVG binnen overheden te verbeteren.

Allereerst worden verdere stappen gezet ter versterking van privacykennis en de vergroting van AVG-bewustzijn op besluitvormend niveau door middel van opleidingen van de Algemene Bestuursdienst (ABD).

Ten tweede is er het Kenniscentrum van de Interbestuurlijke Datastrategie (IBDS), dat onder meer een «Toolbox verantwoord datagebruik», een wegwijzer voor Privacy Enhancing Technologies (PET's) en een keuzehulp voor dataopleidingen biedt. Ook zijn er maatregelen om de rol van de functionaris voor gegevensbescherming te versterken en borgen, waardoor privacy-gerelateerde obstakels worden verminderd.

---

[7] *Kamerstuk* 32 761, nr. 304.

Ten derde is in het beleidskompas vroegtijdige betrokkenheid van uitvoeringsorganisaties gewaarborgd bij de ontwikkeling van nieuwe wet- en regelgeving, met specifieke aandacht voor uitvoerbaarheid en impact op ICT.

Ten slotte ondersteunt de overheid AI-ontwikkeling door subsidies en deelname aan de Nederlandse AI Coalitie, waaronder het AiNed-programma, dat Nederlandse bedrijven en publieke instellingen bij AI-projecten helpt.

Vraag 52: Kunt u uitleggen waarom er ondanks de ervaren verantwoordingslast vooralsnog slechts vijf procent van AI-systemen in het Algoritmeregister staat?

Ik verwijs u naar mijn antwoord op vraag 10.

Vraag 53: Waarom gebruikt de overheid AI-systemen die onder de AI-verordening mogelijk verboden worden of aan strengere eisen moeten voldoen?

De AI-verordening wordt gefaseerd van kracht, en op 2 februari 2025 gaan de bepalingen over de verboden praktijken gelden. Dat betekent dat per 2 februari 2025 dergelijke AI-praktijken niet meer zijn toegestaan. Dit zijn AI-praktijken die mensen schade toebrengen. Het ligt niet voor de hand dat overheden bewust dergelijke AI-praktijken hanteren. Als dat al gebeurt, zou dat ook zonder AI-verordening moeten worden gestaakt.

Aan hoog-risico AI-systemen worden striktere eisen gesteld. Deze eisen zijn er op gericht om mogelijke risico's voor de gezondheid, veiligheid of schending van fundamentele rechten tegen te gaan. Deze bepalingen gaan vanaf 2 augustus 2026 gelden voor hoog-risico AI-systemen die vanaf die datum op de markt worden gebracht of in gebruik worden gesteld. Hoog-risico AI-systemen die voor 2 augustus 2026 op de markt zijn gebracht of in gebruik worden gesteld vallen buiten de toepassing van de AI-verordening, behalve als deze systemen een significante wijziging ondergaan. Voor hoog-risico AI-systemen die bij de overheid voor 2 augustus 2026 in gebruik zijn en geen significante wijziging ondergaan, geldt dat deze systemen uiterlijk 31 december 2030 in lijn met de AI-verordening moeten zijn gebracht.

Zie ook het antwoord bij vraag 10.

Vraag 54: Kunt u inschatten welk aandeel van AI-systemen die nu in gebruik zijn verboden zullen worden onder de AI-verordening? Op welke termijn worden deze buiten gebruik gesteld?

De Rijksoverheid en medeoverheden wordt door middel van handreikingen, een interdepartementale werkgroep, een spreekuur, en webinars hulp geboden bij het inventariseren van verboden AI-praktijken, zodat deze indien nodig tijdig kunnen worden gestaakt. De verantwoordelijkheid van juiste inventarisatie, classificatie en het staken van verboden AI-praktijken ligt bij de desbetreffende overheidsorganisatie.

Vraag 55: Op welke manier bent u als coördinerend bewindspersoon betrokken bij het opstellen van intern beleid en richtlijnen voor de ontwikkeling en toepassing van AI?

Ik verwijs u naar mijn antwoord op vraag 2.

Vraag 56: Welke risico's heeft het ontbreken van een specifiek risicomanagementbeleid gericht op AI? Kan bestaande privacy- en cyberveiligheidsbeleid een-op-een toepasbaar zijn?

Het ontbreken van risicomanagementbeleid kan ervoor zorgen dat aan de voorkant van de ontwikkeling van een AI-systeem onvoldoende risico's op bijvoorbeeld grondrechten en veiligheid in kaart worden gebracht, maar ook dat tijdens het gebruik incidenten kunnen ontstaan. Het ontbreken van risicomanagementbeleid kan er bijvoorbeeld voor zorgen dat de trainingsdata van een AI-systeem vooroordelen bevat, wat tot discriminatie kan leiden.

Zeker bij complexere AI-systemen is de werking veelal niet echt uit te leggen. Dan heb je risicomanagement nodig om bijvoorbeeld onlogische beslissingen te kunnen corrigeren. De risico's kunnen velerlei zijn. Ervan uitgaand dat het systeem zelf correct werkt, moet ook geborgd worden dat de wijze waarop het systeem ingezet wordt en door wie het gebruikt wordt, voldoet aan de voorschriften. Vaak zal een overheidsorganisatie een AI-systeem nog verder moeten trainen met de eigen data. Het is heel goed mogelijk dat het bestaande privacy beleid en cybersecuritybeleid van die organisatie daarvoor aangepast en meer toegespitst moet worden.

De AI-verordening verplicht de aanbieder bij de ontwikkeling van een hoog-risico AI-systeem een systeem voor risicobeheer op te zetten, met als doel risico's voor de gezondheid, veiligheid en grondrechten vast te stellen, te analyseren en evalueren, en vervolgens gepaste en gerichte risicobeheersmaatregelen te treffen. Daarnaast moeten overheidsorganisaties als gebruiksverantwoordelijken voor het gebruik van een hoog-risico AI-systeem een beoordeling maken van de gevolgen voor de grondrechten voor de specifieke toepassing waarvoor dat AI-systeem wordt gebruikt.

Naast de AI-verordening, blijft toepasselijke wet- en regelgeving geldig, waardoor ook de juiste privacy maatregelen moeten worden getroffen. Voor wat betreft cybermaatregelen is de Baseline Informatiebeveiliging Overheid Cybersecurity (BIO) van toepassing op alle overheidsinstanties. Deze ziet specifiek op risicomanagement in verhouding tot informatiebeveiliging. Risicoafwegingen die in dit kader worden gedaan zijn dan ook niet één op één toepasbaar op AI-systemen.

Vraag 57: Is het maken van een risicoafweging een randvoorwaarde voor het inzetten van AI binnen de overheid?

Ja. Zoals aangegeven in de antwoorden op vragen 56 en 63 is het straks verplicht om voor hoog-risico AI-systemen de risico's af te wegen onder de AI-verordening. Vooruitlopend op de AI-verordening en ook voor AI-systemen die niet als hoog risico worden gecategoriseerd bestaan er al verschillende instrumenten om een dergelijke risicoafweging te maken, bijvoorbeeld de Impact Assessment Mensenrechten en Algoritmen (IAMA).

Vraag 58: Onder welke voorwaarden zijn de risico's bij het gebruiken van een AI-systeem klein genoeg om deze binnen de overheid te mogen toepassen?

Alle AI-systemen moeten voldoen aan geldende wet- en regelgeving, ook de systemen met beperkte risico's.

Vraag 59: Moeten AI-systemen waarvan de risico's onbekend zijn per direct worden stopgezet totdat er wel een risicoafweging is gemaakt? Kunt u toelichten waarom wel of niet?

Als de risico's niet bekend zijn dient er een risicobeoordeling plaats te vinden. Aan de hand van de uitkomsten daarvan moet een besluit worden genomen om het AI-systeem al dan niet gedeeltelijk en/of tijdelijk te stoppen.

Vraag 60: Wat is uw reactie op het feit dat van 46 procent van de AI-systemen waarmee wordt geëxperimenteerd of dat wordt gebruikt niet bekend is welke risico's hiermee gemoeid zijn?

Vraag 61: Hoe kunnen de 81 AI-systemen zonder risicoafweging hier zo snel mogelijk wel van worden voorzien?

Vraag 62: Hoe kunt u zo snel mogelijk van de 74 AI-systemen waarvan het onbekend is of er een risicoafweging is gemaakt achterhalen of dit wel is gebeurd?

(Gecombineerd antwoord op vragen 60, 61 en 61)

Ik heb geen inzicht in de informatie die door de ARK is verzameld. Of en in welke mate risicoanalyses hebben plaatsgevonden, is mij niet bekend. Wel weet ik dat het focusonderzoek van de ARK een momentopname is geweest aan de hand van een eerste zelfassessment. Dit assessment is door organisaties binnen beperkte tijd uitgevoerd.

Ik vind het van belang dat bij de inzet van AI-systemen tijdig een risicoafweging plaats vindt. Instrumenten als het eerdergenoemde IAMA maar ook het Algoritmekader ondersteunen overheidsorganisaties daarbij.

Vraag 63: Waar moet een geldige risicoafweging voor het gebruiken van een AI-systeem aan voldoen?

Vanuit de AI-verordening worden eisen gesteld aan een geldige risicoafweging. Zowel de aanbieder als de gebruiksverantwoordelijke overheidsorganisatie van een hoog-risico AI-systeem moeten in verschillende mate een risicoanalyse uitvoeren. De AI-verordening verplicht de aanbieder bij de ontwikkeling van een hoog-risico AI-systeem een systeem voor risicobeheer op te zetten, met als doel risico's voor de gezondheid, veiligheid en grondrechten vast te stellen, te analyseren en te evalueren, en vervolgens gepaste en gerichte risicobeheersmaatregelen te treffen.

Daarnaast moeten overheidsorganisaties als gebruiksverantwoordelijke voor het gebruik van een hoog-risico AI-systeem een beoordeling maken van de gevolgen voor de grondrechten bij dat specifieke gebruik. Hierbij wordt onder andere gekeken naar wat mogelijke risico's zijn die het gebruik van het AI-systeem voor (categorieën van) natuurlijke personen kan hebben. Ook wordt gekeken naar de mogelijkheden om die risico's verder te mitigeren en hoe die risico's zich verhouden tot de risico's in de situatie dat het AI-systeem niet wordt gebruikt.

Vraag 64: Zijn alle instrumenten uit tabel 1 geldige methoden om een risicoafweging te maken voor een AI-systemen? Zo nee, welke zijn wel of niet geldig?

Ja, al deze instrumenten zijn geldige methoden. Bovendien zijn sommige instrumenten, (zoals een DPIA) wettelijk verplicht. Het kabinet vindt het

belangrijk om de verschillende instrumenten te stroomlijnen en te prioriteren. Dat gebeurt via het Algoritmekader, waarvan een volgende versie eind 2024 af zal zijn[8].

Vraag 65: Hoe waarborgt u de democratische controle op de AI-systemen die de overheid gebruikt als er voornamelijk interne protocollen en kaders worden gebruikt om de impact van een toepassing te wegen?

Een groot deel van de verantwoordelijkheid ligt intern, in het primaire proces (algoritme eindverantwoordelijke en het management) en een deel extern, bij het onafhankelijk toezicht. Verplichtingen omtrent het vastleggen van documentatie – bijvoorbeeld in het Algoritmeregister – kunnen het werk van een extern onafhankelijke toezichthouder vergemakkelijken.

Verder wil het kabinet, zoals ook genoemd in het regeerprogramma, signalen van (groepen) burgers beter ophalen, omdat in direct contact met burgers blijkt of de overheid er daadwerkelijk voor hen is. Geadviseerd wordt om een IAMA te doen waarbij ook burgers (of organisaties die hen vertegenwoordigen) worden betrokken. Andere vergelijkbare vormen van geadviseerde maatregelen zijn burgerpanels en/of ethische commissies met vertegenwoordiging van (groepen) burgers.

Vraag 66: Hoe reageert u op de onduidelijkheid die ontstaat door het gebrek aan een rijksbreed instrument om de risico's van AI-systemen mee af te wegen?

Vraag 67: Zodra er een rijksbreed instrument is voor het afwegen van de risico's van AI-systemen, hoe zorgt u er dan voor dat alle reeds in gebruik genomen systemen en lopende experimenten hier aan voldoen?

(Gecombineerd antwoord op vragen 66 en 67)

In het Algoritmekader wordt gewerkt aan verduidelijking van vereisten waaraan een AI-systeem of algoritme moet voldoen. Dit Algoritmekader integreert de vereisten voor AI en algoritmen, zoals de AI-verordening, en te treffen maatregelen voor verantwoorde inzet van AI. Daarmee zet ik, vanuit mijn coördinerende rol, in op het ondersteunen van organisaties bij de verantwoorde inzet van AI en het uniform toepassen van beschikbare instrumenten.

Daarnaast verplicht de AI-verordening een risicoafweging tijdens de ontwikkeling en het gebruik van een hoog-risico AI-systeem (respectievelijk artikel 9 en 27 van de verordening).

Vraag 68: Aan welke eisen moeten intern ontwikkelde AI-systemen voldoen?

Vraag 69: Aan welke eisen moeten ingekochte AI-systemen voldoen?

(Gecombineerd antwoord op vragen 68 en 69)

De AI-verordening maakt geen onderscheid tussen intern ontwikkelde en ingekochte AI-systemen. AI-systemen die onder de reikwijdte van de AI-verordening vallen, moeten – afhankelijk van de risicocategorie waarin

[8] https://minbzk.github.io/algoritmekader/instrumenten/#hoe-we-instrumenten-selecteren

een AI-systeem wordt onderverdeeld – aan bepaalde eisen voldoen. Daarnaast is aan de Algemene Rijksinkoopvoorwaarden bij IT-overeenkomsten een AI-module toegevoegd voor de inkoop van hoog-risico AI-systemen.

AI-praktijken die verboden worden moeten per 2 februari 2025 worden uitgezet indien deze worden gebruikt. Voor hoog-risico AI-systemen moet een conformiteitsbeoordeling zijn uitgevoerd voordat deze systemen op de markt zijn gebracht of in gebruik zijn genomen. Hierbij horen strikte eisen, waarvan de aanbieder moet zorgen dat het systeem daaraan voldoet. Voor AI-systemen met transparantierisico's in de zin van artikel 50 moet het voor natuurlijke personen bijvoorbeeld kenbaar zijn dat content door AI is gegenereerd of gemanipuleerd, of dat zij worden blootgesteld aan emotieherkenningssystemen.

Vraag 70: Moet er te allen tijde duidelijkheid bestaan over de afkomst van AI-systemen die de overheid gebruikt om problematische afhankelijkheden van derden en kwetsbaarheden te voorkomen?

Vraag 71: Zijn er landen waaruit een AI-systeem onder geen enkele voorwaarde mag worden ingekocht? Kunt u garanderen dat er bij de hele overheid geen sprake van is van een dergelijk AI-systeem?

(Gecombineerd antwoord op vragen 70 en 71)

De AI-verordening is van toepassing op alle AI-systemen die binnen de Europese Unie op de markt worden gebracht of in gebruik worden genomen, ongeacht of die AI-systemen binnen of buiten de Unie zijn ontwikkeld. Dit betekent dat aanbieders van AI-systemen uit landen buiten de Unie hun systemen pas op de Europese markt mogen brengen als deze systemen aan de eisen van de AI-verordening voldoen.

Vraag 72: Hoe kunt u de inschatting van het risiconiveau van AI-systemen vertrouwen als dit gebaseerd is op interne protocollen?

Departementen wordt door middel van handreikingen, een interdepartementale werkgroep, een spreekuur, en webinars hulp geboden bij het inventariseren en classificeren van AI-systemen, zodat deze zo accuraat mogelijk worden ingeschat. De CIO-offices en Functionaris Gegevensbescherming spelen hierbij een belangrijke rol als interne toezichthouders. De verantwoordelijkheid van juiste inventarisatie, classificatie en het eventueel uitzetten van AI-systemen ligt bij de desbetreffende Ministers. Voor uitgebreider antwoord op de stelselbenadering verwijs ik u door naar het antwoord op vraag 9.

Daarnaast worden AI-systemen binnen de AI-verordening in bepaalde risicocategorieën geclassificeerd. Op het voldoen aan de verordening (en daarmee ook de juiste classificatie van AI-systemen) zal toezicht worden gehouden. Momenteel wordt aan de inrichting van het toezicht op de AI-verordening gewerkt. Voor uitgebreider antwoord over de inrichting van het toezicht op de AI-verordening verwijs ik u door naar het antwoord op vraag 12.

Vraag 73: Is er onafhankelijk toezicht op de risicoclassificatie van AI-systemen?

Op het voldoen aan de verordening (en daarmee ook de juiste classificatie van AI-systemen) zal toezicht worden gehouden. Momenteel wordt aan de inrichting van het toezicht op de AI-verordening gewerkt. Voor uitgebreider antwoord over de inrichting van het toezicht op de AI-verordening verwijs ik u naar het antwoord op vraag 12.

Vraag 74: Kunt u alle dertig AI-systemen waarvan wordt ingeschat dat deze een hoog risico vormen in kaart brengen?

Ik heb geen inzicht in de informatie waarover de ARK beschikt naar aanleiding van haar onderzoek. Voor de Rijksoverheid geldt dat alle hoog-risico AI-systemen voor eind 2025 in kaart moeten zijn en gepubliceerd zijn in het Algoritmeregister, zoals met uw Kamer afgesproken. Ik verwijs u verder naar mijn antwoord op vraag 10.

Vraag 75: Kunt u de vier genoemde voorbeelden van AI-systemen met een hoog risico nader toelichten en nog dit jaar laten registreren in het Algoritmeregister?

Nee, dat kan ik niet. Ik verwijs u naar mijn antwoord op vraag 74.

Vraag 76: Welke rol speelt u of gaat u spelen om voor februari 2025 te garanderen dat de overheid geen gebruik maakt van AI-systemen met een onaanvaardbaar risico?

De AI-verordening stelt dat verboden AI-praktijken, waar geen uitzonderingsgrond voor geldt, voor februari 2025 worden gestaakt. Departementen wordt door middel van handreikingen, een interdepartementale werkgroep, een spreekuur, en webinars hulp geboden bij het inventariseren en classificeren van AI-systemen. Mijn taak als Staatssecretaris is kaderstellend, voorts ondersteunend, en waar nodig aanjagend naar alle overheidslagen. Ik werk ook toe naar een integrale aanpak op het toezicht hierop. Hierin spelen toezichthouders, uw Kamer en de ARK en ADR ook een rol. Departementen zijn zelf verantwoordelijk voor juiste inventarisatie, classificatie en eventueel staken van verboden AI-praktijken. Dit samenspel moet ertoe leiden dat de overheid verantwoord gebruik maakt van AI-systemen.

Vraag 77: Kunt u voor de vier genoemde voorbeelden van AI-systemen met een hoog risico garanderen dat er sprake is van degelijke menselijke tussenkomst? Op basis van welke kaders beoordeelt u dat?

Nee, dat kan ik niet. Ik heb geen inzicht in de informatie waarover de ARK beschikt n.a.v. haar onderzoek.

Vraag 78: Hoe verantwoordt u het gebruik van AI-systemen die achteraf, na het toepassen van een betrouwbare risicoclassificatie, toch onaanvaardbaar of onwenselijk blijken?

AI-systemen waarvan het gebruik volgens de wettelijke kaders tot onaanvaardbare of onwenselijke risico's leidt, mogen niet gebruikt worden. Een aanbieder van een hoog-risico AI-systeem moet onder de AI-verordening de werking van dat systeem blijven monitoren nadat het op de markt is gebracht. Indien nodig, zal de aanbieder ook aanpassingen moeten doen om te zorgen dat het systeem aan de vereisten blijft voldoen. Ook toezichthouders kunnen systemen controleren als zij aanwijzingen hebben dat die systemen niet (meer) voldoen aan de vereisten.

Ook de gebruiker moet eventuele onregelmatigheden aan de aanbieder melden, zodat daar actie op kan worden ondernomen.

Vraag 79: Wanneer is een AI-systeem dat tekst interpreteert en vertaalt voldoende betrouwbaar?

Er bestaat geen eenduidige checklist om te kunnen controleren of een dergelijk AI-systeem voldoende betrouwbaar is. De betrouwbaarheid hangt af van een veelvoud aan factoren, zoals de data die ten grondslag liggen aan de AI en het algoritme zelf, maar ook aan de context waarin het AI-systeem ingezet wordt en de wijze waarop het door mensen wordt gebruikt. Een AI-systeem kan in de ene context acceptabel zijn, maar in een andere context niet. Zo zal een dergelijk AI-systeem, waarvan de inzet directe impact kan hebben op het leven van burgers, in veel gevallen strikter moeten worden getoetst op betrouwbaarheid dan een systeem dat puur wordt ingezet voor een ondersteunende taak (zonder directe impact op burgers, organisaties of bedrijven). Vanuit de AI-verordening moet het bij AI-systemen die content genereren, zoals teksten en beeldmateriaal, bijvoorbeeld duidelijk zijn dat deze content door middel van AI is gegenereerd. Deze transparantieverplichting gaat gelden vanaf augustus 2026.

Vraag 80: Wanneer is een AI-systeem dat het risico op schulden-problematiek inschat voldoende betrouwbaar?

Er bestaat geen eenduidige checklist om te kunnen controleren of een AI-systeem – al dan niet met betrekking tot schuldenproblematiek – voldoende betrouwbaar is. De betrouwbaarheid hangt af van een veelvoud aan factoren, zoals de data die ten grondslag liggen aan de AI en het algoritme zelf, maar ook aan de context waarin het AI-systeem ingezet wordt en de wijze waarop het door mensen wordt gebruikt. Een AI-systeem kan in de ene context acceptabel zijn, maar in een andere context niet.

In de context van schuldenproblematiek is de kans groot dat AI-systemen betrekking hebben op mensen in een uitermate kwetsbare positie. Dan is het van belang dat niet een enkele partij besluit dat dat systeem betrouwbaar is, maar dat er vanuit verschillende perspectieven (ontwikkelaar, onderzoeker, domeindeskundige, gebruiker, degene op wie de AI van toepassing is) naar wordt gekeken.

Daarom werkt het Ministerie van BZK in het ELSA-lab Armoede en Schulden samen met Triple Helix partners en burgers aan een iteratief proces waarbij de zogenaamde ELSA-aspecten (ethical, legal and societal aspects / ethische, juridische en maatschappelijke aspecten) in alle fasen van het ontwerp van AI aandacht krijgen. Er worden kritische vragen gesteld over de noodzaak, welke maatregelen zijn genomen in het geval iets misgaat, en of het gebruik van deze AI bepaalde groepen in de samenleving benadeelt.

Een dergelijk proces is nooit «af»: het is onmogelijk om betrouwbaarheid eenmalig vast te stellen en er daarna niet meer naar om te kijken. Het is een terugkerend punt van aandacht: met wat we nu weten, vinden we het AI-systeem nog voldoende betrouwbaar? Interdisciplinariteit en diversiteit zijn onmisbaar.

Vraag 81: Hoe garandeert u de kwaliteit van de data waarop AI-systemen van de overheid getraind worden?

Voor het toetsen van gegevenskwaliteit kan het raamwerk gegevenskwaliteit van de Nederlandse overheid referentie architectuur worden ingezet als hulpmiddel. In het stelsel van basisregistraties zijn kwaliteitsafspraken gemaakt en deze worden jaarlijks gemonitord. Verder zijn departementen verantwoordelijk voor de toetsing van de gegevenskwaliteit van de onder hun verantwoordelijkheid tot stand gekomen registers.

Vraag 82: Welke consequenties heeft het voor een departement als deze gebruik maakt van een onaanvaardbaar AI-systeem?

Het staken van verboden AI-praktijken voor februari 2025 heeft prioriteit in de implementatie van de AI-verordening. Als verboden AI-praktijkensystemen, zonder uitzonderingsgrond, ná 2 februari 2025 nog in gebruik zijn, kunnen er sancties volgen. Momenteel wordt gewerkt aan de inrichting van het toezicht op de AI-verordening, en ook op de verboden AI-praktijken. Voor uitgebreider antwoord hierop verwijs ik u door naar het antwoord op vraag 12.