



BENCHMARK AI ACT

AUTHORS

Frank van Vonderen
Sebastiaan Bouthoorn

Voorwoord

De eerste vorm van risico gebaseerde regelgeving voor kunstmatige intelligentie in de EU is een feit. Per 1 augustus 2024 is de Artificiële Intelligentie Verordening (AI Act) in werking getreden. De impact op zowel publieke als private organisaties is groot.

Met de komst van de AI Act worden burgers en bedrijven in de EU beter beschermd tegen onverantwoord gebruik van AI. Potentiële risico's die gepaard gaan met het gebruik van AI-systemen worden zoveel mogelijk gemitigeerd. Dit betekent werk aan de winkel voor organisaties die AI zelf ontwikkelen, dan wel zelf inzetten.

Highberg heeft begin 2025 een enquête uitgevoerd onder publieke en private organisaties in Nederland om de mate van compliance met de AI Act te onderzoeken. Deelnemers geven aan dat zowel het bepalen van de impact als de implementatie ervan veel vragen oproept, bijvoorbeeld wanneer iets wel of niet 'AI' is en wat de gevolgen zijn van het gebruik van generatieve AI in de publieke sector.

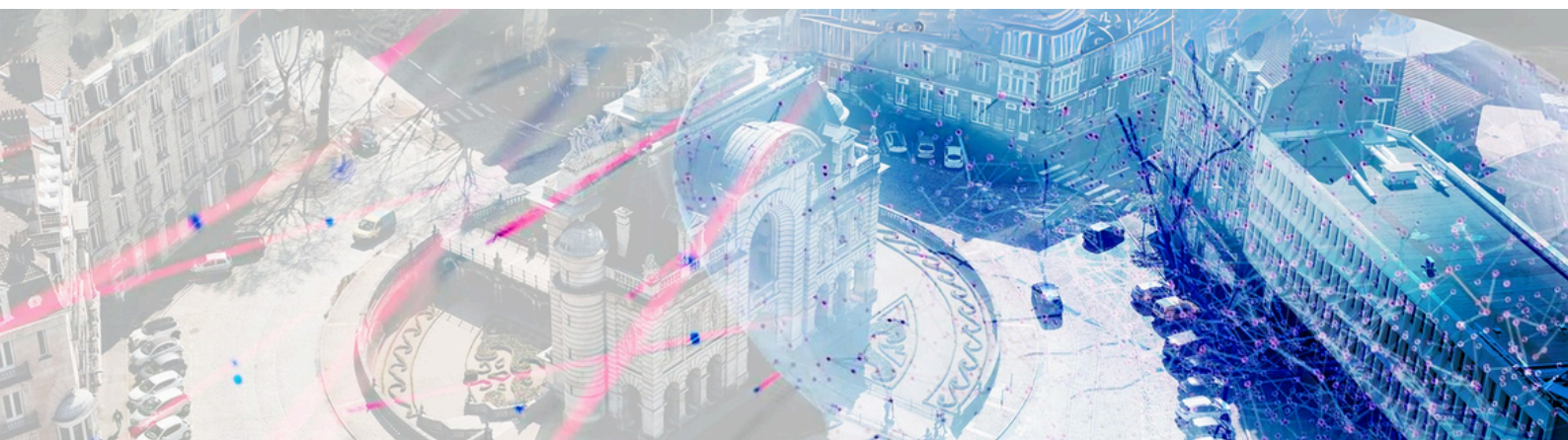
In dit rapport leest u in hoeverre u en uw collega's op de hoogte zijn van deze wetgeving en waar organisaties concreet tegenaan lopen bij het bepalen van de impact. Ook staan we stil bij mogelijke drempels die men ervaart bij de implementatie van deze wet.

De benchmark is gestructureerd aan de hand van de vragen die we bij een publieke enquête hebben gesteld.

We hopen dat deze Benchmark AI Act 2025 inzicht biedt in hoe uw organisatie zich verhoudt tot het nationale beeld en dat hiermee duidelijk wordt welke concrete actiepunten nodig zijn om succesvol tot verantwoorde inzet van data en AI te komen.

We wensen u veel leesplezier.

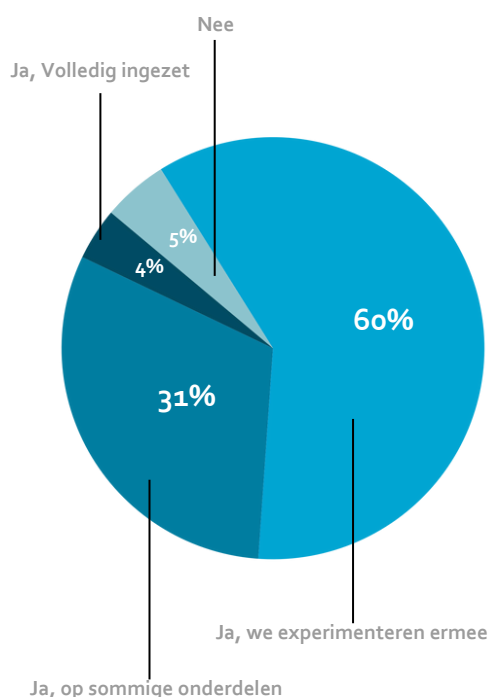
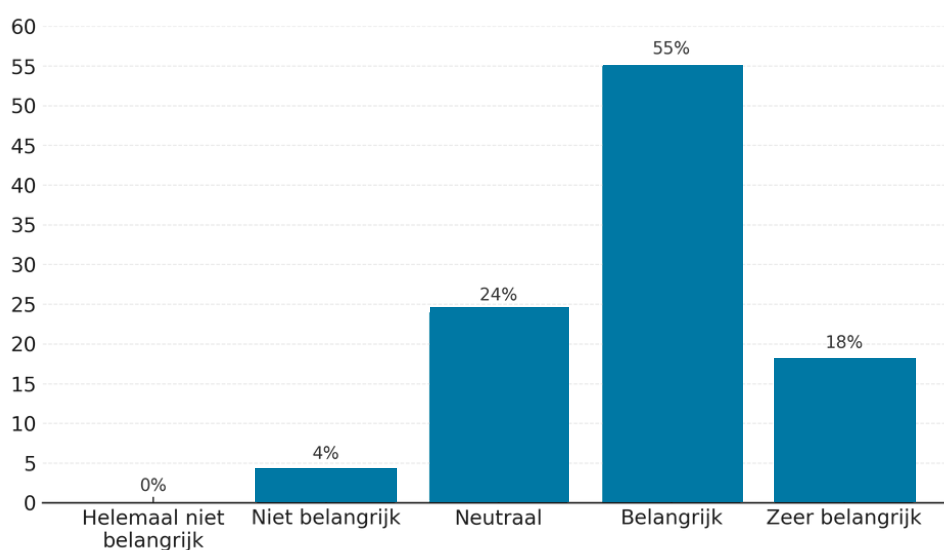
Sebastiaan Bouthoorn en Frank van Vonderen



Hoe belangrijk is AI binnen uw organisatie?

Op papier is het eenvoudig: het belang van AI voor een organisatie is in potentie enorm. Voor de organisatie zelf biedt AI de mogelijkheid om efficiënter te werken door processen te automatiseren en data-analyse te verbeteren, wat leidt tot betere besluitvorming. Medewerkers profiteren van AI doordat repetitieve taken worden overgenomen, waardoor zij zich kunnen richten op meer creatieve en strategische werkzaamheden. Dit verhoogt niet alleen de productiviteit, maar ook de werktevredenheid. Voor klanten betekent AI een verbeterde ervaring door gepersonaliseerde diensten en snellere reacties op hun vragen en behoeften. Bovendien kan AI helpen bij het voorspellen van klantgedrag, waardoor organisaties proactief kunnen inspelen op de wensen van hun klanten.

De deelnemers aan de enquête waardeerden het belang van AI voor hun organisatie overwegend als 'belangrijk' of 'zeer belangrijk.'



Maakt uw organisatie gebruik van AI?

In de afgelopen drie jaar is het gebruik van AI binnen organisaties sterk gegroeid. Uit onze enquête blijkt dat maar liefst 95% van de respondenten aangeeft dat hun organisatie gebruik maakt van AI, zoals weergegeven in de illustratie aan de linkerkant.

Daarnaast biedt het onderzoek van Equote van 2024 interessante inzichten over de gebruikers van AI in het bedrijfsleven.¹ Een paar conclusies:

- "In bepaalde sectoren is het gebruik van AI al ver ingeburgerd verzekeraars (45%), Telecom (35%), IT (35%)."
- Grotere organisaties kennen een grotere acceptatie van AI dan andere organisaties.
- AI leeft vooral in de Randstad."

Kortom: de adoptie van AI groeit snel, al zijn er wel verschillen tussen sectoren. Is uw organisatie klaar om aan de slag te gaan met AI? Doe onze AI-volwassenheidsscan op:

<https://highberg.com/nl/insights/de-highberg-ai-volwassenheidsscan>

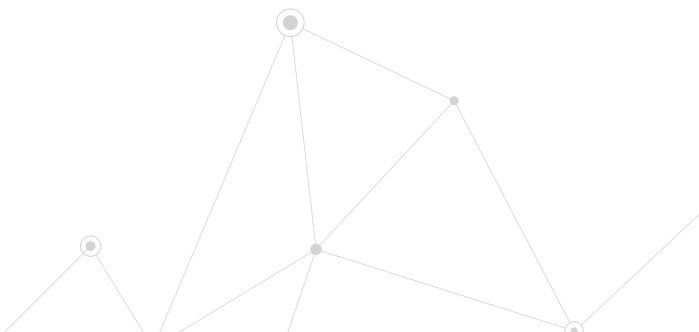
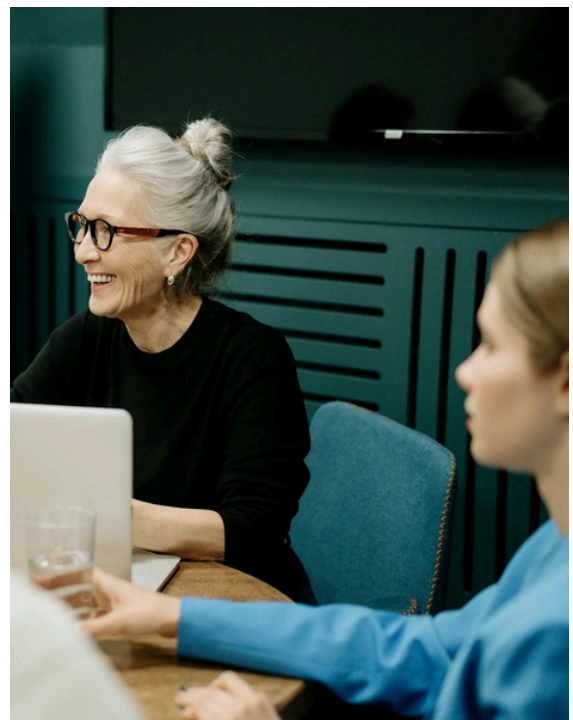
1 | <https://equote.nl/onderzoek-deze-sector-maakt-het-meest-gebruik-van-ai/>

In hoeverre is uw organisatie voorbereid op de implicaties van de AI Act en hoe waardeert uw organisatie deze?



Deze vraag laat zien dat organisaties misschien nog niet in alle gevallen zijn voorbereid, maar dat ze wel de voordelen zien van de AI Act. Een interessante constatering is dat de respondenten aangeven dat zij de AI Act niet als 'moetje' zien. Zo blijkt dat deelnemers intrinsieke motivatie hebben om aan deze regelgeving te voldoen, waarvan een groot deel aangeeft de implementatie als toegevoegde waarde te zien. Onderzoek van het World Economic Forum (2023) benadrukt dat organisaties die verantwoordelijk omgaan met AI niet alleen voldoen aan regelgeving, maar ook betere prestaties leveren door verbeterde klantrelaties en operationele efficiëntie.² Een bemoedigende constatering in tijden van toegenomen regeldruk.

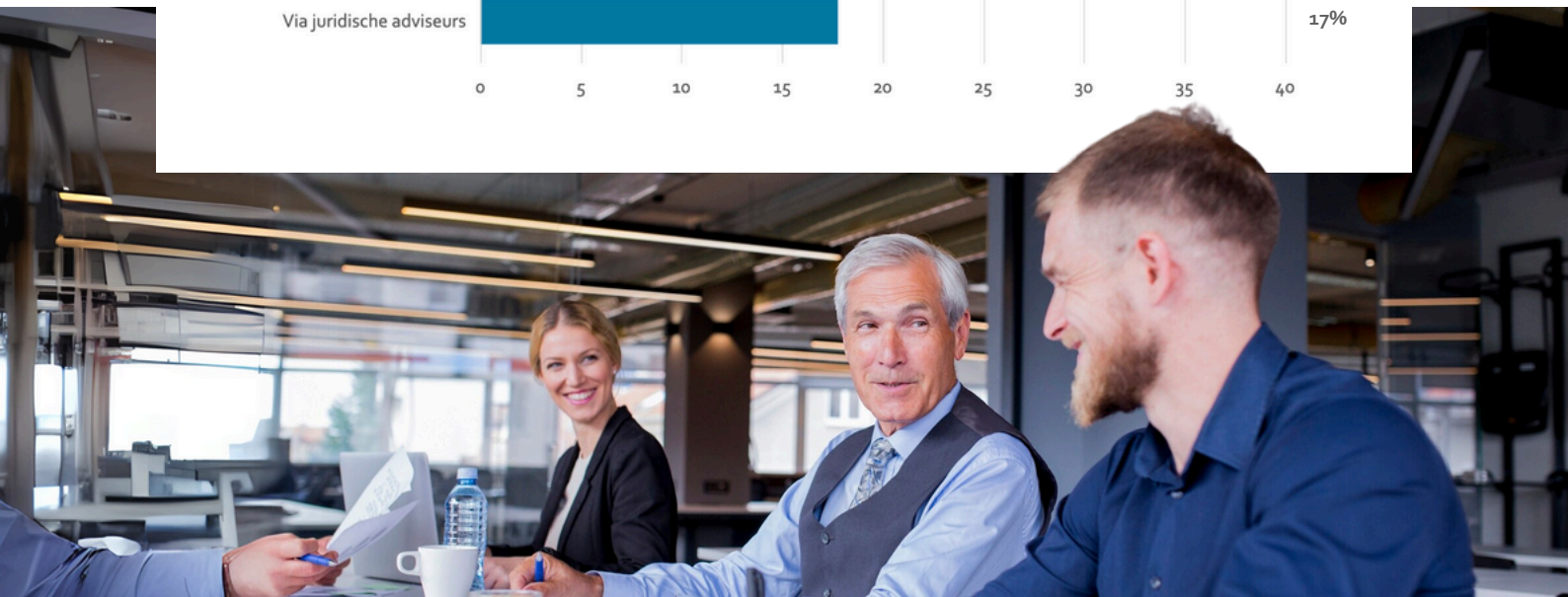
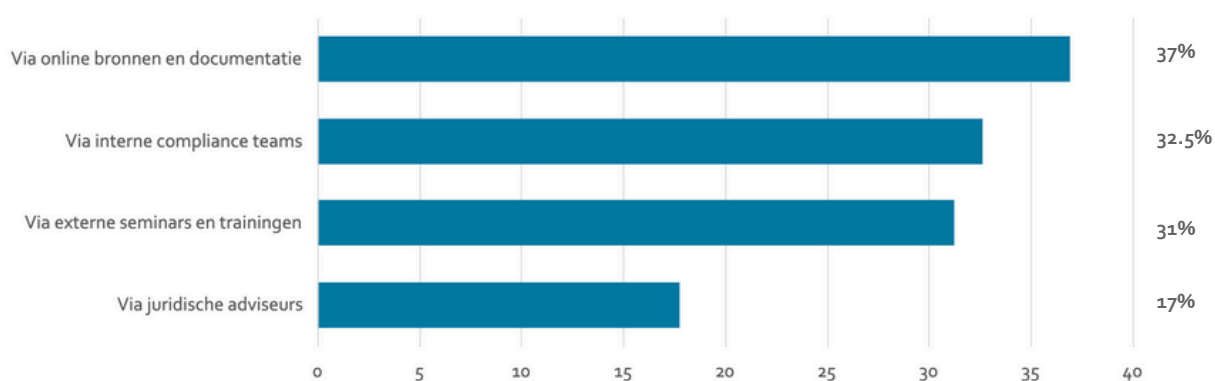
Een mogelijke reden hiervoor is dat veel mensen niet alleen de enorme potentie zien van AI, maar ook de afbreukrisico's. Door deze combinatie is het voor de respondenten blijkbaar logisch om regels te stellen.



2 | https://www.weforum.org/stories/2023/03/why-businesses-should-commit-to-responsible-ai/?utm_source=chatgpt.com

Hoe verkrijgt uw organisatie informatie over de AI Act?

Deze vraag laat zien dat respondenten zich op verschillende manieren laten informeren. Tegelijk laten de antwoorden ook zien dat veel gebruik wordt gemaakt van online bronnen en relatief weinig van externe juridisch adviseurs. Dit resultaat is enerzijds opmerkelijk, omdat online bronnen weliswaar snel en makkelijk toegankelijk zijn, maar ook algemeen blijven. Juridisch advies is meestal diepgaander en specifiek toepasbaar op de organisatie. Anderzijds benadrukt dit de trend dat organisaties steeds meer vertrouwen op digitale kanalen voor actuele informatie.



Zo blijkt uit een onderzoek van de International Association of Privacy Professionals (IAPP) dat veel organisaties online bronnen zoals webinars, whitepapers en websites van regelgevende instanties gebruiken om op de hoogte te blijven van AI-wetgeving.

Deelname aan webinars en seminars is een effectieve manier om op de hoogte te blijven van de nieuwste ontwikkelingen, het bewustzijn te vergroten en inzicht te krijgen in complexe regelgeving. Een voorbeeld hiervan is onze webinarreeks 'Impact en Implementatie' waar onze experts praktische tips en case studies delen rondom digitale wet- en regelgeving. Geïnteresseerden kunnen de webinars hier terugkijken:

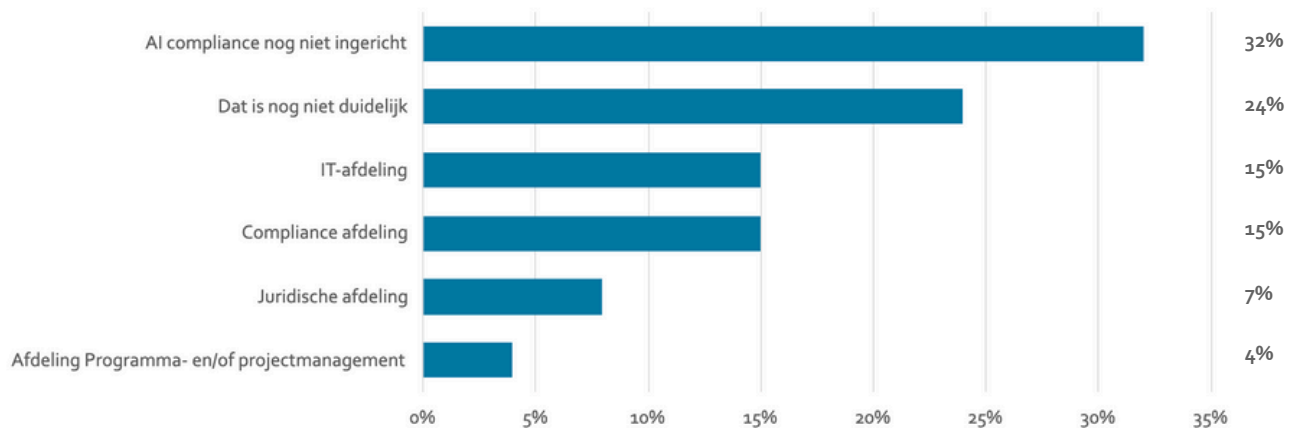


[Click here](#)

[YouTube Playlist](#)

Welke afdeling is verantwoordelijk voor AI-compliance? Heeft uw organisatie hiervoor een vast aanspreekpunt?

Deze vraag laat een grote verdeeldheid zien. De verantwoordelijkheid ligt bij verschillende afdelingen, zoals juridische afdelingen, IT of speciaal daarvoor opgerichte compliance afdelingen. Daarnaast blijkt dat als er al een duidelijke afdeling is aangewezen, het nog sterk verschilt welke rollen hierin verantwoordelijk zijn. Vaak zien we dat bestaande functies zoals FG's, CISO's, of projectmanagers deze verantwoordelijkheid erbij nemen. Daarnaast zien we bij een derde van de deelnemers dat AI-compliance sowieso nog niet is ingericht.



De AI Act volgt hierbij het pad dat we herkennen van eerdere compliance thema's, zoals security, privacy en risicomanagement. Ook bij deze onderwerpen was in het verleden zichtbaar dat niet altijd duidelijk is wie verantwoordelijk is voor compliance op deze gebieden. Dit geldt ook bij onderwerpen als digitale ethiek waar de verantwoordelijkheid in veel organisaties nog onduidelijk is of niet wordt gevoeld.

Uiteindelijk wordt gekozen voor een inrichting, waarbij 'de business', ofwel de verantwoordelijken voor de processen ook de verantwoordelijkheid hebben over het zorgvuldige gebruik van AI in hun processen. En dat zij hierbij worden ondersteund door specialisten in een stafafdeling, die hen voorzien van procedures, richtlijnen en specifiek advies.

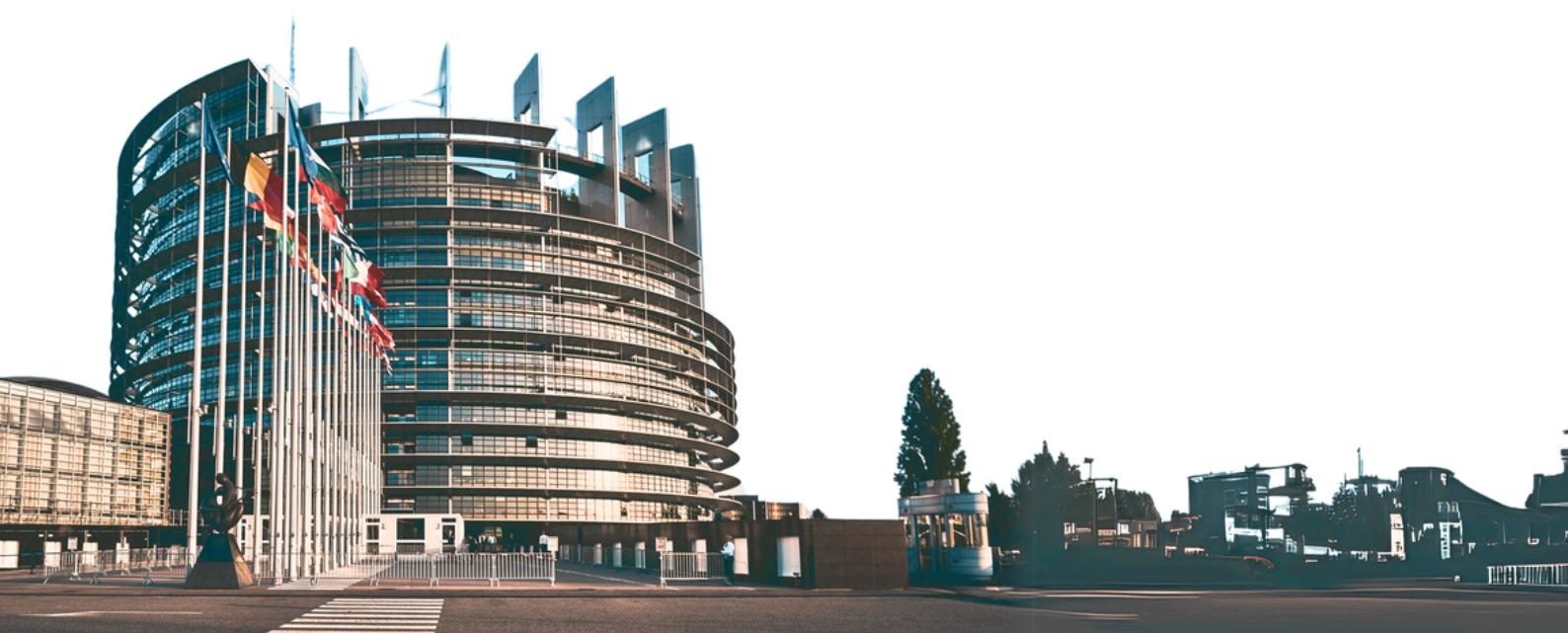
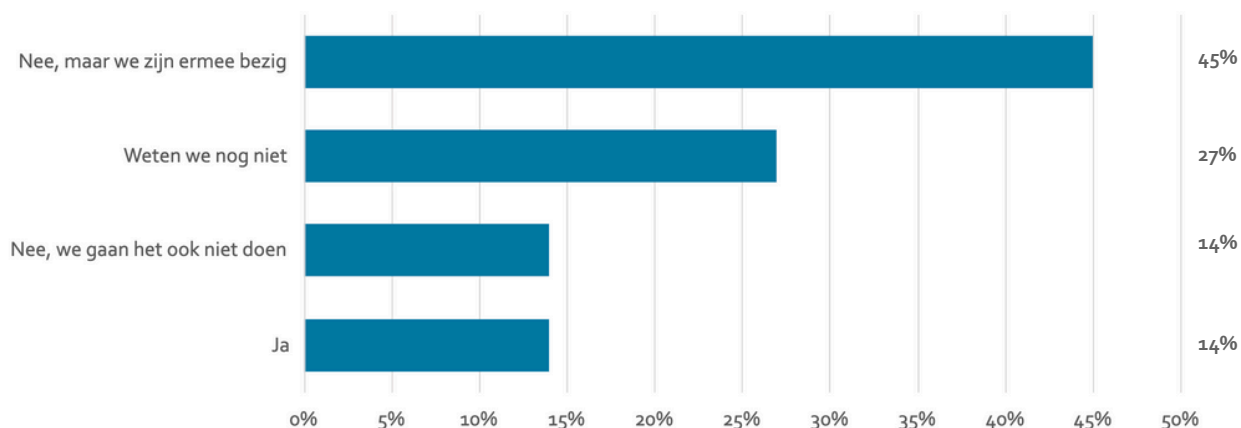


Beschikt uw organisatie over een inventarisatie van 'hoog risico AI' die wordt gebruikt of in ontwikkeling is?

Een klein deel van de respondenten geeft aan dat zij beschikken over een complete inventarisatie van 'hoog risico AI-systemen' die zij gebruiken. Een van de lastige onderwerpen uit de AI Act is de vraag wanneer een AI nu exact kwalificeert als een hoog risico AI. De toezichthouders geven daartoe specifieke richtlijnen³, maar er zijn ook nog verschillende vragen, bijvoorbeeld:

- Wat is nu de exacte definitie van een AI-systeem en waar liggen de grenzen?
- Moet de afweging van het 'hoge risico' worden beschouwd tegen de functie van het AI-systeem an sich, of binnen de context van de verwerking?

Wij verwachten dat er nog Europese richtlijnen komen over de exacte interpretatie van wat 'hoog risico AI' is. Vergeet overigens ook niet om zicht te houden op de AI met een beperkt risico, zoals bij het gebruik van generatieve AI en GPAI. Hierbij kan gedacht worden aan taalmodellen (GPT's) en chatbots die u helpen bij het opstellen van teksten en het beantwoorden van klantvragen. Hiervoor kent de AI Act transparantieverplichtingen.



3. | <https://www.autoriteitpersoonsgegevens.nl/themas/algorithmes-ai/ai-verordening/risicogroepen-ai-verordening>

Ook is het goed om te weten dat er vanuit de Rijksoverheid een [Gids AI-verordening](#) is uitgebracht waarin de definitie van AI en de belangrijkste rollen met bijbehorende verplichtingen behandeld worden.

Naast een gids met algemene informatie wordt er gewerkt aan een [AI-verordening implementatie tool](#). Deze tool helpt u als gebruiker en/of ontwikkelaar met behulp van vragenlijsten met het identificeren van zowel AI-systemen als impactvolle algoritmes. Ook geeft het inzicht in de verschillende risico categorieën en verboden toepassingen om zelf te kunnen bepalen wat de impact van de AI Act is op uw bedrijfsvoering.

Tot slot is het goed om te weten dat niet alle algoritmes kwalificeren als een 'AI-systeem' onder de AI Act, ook zijn die soms wel degelijk van invloed op burgers en bedrijven. We hebben het dan over de zogeheten 'impactvolle algoritmes'. Als definitie van impact wordt vaak gebruik gemaakt van de definitie in de Ethische Richtsnoeren voor betrouwbare Kunstmatige Intelligentie gepubliceerd door de EU in 2019:

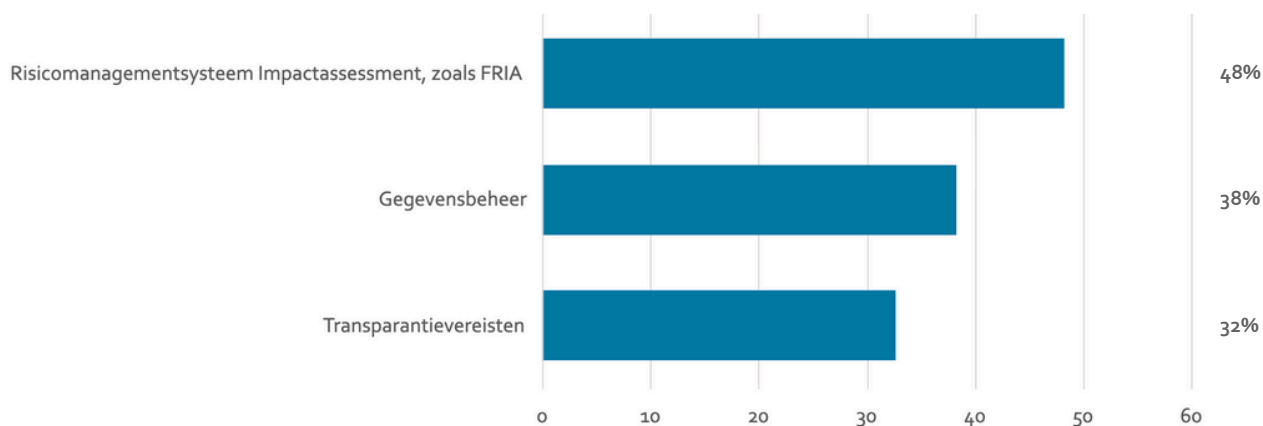
"Gegevensverwerking treft iemand volgens de richtsnoeren in aanmerkelijke mate wanneer de effecten van de verwerking groot of belangrijk genoeg zijn om aandacht te verdienen. Het besluit moet het potentieel hebben om de omstandigheden, het gedrag of de keuzen van de betrokken personen in aanmerkelijke mate te treffen, een langdurig of blijvend effect op de betrokkene te hebben, of in het uiterste geval, tot uitsluiting of discriminatie van personen te leiden."

Ook voor algoritmes die buiten de reikwijdte van de AI Act vallen, is het van belang om risico's te beheersen en transparantie te waarborgen. Een manier om dit te doen, is door impactvolle algoritmes vast te leggen in het [Landelijk Algoritmeregister](#). Dit draagt bij aan inzicht in het gebruik van algoritmes en versterkt publieke verantwoording.



Welke van de onderstaande implementatie vereisten uit de AI Act vraagt nog veel aandacht van uw organisatie?

Uit de enquête blijkt dat risicomanagementsystemen, impactassessments en transparantie bij veel organisaties nog veel aandacht vragen én bovenaan de prioriteitenlijst staan. Enerzijds geeft dit aan dat men zich bewust is van hoe belangrijk deze onderdelen zijn in het kader van compliance. Anderzijds blijkt hieruit dat de AI Act niet alleen een juridische verplichting is, maar ook een kans biedt om strategisch na te denken over de manier waarop AI-systemen worden ontworpen, gebruikt en hoe erover wordt gecommuniceerd.



Tegelijkertijd zien we bij veel organisaties een toename in nieuwe AI-initiatieven. Deze worden vaak geïnspireerd door projecten bij andere publieke organisaties of aangedragen door leveranciers en startups. Denk bijvoorbeeld aan AI-toepassingen zoals slimme chatbots, virtuele assistenten of systemen die gespreksverslagen genereren. Dit zijn waardevolle innovaties om processen efficiënter te maken, maar ze brengen ook risico's met zich mee en niet alles is toegestaan onder de AI Act.



Generatieve AI en extra verplichtingen

Veel van de nieuwe initiatieven maken gebruik van generatieve AI. Dit type AI brengt specifieke transparantieplichtingen met zich mee, zoals beschreven in artikel 50 e.v. van de AI Act. Aanbieders van generatieve AI moeten bijvoorbeeld zorgen dat de gegenereerde output gemarkeerd wordt als kunstmatig, en gebruikers van dergelijke systemen moeten duidelijk maken dat de inhoud door AI is gegenereerd. Deze verplichtingen gelden los van het hoog-risicodomein.

Wanneer generatieve AI ook wordt ingezet in een toepassing die onder het hoog risicodomein valt, bijvoorbeeld wanneer deze gebruikt wordt bij het al dan niet toekennen van een WMO-uitkering in het sociaal domein, dan gelden aanvullende eisen. Denk bijvoorbeeld aan het uitvoeren van een FRIA en het inrichten van risicomanagement. Om u hierbij alvast op weg te helpen, hebben we per rol – gebruiksverantwoordelijke en aanbieder – de belangrijkste verplichtingen op een rij gezet.

Met dit overzicht ziet u in een oogopslag in welke rol u geraakt wordt en wat de bijbehorende verplichtingen zijn. Zo benut u de kansen die AI biedt én voldoet u als organisatie aan de AI Act.

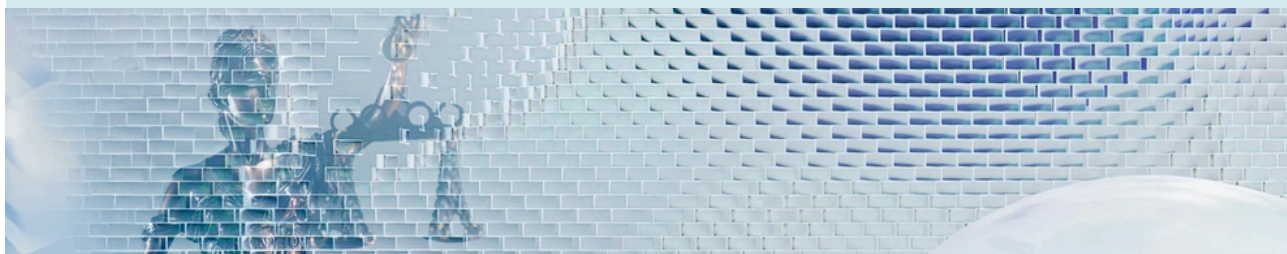
Product	Aanbieder	Gebruiksverantwoordelijke
<i>De AI Act stelt eisen aan AI-systemen.</i>	<i>De organisatie die het AI-systeem ontwikkelt, in het Engels: de Provider.</i>	<i>De organisatie die het AI-systeem gebruikt, in het Engels: de Deployer.</i>
Verplichtingen voor hoog risico AI-systemen		
• Risicomanagement systeem • Data en datagovernance • Technische documentatie • Transparantie • Menselijk toezicht • Nauwkeurigheid, robuustheid, veiligheid	• Product compliance • Kwaliteitsmanagement systeem • Conformiteits assessment + CE markering • Registratie	• Menselijk toezicht • Datakwaliteit • Logging en monitoring • Mensenrechtentoets



Impact assessment – De AI Act kent in artikel 27 de plicht voor het uitvoeren van een 'Fundamental Rights Impact Assessment (FRIA)' bij de inzet van algoritmes met een hoog risico. Deze verplichting ligt bij de organisatie die de AI inzet (de 'deployer') omdat die ook goed de kenmerken van de doelgroep en de gebruiksccontext kent. Niet elke deployer van een hoog risico AI moet echter een FRIA doen: deze verplichting geldt enkel voor "gebruiksverantwoordelijken die publiekrechtelijke organen zijn of particuliere entiteiten zijn die openbare diensten verlenen". Het staat andere organisaties natuurlijk vrij om zelf te besluiten om een dergelijke beoordeling te doen.

Iets concreter: wat valt er dan onder de definitie 'gebruiksverantwoordelijken die publiekrechtelijke organen zijn of particuliere entiteiten zijn die openbare diensten verlenen'? Overweging 59 geeft iets meer richting. Deze verplichting geldt voor:

- Overheidsinstanties (bijvoorbeeld zorgverlening, beoordeling rechten op uitkering en huisvesting) en de private partijen die publieke diensten aanbieden.
- Instellingen die kredietwaardigheidschecks uitvoeren.
- Verzekeraars die AI inzetten bij risicobeoordeling voorafgaande aan acceptatie van verzekerden of prijsbepaling van de dienstverlening.



Intussen zijn er diverse goede manieren beschikbaar gekomen om een dergelijke beoordeling goed uit te voeren. Elk van de manieren heeft daarbij zijn eigen sterke en minder sterke punten en ideale toepassingsgebied. Een IAMA (Impact Assessment Mensenrechten en Algoritmes) bijvoorbeeld is een vorm van ethische beoordeling die in veel gevallen volstaat als een FRIA (Fundamental Rights Impact Assessment), zoals vereist onder de AI Act. De IAMA richt zich specifiek op de maatschappelijke en ethische impact van algoritmes en biedt daarmee een solide basis om de fundamentele rechtenrisico's van AI-toepassingen in kaart te brengen.

Let op: niet alle ethische assessments voldoen volledig aan de eisen van een FRIA. Methodes zoals een moreel beraad kunnen bijvoorbeeld waardevolle inzichten bieden, maar missen vaak de juridische en technische diepgang die een FRIA vereist. Deze ethische tools kunnen wel ondersteunend zijn bij het voorbereiden van een FRIA, door relevante risico's en overwegingen helder te maken. Om de bepalen welke methode voor uw organisatie het beste is, is deze keuzehulp ontworpen:



Click here

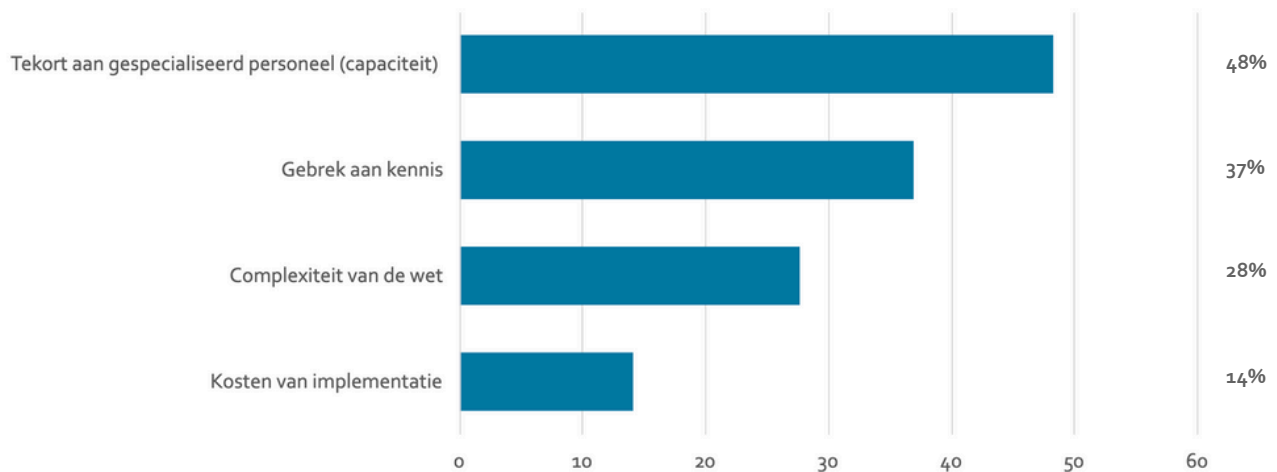
[Adviesgids Data-ethiek methodes](#)

Risicomanagement systemen – Risico management in de context van AI kent twee interpretaties. Allereerst de letterlijke interpretatie vanuit de AI Act, dat organisaties een inschatting maken van het risiconiveau van de toepassing. De tweede interpretatie van risicomanagement is in de AI Act te vinden in artikel 9, voor 'AI-systemen met een hoog risico wordt een systeem voor risicobeheer vastgesteld, uitgevoerd, gedocumenteerd en in stand gehouden'. In de ISO 42001 standaard, de wereldwijd toegepaste norm voor een AI management systeem, wordt een passende methode voor risico management beschreven, die aandacht besteedt aan de voortdurende beheersing van risico's. Denk hierbij aan het identificeren, beheersen en (her)evalueren van risico's rondom de ontwikkeling, de toepassing en het gebruik van AI. Overigens helpt deze ISO 42001 standaard ook enorm bij het inrichten van een 'systeem voor kwaliteitsbeheer', zoals de AI Act onder artikel 17 beschrijft.



Wat zijn de grootste uitdagingen bij het implementeren van de AI Act en waarom?

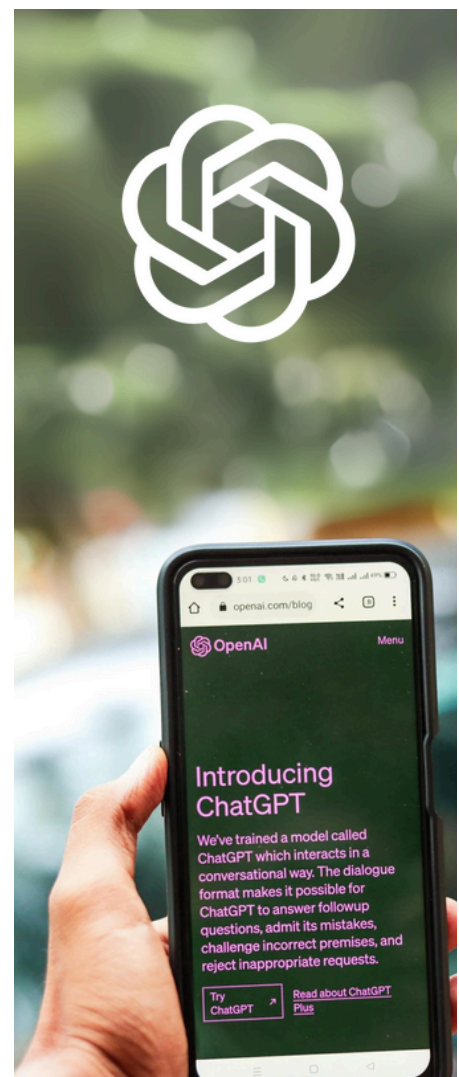
Op basis van de antwoorden blijkt budget wel een relevant knelpunt, maar niet het grootste knelpunt. De benodigde specialistische kennis en (vooral) de benodigde hoeveelheid inhoudelijke capaciteit lijken de belangrijkste bottle necks te zijn.



De kennisontwikkeling vraagt nog de nodige aandacht. Hoewel het werken met LLM's (zoals ChatGPT) vaak als laagdrempelig wordt ervaren, vereist het gebruik ervan meer inzicht dan op het eerste gezicht lijkt. De kunst van het prompten speelt hierbij een grote rol: wie effectief wil werken met LLM's, moet begrijpen hoe ze te sturen zijn om het maximale resultaat te behalen. Tevens vormt dit een belangrijk onderdeel van AI-geletterdheid, waarover in de toelichting van de volgende vraag (13) meer. Dit geldt niet alleen voor specialisten, maar ook voor andere doelgroepen binnen de organisatie.

Voor een zorgvuldige toepassing van AI is het essentieel om álle betrokkenen binnen de organisatie goed te informeren en te trainen. Dit gaat niet alleen over AI-specialisten zoals technenuten of compliance managers, maar ook bestuurders, gebruikers, juristen en inkopers. De uitdaging ligt in het aanbieden van trainingen die aansluiten bij de uiteenlopende rollen en verantwoordelijkheden binnen een organisatie. Er komen wel steeds meer specialistische trainingen op de markt die gericht zijn op AI-compliance managers, maar voor andere doelgroepen zijn nog weinig laagdrempeliger trainingen beschikbaar. Dit 'kennisgat' vergroot de druk op specialisten en maakt het lastiger om AI op een verantwoorde en geïnformeerde manier te implementeren.

Naar ons beeld gaat er een grote behoefte bestaan aan basistrainingen die de diverse doelgroepen exact uitleggen wat de toepassing voor hun eigen werk betekent. Door laagdrempelige kennis aan te bieden aan een bredere doelgroep, wordt ook de druk op de beschikbaarheid van specialistische kennis verlaagd. Relatief eenvoudige vragen kunnen door meerdere mensen worden beantwoord en specialistische kennis wordt alleen aangesproken voor specialistische vragen.



Responsible by design - gouden tips

Naast de wettelijke verplichtingen waar je als organisatie aan moet voldoen, zijn er inmiddels ook een aantal nuttige best practices ontstaan. Met name op het gebied van generatieve AI. Deze bieden handvatten om niet alleen compliant te zijn, maar ook om AI op een ethisch verantwoorde manier te implementeren. Drie principes uit de praktijk die direct toepasbaar zijn en die we graag met u delen:

1

Zorg voor veilige dataopslag

Sla bij het gebruik van GPT's gegevens op in een veilige, afgescheiden cloudomgeving, bij voorkeur binnen de grenzen van uw eigen organisatie en in een omgeving zoals Azure. Zo wordt voorkomen dat (gevoelige) data door de leverancier wordt gebruikt voor het trainen van hun algoritmes. Dit geldt ook voor de opgeslagen queries. Zo beschouwt de Autoriteit Persoonsgegevens (AP)⁴ het delen van persoonsgegevens met tools zoals ChatGPT als een potentieel datalek. Dit benadrukt het belang van het zorgvuldig beheer van data en kan voor publieke organisaties aanleiding zijn om bepaalde projecten intern op te pakken in plaats van met een externe leverancier.

2

Voer een IAMA uit

Voor hoog risico AI is een FRIA verplicht. Dit is een uitgebreide analyse waarin technische en organisatorische keuzes worden beschreven, evenals een beoordeling van de mogelijke effecten en risico's van het AI-systeem op fundamentele mensenrechten. In Nederland wordt de IAMA gezien als een best practice voor het uitvoeren van een FRIA. Het opstellen van een IAMA vraagt om input van een multidisciplinaire groep en neemt doorgaans 5 tot 10 uur in beslag.

Voor organisaties die al een DPIA (Data Protection Impact Assessment) hebben uitgevoerd, kan een deel van deze analyse direct worden gebruikt als input voor de IAMA. Dit maakt het proces efficiënter en creëert meer draagvlak.

Wist u dat: een goed uitgevoerde IAMA niet alleen compliance met de AI Act oplevert, maar ook de ethische integriteit van het AI-systeem versterkt? Het Alan Turing Institute⁵ heeft een gids gepubliceerd over AI-ethiek en veiligheid, waarin wordt benadrukt dat organisaties die dergelijke assessments uitvoeren, vaker vertrouwen genieten van gebruikers en burgers, omdat zij aantoonbaar rekening houden met ethische en juridische normen in hun AI-toepassingen.

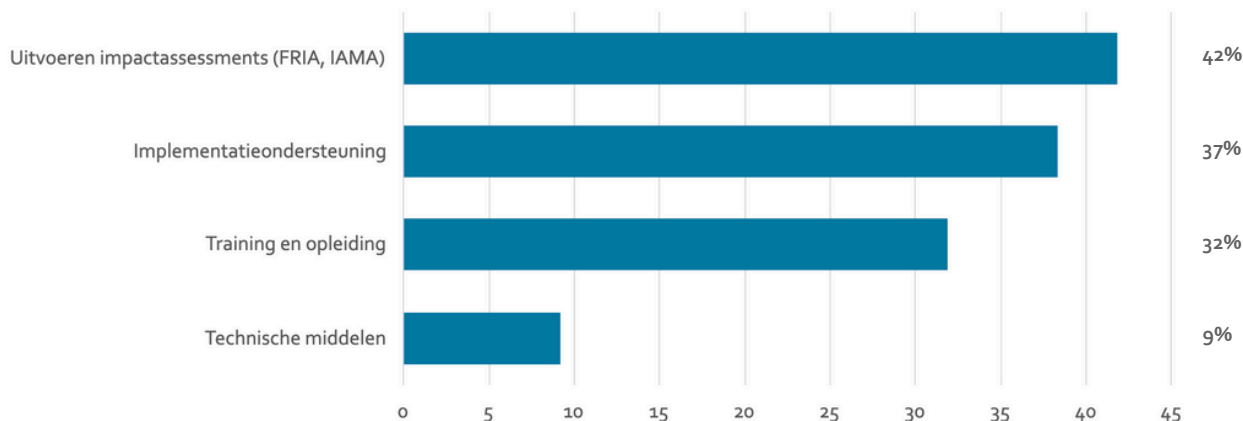


4 | <https://www.autoriteitpersoonsgegevens.nl/actueel/let-op-gebruik-ai-chatbot-kan-leiden-tot-datalekken>

5 | https://www.turing.ac.uk/news/publications/understanding-artificial-intelligence-ethics-and-safety?utm_source=chatgpt.com

Op welke punten zou uw organisatie meer capaciteit kunnen gebruiken om aan de AI Act te kunnen voldoen?

De deelnemers aan de enquête voorzagen de volgende noodzaak voor capaciteit:



Uit de antwoorden blijkt dat training en opleiding voor medewerkers de grootste behoefte is, gevolgd door toegang tot technische middelen zoals algoritmeregisters en tools voor risicobeheersing. Ook wordt er een duidelijke vraag gesignaleerd naar praktische ondersteuning bij de implementatie, zoals begeleiding bij het aanpassen van processen en het waarborgen van compliance. Dit suggereert dat organisaties niet alleen technische uitdagingen ervaren, maar vooral een kenniskloof moeten overbruggen om compliance te realiseren.

Training en opleiding – Het is belangrijk om medewerkers voor te bereiden op de technologische vooruitgang die AI kan bieden. Opleidingen en cursussen zijn een goede manier om kennis en ervaring op te doen met wetgeving zoals de AI Act.

Een belangrijke verplichting waar organisaties vanaf februari 2025 aan moeten voldoen is AI-geletterdheid. Werk je als organisatie met AI, dan moet je ervoor zorgen dat medewerkers voldoende kennis, vaardigheden en begrip hebben om AI-systemen op een geïnformeerde en verantwoorde manier te gebruiken. AI-geletterdheid omvat niet alleen technische kennis, maar ook inzicht in de ethische en juridische aspecten van AI. Om deze reden is het cruciaal dat medewerkers van verschillende afdelingen hierin getraind worden, met een maatwerkopleiding waarin zij kennismaken met de aspecten van AI die specifiek van toepassing zijn voor hun werk. Het niet naleven kan leiden tot fikse boetes - oplopend tot 7,5 miljoen euro.

In de wet staat hierover het volgende opgenomen:

Artikel 4 AI Act:

Aanbieders en gebruiksverantwoordelijken van AI-systemen nemen maatregelen om, zoveel als mogelijk, te zorgen voor een toereikend niveau van AI-geletterdheid bij hun personeel (...), en houden daarbij rekening met hun technische kennis, ervaring, onderwijs en opleiding en de context waarin de AI-systemen zullen worden gebruikt (...)

Overweging 56 AI Act:

"AI-geletterdheid": vaardigheden, kennis en begrip die aanbieders, gebruiksverantwoordelijken en betrokken personen, rekening houdend met hun respectieve rechten en plichten in het kader van deze verordening, in staat stellen geïnformeerd AI-systemen in te zetten en zich bewuster te worden van de kansen en risico's van AI en de mogelijke schade die zij kan veroorzaken;

Twee manieren om alvast met AI-geletterdheid aan de slag te gaan



1

Stel een AI-geletterdheidsprogramma op

Ontwikkel een intern trainingsprogramma dat aansluit bij de specifieke behoeften en functies binnen de organisatie. Dit kan variëren van technische cursussen voor IT-specialisten tot workshops over ethische en juridische implicaties van AI voor management en beleidsmakers. Maak eventueel gebruik van externe aanbieders met expertise in AI-wetgeving en praktijkvoorbeelden om de inhoud actueel en relevant te houden.

Organiseer multidisciplinaire workshops en simulatie

Breng medewerkers van verschillende afdelingen samen in interactieve workshops waarin praktische scenario's worden uitgewerkt. Bijvoorbeeld: hoe om te gaan met een hoog risico AI-systeem of hoe transparantievereisten te implementeren. Simulaties kunnen helpen om de complexe impact van AI-toepassingen te begrijpen en zorgen voor gedeeld inzicht en samenwerking tussen teams.

2

Implementatieondersteuning – De AI Act stelt specifieke eisen aan processen, systemen en documentatie, met name voor organisaties die werken met hoog risico AI-systemen. Het opzetten van een duidelijke governance-structuur en het uitvoeren van verplichte impact assessments zijn tijdsintensieve taken waarvoor vaak gespecialiseerde kennis nodig is.

Uitvoeren impact assessments – Dat de respondenten aangeven capaciteit nodig te hebben voor het uitvoeren van impact assessments is begrijpelijk. Sinds de AVG hebben we geleerd dat het uitvoeren van een privacy impact assessment (een DPIA), om verschillende redenen niet eenvoudig is. Bij vraag 9 en 10 gaven we al aan dat er ook verschillende methodes zijn om Impact Assessment Mensenrechten en Algoritmes (IAMA) uit te voeren. Organisaties zoeken de mogelijkheden om bijvoorbeeld het uitvoeren van de IAMA te combineren met een DPIA. In de praktijk zien we ook al dat dit ook goed kan (bijvoorbeeld door een 'DPIAMA' uit te voeren).

Technische middelen – Met technische middelen bedoelen we concrete tools en systemen die nodig zijn om invulling te geven aan de eisen van de AI Act. Dit kan bijvoorbeeld een algoritmeregister zijn, een online platform waarin alle gebruikte AI-systemen binnen een organisatie worden vastgelegd, inclusief informatie over werking, datasets en risicoanalyses. Ook tools voor gegevensbeheer, zoals data warehouses of systemen voor datacatalogisering, zijn van belang om transparantie en naleving te waarborgen. Verder kan GRC-tooling (Governance, Risk en Compliance) worden ingezet om risico's te monitoren, compliance-processen te beheren, en interne controles uit te voeren.



In hoeverre voldoet uw organisatie momenteel aan de AI Act? Wanneer is/wordt er een start gemaakt met de implementatie van de AI Act?

Het is geen verrassing dat nog geen enkele organisatie volledig compliant is met de AI Act. Een logische verklaring hiervoor is dat de officiële deadlines voor implementatie nog niet verstreken zijn, waardoor veel organisaties andere prioriteiten stellen. De deadlines verschillen per risicocategorie, wat de aanpak beïnvloedt. Zo moeten verboden AI-systemen al vanaf 2025 worden gestaakt, wat begrijpelijk een hogere urgentie krijgt. Veel organisaties hebben hun implementatietraject pas recent opgestart of plannen dit binnen de komende 6-12 maanden te doen.

In de onderstaande tijdlijn lichten we de belangrijkste mijlpalen van de AI Act voor u uit.

2 februari 2025

Vanaf deze datum mogen verboden AI-systemen niet langer worden gebruikt. Dit zijn systemen die in strijd zijn met de fundamentele rechten en veiligheid, zoals sociale scoring door overheden en systemen voor subliminale manipulatie. Daarnaast is dit het moment voor organisaties om te starten met programma's voor AI-geletterdheid, zodat werknemers en stakeholders bekend raken met de basisprincipes van AI en de risico's ervan.

2 augustus 2025

Organisaties die generatieve AI gebruiken, zoals chatbots en creatieve tools, moeten vanaf deze datum voldoen aan specifieke voorwaarden. Dit omvat bijvoorbeeld het duidelijk maken dat gegenereerde content door AI is gemaakt en het uitleggen van brongebruik.

2 augustus 2026

Hoog risico-AI-systemen, zoals die worden gebruikt in de gezondheidszorg, rechtshandhaving of transport, moeten volledig aan de eisen van de AI Act voldoen. Dit omvat het doorlopen van Impact Assessments, documentatie van technische en organisatorische keuzes, en het waarborgen van transparantie en veiligheid. Zie voor een uitgebreid overzicht van deze verplichtingen [pagina 11](#).

2 augustus 2030

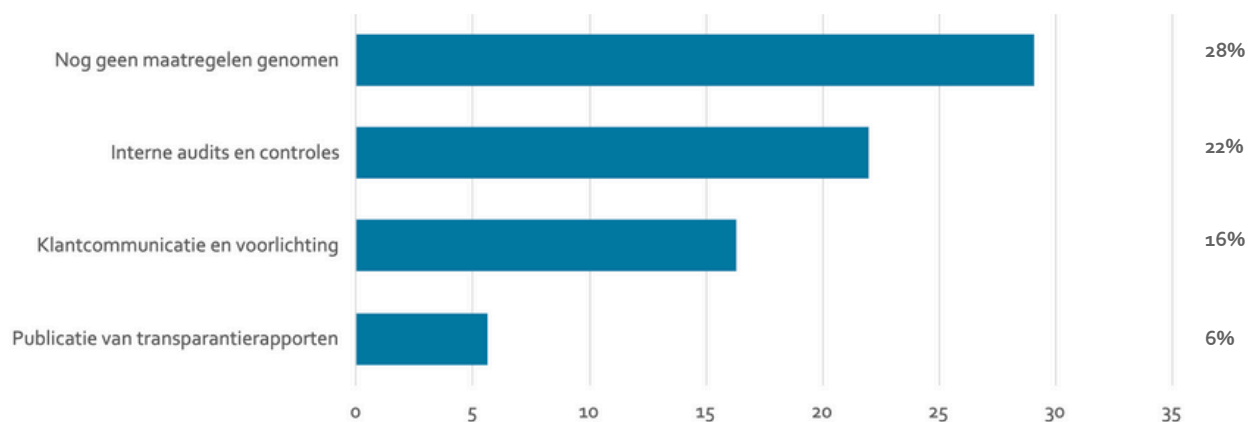
Overheden die gebruik maakten van AI-systemen vóór de inwerkingtreding van de AI Act, hebben van de wetgever een langere overgangperiode. Deze systemen moeten uiterlijk in 2030 volledig voldoen aan de regelgeving. Dit biedt overheden meer tijd om bestaande technologieën te evalueren en waar nodig aanpassingen door te voeren zonder dat cruciale processen verstoord raken.



Welke maatregelen heeft uw organisatie genomen om te voldoen aan de transparantievereisten van de AI Act?

Transparantie wordt vaak ten onrechte alleen geassocieerd met generatieve AI en laag risico AI-systemen terwijl het een minstens net zo cruciale rol speelt in het hoog risico domein. De AI Act vereist duidelijke informatie over het gebruik, de werking en de impact van AI-systemen, ongeacht het type. Bij hoog risico AI is dit zelfs extra belangrijk, omdat output zoals beslissingen of adviezen direct invloed kunnen hebben op burgers en organisaties.

Een belangrijk onderdeel van transparantie is het inzichtelijk maken van hoe data en AI-systemen worden gebruikt, bijvoorbeeld via een algoritmeregister. Hierin legt u vast hoe bepaalde AI-systemen werken, wat de doelen zijn en welke datasets worden gebruikt. Transparantie beperkt zich echter niet alleen tot technische verplichtingen, maar vraagt ook om heldere communicatie naar alle betrokkenen.



Publicatie van transparantierapporten - Aanbieders van hoog risico AI-systemen zijn volgens de AI Act (bijvoorbeeld artikelen 13 en 50 e.v.) verplicht om transparantierapporten op te stellen. Deze rapporten bevatten informatie over de werking van het AI-systeem, gebruikte datasets, risicoanalyses en de genomen maatregelen om veiligheid en betrouwbaarheid te waarborgen. Voor gebruiksverantwoordelijken is dit niet altijd een harde verplichting, maar het publiceren van transparante informatie wordt sterk aanbevolen als onderdeel van goed bestuur. Denk bijvoorbeeld aan de situatie waarbij je als overheidsorganisatie AI inkoopt en gebruikt, en over de werking en de effecten op burgers toelichting geeft in een algoritmeregister.

Interne audits en controles - Naast strenge transparantievereisten geldt voor hoog risico AI-systemen ook dat je interne audits moet uitvoeren om naleving van de wet te waarborgen (zie bijvoorbeeld artikel 17). Dit omvat onder meer het monitoren van de werking van systemen, het evalueren van risico's en het controleren van datakwaliteit en nauwkeurigheid. Deze controles helpen om afwijkingen vroegtijdig te signaleren en minimaliseren juridische en ethische risico's. Gebruikers moeten daarnaast zorgen voor adequaat toezicht op hoe AI-systemen in de praktijk worden ingezet.

Klantcommunicatie en voorlichting - Artikel 50 benadrukt ook het belang van heldere communicatie over de werking en gebruik van AI-systemen naar gebruikers en stakeholders. Dit omvat bijvoorbeeld informatie over hoe een AI-systeem werkt en welke gegevens worden gebruikt, maar ook wat de beperkingen en risico's zijn. Vooral wanneer het gaat om hoog risico toepassingen. Zorg ervoor dat de informatie begrijpelijk is voor iedereen, ongeacht achtergrond of expertise. Dat kun je bijvoorbeeld doen door te schrijven op B1-niveau. Dit betekent eenvoudig taalgebruik, korte zinnen, en waar mogelijk visuele ondersteuning zoals schema's of infographics. Op deze manier maak je informatie toegankelijk voor alle gebruikers, ook voor mensen zonder specifieke kennis van AI.

BENCHMARK AI ACT



Vragen over deze benchmark? Neem contact op met één van onze experts:

Sebastiaan Bouthoorn

+31 (0)6 515 805 37

sebastiaan.bouthoorn@highberg.com

Frank van Vonderen

+31 (0)6 125 573 58

frank.vanvonderen@highberg.com

