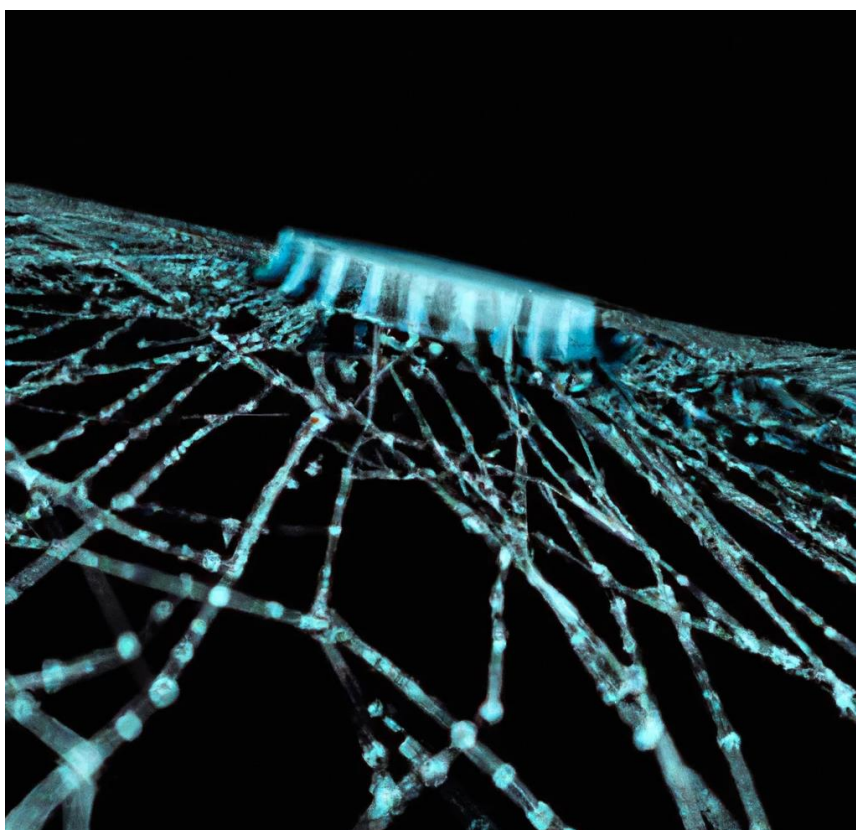


KADERS VOOR HET GEBRUIK VAN KUNSTMATIGE INTELLIGENTIE (AI) BINNEN DE VRK



Versie 2.0

Datum: 18-3-2025

Status: Goedgekeurd

Versiebeheer:

Versie	Door	Datum	Opmerkingen
0.1	Erik Beukenkamp Marije Frijlink Bart Hermus Veronica Jonker Ruben Modderman Jeroen Schulten Gabriel Sobrino Indra van der Wolf	December 2023	Eerste conceptversie.
1.0	Erik Beukenkamp Marije Frijlink Bart Hermus Veronica Jonker Ruben Modderman Jeroen Schulten Gabriel Sobrino Indra van der Wolf	Januari 2024	Diverse aanscherpingen en definitief maken van het document.
1.1	Gabriel Sobrino	4 Juni 2024	Update van het document en van de toetsingscriteria n.a.v. de definitieve Europese AI-verordening: EU Artificial Intelligence Act Up-to-date developments and analyses of the EU AI Act
2.0	Gabriel Sobrino	22 April 2025	Aanscherpingen n.a.v. de terugkoppeling van de Pilotgroep AI. Aanpassingen en aanvullingen n.a.v. verduidelijkingen in de Europese AI-wet . Aanscherpingen n.a.v. het geüpdatete overheidsbrede standpunt m.b.t. het gebruik van generatie AI .

Inhoud

Versiebeheer:	2
1 Inleiding	4
1.1 Aanleiding.....	4
1.2 Waar en op wie zijn deze kaders van toepassing?	4
1.3 Waar kan ik terecht met vragen?	4
2 Wat is AI en wat valt er onder het beleid?	4
3 Kaders gebruik AI.....	5
3.1 Welke AI-producten mogen worden gebruikt?	5
3.1.1 Hoe vraag ik een AI-product aan?	6
3.2 Welke informatie mag je gebruiken in AI-producten?.....	6
3.2.1 Beperkingen op informatie die gebruikt kan in een AI-systeem	8
3.2.2 Uitzonderingen (aanvragen) op het beleid m.b.t. informatiegebruik	11
3.3 Eigen verantwoordelijkheid van het gebruik van AI?	11
4 AI-geletterdheid.....	11
Bijlagen	12
Bijlage 1 – Toetsingscriteria AI-Producten en AI-systemen	12
Bijlage 2 – Landen binnen de EER & adequaatheidsbesluit	14
Bijlage 3 - Minimale transparantievoorwaarden van de AI-wet.....	15
Bijlage 4 – Aandachtsgebieden die in een EU-databank moeten worden geregistreerd	16
Bijlage 5 – Hoog risico systemen en veiligheidscomponenten volgens de AI-wet	17
Bijlage 6 – Verboden AI-systemen	20
Bijlage 7 – Verboden criminele handelingen	21
Verklarende begrippenlijst	22
Bibliografie.....	23

1 Inleiding

1.1 Aanleiding

Kunstmatige Intelligentie (Artificial Intelligence ofwel AI) is een transformatieve technologie die de maatschappij diep zal blijven beïnvloeden de komende jaren. Dit maakt het opstellen van kaders m.b.t. het gebruik van deze technologie noodzakelijk voor alle organisaties in de particuliere en publieke sectoren.

1.2 Waar en op wie zijn deze kaders van toepassing?

Deze kaders zijn op alle afdelingen binnen de VRK van toepassing.

1.3 Waar kan ik terecht met vragen?

Voor vragen over dit beleid kun je terecht bij de verschillende leden van het ICT-IM-Board. Wie dit zijn kun je vinden op de volgende pagina: [ICT-IM Board - Startpagina \(sharepoint.com\)](https://sharepoint.com/ICT-IM-Board-Startpagina)

2 Wat is AI en wat valt er onder het beleid?

AI, of kunstmatige intelligentie, is een terrein binnen informatica; dit begrip, aanvankelijk bedacht door emeritus Stanford Professor John McCarthy in 1955, werd door hem gedefinieerd als “de wetenschap en techniek van het maken van intelligente machines”. Veel onderzoek heeft mensen de mogelijkheid gegeven machines te programmeren om zich op een slimme manier te gedragen. Een van deze toepassingen is schaken, maar tegenwoordig wordt de nadruk gelegd op technologieën die zelf informatie kunnen associëren en “leren”, op een manier vergelijkbaar aan hoe de mens denkt ([AI-Definitions-HAI.pdf \(stanford.edu\)](https://stanford.edu/Definitions-HAI.pdf)).

De [Rijksoverheid](#) definieert kunstmatige intelligentie als: “systemen die intelligent gedrag vertonen door hun omgeving te analyseren en - met een zekere mate van zelfstandigheid - actie ondernemen om specifieke doelen te bereiken.”

Dit beleid geldt voor alle toepassingen die (gedeeltelijk) gebruik maken van technieken die bijdragen aan systemen die functioneren zoals beschreven in de bovenstaande definitie.

2.1 Ontwikkeling van AI over de jaren heen

AI is niet nieuw, sinds de jaren '50 vinden er ontwikkelingen plaats op dit gebied. Sinds eind jaren '80 zijn er al schakcomputers die vaardige spelers kunnen verslaan. Deze eerste vormen van kunstmatige intelligentie zijn opgezet op basis van logische regels, met condities die een gevolg veroorzaken. Het concept is als volgt: “Als er iets gebeurt, dan reageert de toepassing op een bepaalde manier”. Dit concept staat bekend als **Expert systems**, omdat de regels die deze systemen volgen aanvankelijk ontwikkeld zijn door (menselijke) experts op het gebied waarvoor ze ontworpen zijn.

In de jaren '90 werd het echter mogelijk om AI anders te benaderen. Programmeurs konden namelijk computers zelf laten “leren” aan de hand van informatie. Computers konden dan zelf bepalen welke acties te ondernemen, in plaats van dit af te leiden van een logische conditie-gevolg-regel. Deze aanpak, bekend als **Machine Learning**, is de basis van moderne AI-modellen. Daarbij kunnen die modellen zelf een uitkomst berekenen op basis van het leggen van statistische relaties tussen grote hoeveelheden informatie die ze eerder hebben geanalyseerd. Machine learning en de daarop gebaseerde **Deep learning**-technieken werden mogelijk dankzij het ontstaan van geavanceerde **Neural Networks**: computers die informatie opslaan en verwerken op een manier die het menselijke brein imiteert.

2.2 Soorten AI

Er is ruwweg een tweedeling met betrekking tot de doeleinden waar AI voor gebruikt kan worden:

Doelspecifieke (narrow) AI: systemen die ontworpen en getraind zijn om een (aantal) specifieke functie(s) uit te voeren of die bruikbaar zijn binnen een specifiek veld/discipline. Een voorbeeld van een doelspecifiek AI-systeem gebaseerd op deep learning is *AlphaFold*, een AI-model dat ontwikkeld is om de structuur van eiwitten te voorspellen.

Generalistische (general purpose) AI: AI die in staat is om meerdere soorten resultaten (output) te produceren en toepassingen kent voor meerdere doeleinden en bij meerdere kennisdomeinen. Een Voorbeeld hiervan is de chatbot ChatGPT.

2.3 Generatieve AI

Generatieve AI verwijst naar producten die ontworpen zijn om nieuwe informatie te produceren/genereren op basis van reeds geanalyseerde data. Dit kan tekstuele informatie, computercode, afbeeldingen en dergelijke zijn (zoals ChatGPT), maar kan ook gaan om het genereren van een specifiek soort output binnen een specifiek veld (zoals AlphaFold). De hierboven genoemde voorbeelden van doelspecifieke en generalistische AI zijn tevens ook voorbeelden van generatieve AI.

3 Kaders gebruik AI

AI is een ingewikkeld, zeer technisch onderwerp; zelfs de wetenschappers die AI-technologie ontwikkelen begrijpen niet helemaal hoe het werkt. Ondanks de vooruitgang in de ontwikkeling van AI blijft AI nog onvoorspelbaar en dit brengt risico's met zich. Een aantal van de belangrijkste risico's zijn door de AIVD uitgewerkt in een [begrijpelijk document](#) (AIVD, 2023).

Voor een nieuwe ontwikkeling als deze is het belangrijk goed vast te stellen wat wel en wat niet gebruikt mag worden. Dit hoofdstuk biedt daar een handvat voor en is ingedeeld in drie delen:

- Welke AI-producten mogen wel door VRK-medewerkers worden gehanteerd ([3.1](#)).
- Welk soort informatie mogen VRK-medewerkers bieden aan de toegestane AI-producten ([3.2](#)).
- Wat is de verantwoordelijkheid van de gebruikers bij het gebruik van AI-producten ([3.3](#)).

De onderstaande kaders volgen de richtlijnen en aanbevelingen die gedefinieerd zijn door o.a.:

- Rijksoverheid (advies van het Kabinet m.b.t. het gebruik van generatieve AI, geldig sinds december 2023)
- Europese Unie (European AI Act¹, die op 1 augustus 2024 in werking is getreden)
- AIVD (advies m.b.t. het verzachten van risico's van AI)

Geüpdatet [overheidsbreed standpunt voor de inzet van generatieve AI](#), dat op 22 april 2025 is gepubliceerd.

3.1 Welke AI-producten mogen worden gebruikt?

Het vertrekpunt is dat vóór gebruik van AI-producten door medewerkers van de VRK, toetsing en goedkeuring nodig is op basis van de toetsingscriteria die beschreven zijn in [Bijlage 1](#).

¹ De European AI Act, ook bekend als Europese AI-verordening wordt in dit document gerefereerd als "AI-wet" gezien dat dit de benaming is die de Rijksoverheid in Nederland vaker hanteert.

Het ICT-IM Board toetst de aangevraagde AI-producten en adviseert (op basis van de uitkomst van de toetsing) over het wel/niet gebruiken van die AI-producten en de eventuele voorwaarden die bij het gebruik daarvan gelden. Het advies van het ICT-IM Board hierover is bindend en er kan alleen middels een directiebesluit van worden afgeweken.

Het streven is een eenduidig aanbod van AI-producten vast te stellen voor de medewerkers van de VRK; dit betekent dat de organisatie voor het doel van een aanvraag, organisatiebreed, maar één AI-product selecteert. Voor elke volgende aanvraag met datzelfde doel, is alleen gebruik van dat AI-product toegestaan.

Alle producten die niet door het ICT-IM Board zijn goedgekeurd voor gebruik binnen de VRK zijn niet toegestaan binnen de omgevingen van de VRK, noch lokaal op de VRK laptops, noch via externe (SaaS)-diensten en -applicaties.

Bij het gebruik van door het ICT-IM Board goedgekeurde AI-producten geldt dat informatie uit de categorieën die expliciet uitgezonderd zijn in 3.2, op geen enkel moment mag worden ingevoerd in/aangeboden aan een AI-product, tenzij hier een uitzondering voor is verleend via een directiebesluit.

3.1.1 Hoe vraag ik een AI-product aan?

Wanneer er behoefte is aan een AI-product waar de VRK geen goedgekeurde producten voor heeft geselecteerd kan een medewerker het gewenste AI-product via de Servicedesk ([Mijn Desk](#)) aanvragen (aanvraag nieuwe software). Die aanvragen worden behandeld en geëvalueerd door het ICT-IM Board.

Let op! Net zoals bij andere aanvragen t.b.v. (nieuwe) software is de aanvrager verantwoordelijk voor de bekostiging van de aangevraagde AI-producten. Het goedkeuren van een AI-product voor gebruik door het ICT-IM Board is daarom geen toezegging van middelen t.b.v. de bekostiging ervan. In het geval van AI-producten waarvoor inzet óf door meerdere sectoren of zelfs organisatie breed beoogd is, zal er worden gekeken naar een passende regeling voor de bekostiging.

3.2 Welke informatie mag je gebruiken in AI-producten?

AI-producten gaan op verschillende manieren om met het verwerken en opslaan van data. Dit kan in meerdere gevallen betekenen dat waarborging van de veiligheid en privacy van de informatie die AI-producten verwerken en opslaan niet mogelijk is. Om deze reden zijn er beperkingen aan de verwerking van het soort informatie door een AI-product. Deze beperkingen zijn gebaseerd op de wettelijke kijk op de risico's die kunnen ontstaan door de verwerking van informatie in AI-systemen. In de onderstaande paragrafen wordt beschreven welke informatie wel en niet mag worden aangeboden.

Let op! De onderstaande richtlijnen gelden voor alle soorten input die AI-producten kunnen accepteren, waaronder inbegrepen maar niet beperkt tot: bestanden van alle soorten tekst, afbeeldingen, video-opnames, audio-opnames, kwantitatieve informatie en ongestructureerde informatie.

De basisregel is dat alle AI-producten die door de VRK zijn goedgekeurd, mogen worden gebruikt met openbare informatie, dat wil zeggen informatie die iedereen mag hebben, delen en opslaan.

Denk bijvoorbeeld aan informatie die bedoeld is voor publicatie in openbare bronnen zoals de website van de VRK of openbare nieuwsbrieven.

Er zijn echter soorten informatie die volgens de AI-wet nooit mogen worden geüpload of aangeboden aan AI-producten (ook al zijn de betreffende AI-producten goedgekeurd voor gebruik binnen de VRK). Deze soorten informatie staan beschreven op de tabel in [3.2.1](#).

Bij twijfelgevallen (als niet met zekerheid kan worden vastgesteld of de informatie openbaar is of niet) dienen de Privacy-officer en/of Functionaris Gegevensbescherming te worden geraadpleegd.

Geadviseerde “best practice” voor het wel/niet gebruiken van informatie in een AI-systeem: Bij de afweging over het wel/niet aanbieden van informatie aan een AI-systeem, denk aan de volgende vraag: *“zou ik het goed vinden als deze informatie morgen in de krant verschijnt?”*. Als het niet wenselijk is dat die informatie openbaar wordt gemaakt, dan is het verstandig om die informatie **niet** aan te bieden aan een AI-systeem.

3.2.1 Beperkingen op informatie die gebruikt kan in een AI-systeem

Bedrijfsinformatie:

<u>Bedrijfsinformatie</u>	<u>Voorbeeld</u>	<u>Risicocategorie</u> (volgens de AI-wet)	<u>Impact</u>	<u>Wat mag wel?</u>
Patenten en intellectueel eigendom	Technische details van patenten en/of daar bijhorende processen.	Hoog	• Mogelijk verlies van intellectuele eigendom, en bedrijfsgeheimen.	• Geanonimiseerde informatie die niet af te leiden is, en geen identificeerbare of traceerbare data bevat.
Strategische plannen	Bedrijfsstrategieën, teamplannen, , overnames, fusies.	Hoog	• Mogelijk lek van strategische afwegingen en plannen van de organisatie.	• Geanonimiseerde informatie die niet af te leiden is, en geen identificeerbare of traceerbare data bevat.
Operationele informatie	Dienstroosters, rijroutes, personeelsbezetting.	Onacceptabel	• Veiligheids- en continuïteitsgevaar indien kwaadaardige partijen in staat zijn om onze operaties en activiteiten te verstoren.	• Geanonimiseerde informatie die niet af te leiden is, en geen identificeerbare of traceerbare data bevat.
Financiële gegevens	Inkomsten, uitgaven, winst- en verliesrekeningen, belastingaangiften.	Hoog	• Lek van financiële informatie kan ernstige repercussies hebben voor de reputatie en operaties van de VRK.	• Geanonimiseerde informatie die niet af te leiden is, en geen identificeerbare of traceerbare data bevat.
Softwarebroncode	De broncode van aangepaste software of apps.	Onacceptabel	• Veiligheids- en continuïteitsgevaar indien kwaadaardige partijen gebruikmaken van kwetsbaarheden in de code van onze applicaties om onze activiteiten te verstoren.	• Vragen m.b.t. specifieke codelijnen zonder dat de hele broncode gedeeld wordt. • Broncode van volledige open source toepassingen die openbaar moeten zijn (bijvoorbeeld volgens de Wet Open Data Implementatie Richtlijn).

Persoonsgegevens:

<u>Persoonsgegevens</u>	<u>Voorbeeld</u>	<u>Risicocategorie (volgens AI-wet)</u>	<u>Impact</u>	<u>Wat mag wel?</u>
Identificatiegegevens	BSN-nummers of andere ID-nummers, paspoort, rijbewijsnummers.	Onacceptabel	• Lek van persoons gegevens levert zeer ernstige gevolgen op voor de VRK. Het lekken van deze informatie leidt tot gevaar en risico's (fraude, identiteitsdiefstal enz.) voor de gedupeerden.	• Alleen als Directie hier een uitzondering voor verleent.
Gezondheidsinformatie	Medische dossiers, ziektegeschiedenis, medicatiegegevens.	Onacceptabel	• Lek van persoonlijke gegevens levert zeer ernstige gevolgen op voor de VRK.	• Alleen als Directie hier een uitzondering voor verleent. • Hoewel deze informatie niet mag worden aangeboden, is het gebruiken van volledig geanonimiseerde situaties wel mogelijk, bijvoorbeeld voor het opstellen van een brief aan iemand zonder de daadwerkelijke naam of adres en persoonlijke gegevens te hanteren.
Juridische gegevens	Details over lopende juridische geschillen, strafbladen, gerechtelijke procedures.	Onacceptabel	• Lek van persoonlijke gegevens levert zeer ernstige gevolgen op voor de VRK.	• Alleen als Directie hier een uitzondering voor verleent. • Hoewel deze informatie niet mag worden aangeboden, is het gedeeltelijk gebruiken van volledig geanonimiseerde situaties wel mogelijk, bijvoorbeeld voor het opstellen van een brief aan iemand zonder de daadwerkelijke naam of adres en persoonlijke gegevens te hanteren.

<u>Persoonsgegevens</u>	<u>Voorbeeld</u>	<u>Risicocategorie (volgens AI-wet)</u>	<u>Impact</u>	<u>Wat mag wel?</u>
Gevoelige persoonlijke meningen of overtuigingen	Religieuze, politieke of andersoortige overtuigingen.	Onacceptabel	• Lek van persoonlijke gegevens levert zeer ernstige gevolgen op voor de VRK. Kan burgers in gevaar brengen of leiden tot discriminatie.	• Alleen als Directie hier een uitzondering voor verleent. • Hoewel deze informatie niet mag worden aangeboden, is het gedeeltelijk gebruiken van volledig geanonimiseerde situaties wel mogelijk, bijvoorbeeld voor het opstellen van een brief aan iemand zonder de daadwerkelijke naam of adres en persoonlijke gegevens te hanteren.
Financiële gegevens	Bankrekeningnummers, creditcardgegevens, inloggegevens voor online bankieren.	Onacceptabel	• Lek van persoonlijke gegevens levert zeer ernstige gevolgen op voor de VRK. Het lekken van deze informatie leidt tot gevaar en risico's (fraude, identiteitsdiefstal enz.) voor de gedupeerden.	
Privécommunicatie	Persoonlijke e-mails, chatgesprekken, inhoud met vertrouwelijke informatie.	Onacceptabel	• Lek van persoonlijke gegevens levert zeer ernstige gevolgen op voor de VRK. Het lekken van deze informatie leidt tot gevaar en risico's (fraude, identiteitsdiefstal enz.) voor de gedupeerden.	• Alleen als Directie hier een uitzondering voor verleent. • Bij voor de VRK goedgekeurde AI-producten kan je wel de contactgegevens van collega's, medewerkers en zakelijke contacten gebruiken die normaal gesproken ook beschikbaar is in andere applicaties zoals Outlook/mail, digitale visitekaartjes, LinkedIn, enz.

3.2.2 Uitzonderingen (aanvragen) op het beleid m.b.t. informatiegebruik

Er kunnen argumenten ontstaan om gebruik te maken van gevoelige informatie (beschreven in hoofdstuk [3.2.1](#)) binnen een AI-systeem. Een uitzondering op de geldende beperkingen kan daarom worden aangevraagd aan de hand van een valide grondslag voor het gebruik van gevoelige data, en als er voldoende maatregelen zijn toegepast om de beveiliging en integriteit van de data te garanderen.

Wanneer er aanleiding is om niet toegestane informatie te gebruiken in een AI-product dient er eerst een [DPIA Quicksan](#) te worden uitgevoerd, en mogelijk een DPIA indien gewenst door het Privacyteam. De resulterende DPIA wordt dan voorgelegd aan het ICT-IM Board, en op basis hiervan zal het Board advies formuleren m.b.t. de gewenste uitzondering. Dit advies wordt dan voorgelegd aan de Directie die beslist over het wel of niet verlenen van een uitzondering.

Het resulterende besluit van Directie m.b.t. het wel/niet toestaan van een uitzondering is bindend.

3.3 Eigen verantwoordelijkheid van het gebruik van AI?

AI-technieken werken op basis van complexe statistische voorspellingen, en om deze reden zijn ze niet op *feiten* gebaseerd maar op de statistische waarschijnlijkheid van de patronen in de data waarop AI is getraind. Dit betekent dat de informatie die een AI-systeem genereert nooit 100% zeker is. Bij het gebruik van AI-systeem is er altijd een inherent risico aanwezig dat de informatie die geproduceerd is met AI niet juist, compleet of correct is.

Om deze reden ligt de verantwoordelijkheid voor het gebruik van AI en door AI-gegenereerde informatie bij de gebruiker van de systemen. Let daarom goed op en controleer goed de informatie die een AI-systeem produceert vóór het delen of handelen op basis daarvan. Bij twijfels raadpleeg de bronnen en of neem stappen op de informatie te verifiëren.

4 AI-geletterdheid

Sinds 2 februari 2025 verplicht de AI-verordening (overheids)organisaties werk te maken van AI-geletterdheid. AI-geletterdheid is een verzamelnaam voor kennis en kunde op het vlak van Artificiële Intelligentie (AI). Denk bijvoorbeeld aan dat je weet hoe deze technologie (op basaal niveau) werkt, waar de kansen liggen en welke risico's er aan verbonden zijn. Hierbij gaat het dus niet alleen om technische kennis, maar ook om sociale, ethische en praktische aspecten. Als aanbieder of gebruiksverantwoordelijke van AI-systemen wordt in de AI-verordening ([artikel 4](#)) beschreven dat organisaties een toereikend niveau van AI-geletterdheid waarborgen.²

Om AI-geletterdheid te verhogen heeft de VRK een aantal materialen (w.o. eenvoudige animaties en handreikingen) ontwikkeld om basiskennis m.b.t. AI te bieden aan alle medewerkers. Medewerkers worden verzocht om deze materialen te lezen en raadplegen. Vragen m.b.t. AI, AI-geletterdheid, dit beleidsdocument of de visie van de VRK omtrent AI kunnen worden gesteld via het adres ai@vrk.nl.

² Bron: [Wat je moet weten over AI-geletterdheid - Digitale Overheid](#)

Bijlagen

Bijlage 1 – Toetsingscriteria AI-Producten en AI-systemen

Toetsingscriteria	Onderbouwing
Vindt de opslag en/of verwerking van persoonsgegevens plaats binnen de EER en/of een land buiten EER waarbij een adequaatheidsbesluit geldt? Zie Bijlage 2 voor meer informatie over het EER gebied.	Verplicht door AVG en de AI-wet.
Wanneer het AI-product gebruikt wordt in een hoog risico systeem of veiligheidscomponent (zie Bijlage 5): voldoet het AI-product aan de productveiligheidswetgeving van de EU?	Verplicht door de productveiligheidswetgeving van de EU.
Wanneer het AI-product data verwerkt die gerelateerd is aan (één van) de 8 specifieke aandachtsgebieden waarvan registratie nodig is in een database van de EU: is de registratie van de data aantoonbaar gedaan in een database binnen de EU? Zie Bijlage 4 .	Verplicht door de AI-wet.
Is een DPIA en/of een IAMA uitgevoerd (alleen voor AI-producten die persoonsgegevens verwerken)?	Verplicht door de AI-wet en gesteld als eis door het Kabinet in december 2023.
Voldoet het AI-product aan de minimale transparantie-eisen van de Europese Commissie? Zie Bijlage 3 .	Verplicht door de AI-wet.
Is er voldoende informatie beschikbaar over hoe en waar het AI-product AI technieken voor gebruikt?	Verplicht door de AI-wet.
Is het onderliggende AI-model dat gebruikt wordt in een AI-product opgenomen in het Foundation Model Transparency Index ?	Dit criterium helpt met het garanderen van de betrouwbaarheid van de aanbieder van een AI-product en van het product zelf.
Is het product gecontracteerd? ³	Gesteld als eis door het Kabinet in december 2023.
Voldoet het AI-product aan de Algemene Rijksvoorwaarden bij IT-overeenkomsten 2022?	Gesteld als eis door het Kabinet in december 2023.
Is het product ontworpen om ongewenste/discriminerende/gevaarlijke informatie uit te sluiten en voorkomen?	Eigen regel van de VRK – AI-producten die geen censuur kennen en ongewenste, discriminerende, beledigende of gevaarlijke informatie kunnen produceren zijn categorisch uitgesloten.
Is het AI-product expliciet verboden zijn door de Rijksoverheid of de EU? Zie Bijlage 6 .	Verplicht door de AI-wet.
Is het AI-product ontworpen om onwettelijke of criminele handelingen te faciliteren? Zie Bijlage 7 .	Verplicht door de AI-wet.

Let op! Naast het toetsen van de bovengenoemde criteria is het invullen van de [EU AI Act Compliance Checker](#) ook verplicht voor elk product dat wordt geëvalueerd. De aanbevelingen van de EU AI Act Compliance Checker moeten worden meegenomen in de risicoanalyse van een AI-product.

Voor meer informatie over de Europese AI-verordening (European Artificial Intelligence Act) zie: [EU Artificial Intelligence Act | Up-to-date developments and analyses of the EU AI Act](#)

³ Gecontracteerd betekent formeel aangeschaft conform de officiële aanbestedingsprocedures, met een geldende overeenkomst een SLA, en een verwerkersovereenkomst getekend door de aanbieder.

Bijlage 2 – Landen binnen de EER & adequaatheidsbesluit

Landen binnen de EER

- | | | |
|---------------|-----------------|--------------|
| - België | - Ierland | - Noorwegen |
| - Bulgarije | - IJsland | - Oostenrijk |
| - Cyprus | - Italië | - Polen |
| - Denemarken | - Kroatië | - Portugal |
| - Duitsland | - Letland | - Roemenië |
| - Estland | - Liechtenstein | - Slovenië |
| - Finland | - Litouwen | - Slowakije |
| - Frankrijk | - Luxemburg | - Spanje |
| - Griekenland | - Malta | - Tsjechië |
| - Hongarije | - Nederland | - Zweden |

Landen buiten de EER die in aanmerking komen voor een adequaatheidsbesluit

- | | | |
|--------------------|-----------------|-----------------------|
| - Andorra | - Isle of Man | - Uruguay |
| - Argentinië | - Israël | - Verenigd Koninkrijk |
| - Canada | - Japan | - Verenigde Staten |
| - Faeröer Eilanden | - Jersey | |
| - Guernsey | - Nieuw-Zeeland | |

Bijlage 3 - Minimale transparantievoorwaarden van de AI-wet

- AI-producten waarmee personen kunnen interacteren moeten te allen tijde duidelijk maken dat ze geen mens zijn maar een AI-product.
- Bij audio- beeld-, videomateriaal en tekst die geproduceerd is met/door een AI-product moet een duidelijke aanduiding aanwezig zijn die aangeeft dat de inhoud geproduceerd is door/met AI. Deze “geproduceerd met AI” aanduiding moet zowel door de mens als door computers kunnen worden geïdentificeerd.
- AI-producten die emoties kunnen herkennen e/o die biometrische gegevens kunnen verwerken moeten menselijke gebruikers expliciet waarschuwen over de manier hoe hun data wordt verwerkt en de doelen van de verwerking.
- Bij audio- beeld-, videomateriaal die geproduceerd is met/door een AI-product om een “deep fake” te genereren moet een duidelijke aanduiding aanwezig zijn die aangeeft dat de inhoud geproduceerd is door/met AI en dat het resultaat een “deep fake” is. Deze “geproduceerd met AI” aanduiding moet zowel door de mens als door computers kunnen worden geïdentificeerd.

Bijlage 4 – Aandachtsgebieden die in een EU-databank moeten worden geregistreerd

- Beheer en exploitatie van kritieke infrastructuur
- Onderwijs en beroepsopleiding
- Werkgelegenheid, personeelsbeheer en toegang tot zelfstandige arbeid
- Toegang tot en gebruik van essentiële particuliere diensten en openbare diensten en uitkeringen
- Rechtshandhaving
- Migratie, asiel en beheer van grenscontroles
- Ondersteuning van rechterlijke instanties bij het uitleggen van feiten en toepassing van het recht

Bijlage 5 – Hoog risico systemen en veiligheidscomponenten volgens de AI-wet

AI-systemen met een hoog risico op grond van artikel 6, lid 2, zijn de vermelde AI-systemen op de volgende gebieden:

1. Biometrie, voor zover het gebruik ervan is toegestaan op grond van het toepasselijke Unierecht of nationale recht:

a) systemen voor biometrische identificatie op afstand.

Dit geldt niet voor AI-systemen die bedoeld zijn om te worden gebruikt voor biometrische verificatie met als enig doel te bevestigen dat een specifieke natuurlijke persoon de persoon is die hij of zij beweert te zijn;

b) AI-systemen die bedoeld zijn om te worden gebruikt voor biometrische categorisering op basis van gevoelige of beschermde eigenschappen of kenmerken, of op basis van wat uit die eigenschappen of kenmerken wordt afgeleid;

c) AI-systemen die bedoeld zijn om te worden gebruikt voor emotieherkenning.

2. Kritieke infrastructuur: AI-systemen die bedoeld zijn om te worden gebruikt als veiligheidscomponent bij het beheer of de exploitatie van kritieke digitale infrastructuur, wegverkeer of bij de levering van water, gas, verwarming en elektriciteit.

3. Onderwijs en beroepsopleiding:

a) AI-systemen die bedoeld zijn om te worden gebruikt voor het bepalen van toegang of toelating tot of het toewijzen van natuurlijke personen aan instellingen voor onderwijs en beroepsonderwijs op alle niveaus;

b) AI-systemen die bedoeld zijn om te worden gebruikt voor het evalueren van leerresultaten, ook wanneer die resultaten worden gebruikt voor het sturen van het leerproces van natuurlijke personen in instellingen voor onderwijs en beroepsonderwijs op alle niveaus;

c) AI-systemen die bedoeld zijn om te worden gebruikt voor het beoordelen van het passende onderwijsniveau dat een persoon zal ontvangen of waartoe hij toegang zal hebben, in het kader van of binnen instellingen voor onderwijs en beroepsonderwijs op alle niveaus;

d) AI-systemen die bedoeld zijn om te worden gebruikt voor het monitoren en detecteren van ongeoorloofd gedrag van studenten tijdens toetsen in de context van of binnen instellingen voor onderwijs en beroepsonderwijs op alle niveaus.

4. Werkgelegenheid, personeelsbeheer en toegang tot zelfstandige arbeid:

a) AI-systemen die bedoeld zijn om te worden gebruikt voor het werven of selecteren van natuurlijke personen, met name voor het plaatsen van gerichte vacatures, het analyseren en filteren van sollicitaties, en het beoordelen van kandidaten;

b) AI-systemen die bedoeld zijn om te worden gebruikt voor het nemen van besluiten die van invloed zijn op de voorwaarden van arbeidsgelateerde betrekkingen, de bevordering of beëindiging van arbeidsgelateerde contractuele betrekkingen, voor het toewijzen van taken op basis van individueel gedrag of persoonlijke eigenschappen of kenmerken, of voor het monitoren en evalueren van prestaties en gedrag van personen in dergelijke betrekkingen.

5. Toegang tot en gebruik van essentiële particuliere en publieke diensten en uitkeringen:

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

6. Rechtshandhaving, voor zover het gebruik ervan is toegestaan op grond van het toepasselijke Unierecht of nationale recht:

- a) AI-systemen die bedoeld zijn om door of namens rechtshandhavingsinstanties, of door instellingen, organen of instanties van de Unie ter ondersteuning van rechtshandhavingsinstanties of namens hen, te worden gebruikt om het risico te beoordelen dat een natuurlijke persoon het slachtoffer wordt van strafbare feiten;
- b) AI-systemen die bedoeld zijn om door of namens rechtshandhavingsinstanties of door instellingen, organen of instanties van de Unie ter ondersteuning van rechtshandhavingsinstanties te worden gebruikt als leugendetector of soortgelijke instrumenten;
- c) AI-systemen die bedoeld zijn om door of namens rechtshandhavingsinstanties of door instellingen, organen of instanties van de Unie ter ondersteuning van rechtshandhavingsinstanties te worden gebruikt om de betrouwbaarheid van bewijsmateriaal tijdens het onderzoek naar of de vervolging van strafbare feiten te beoordelen;
- d) AI-systemen die bedoeld zijn om door of namens rechtshandhavingsinstanties of door instellingen, organen of instanties van de Unie ter ondersteuning van rechtshandhavingsinstanties te worden gebruikt om te beoordelen hoe groot het risico is dat een natuurlijke persoon (opnieuw) een strafbaar feit zal plegen, niet uitsluitend op basis van profilering van natuurlijke personen als bedoeld in artikel 3, punt 4, van Richtlijn (EU) 2016/680, of om persoonlijkheidskenmerken en eigenschappen of eerder crimineel gedrag van natuurlijke personen of groepen te beoordelen;
- e) AI-systemen die bedoeld zijn om door of namens rechtshandhavingsinstanties of door instellingen, organen en instanties van de Unie ter ondersteuning van rechtshandhavingsinstanties te worden gebruikt om natuurlijke personen te profileren als bedoeld in artikel 3, punt 4, van Richtlijn (EU) 2016/680, tijdens het opsporen, onderzoeken of vervolgen van strafbare feiten.

7. Migratie-, asiel- en grenstoezichtsbeheer, voor zover het gebruik ervan is toegestaan op grond van het toepasselijke Unierecht of nationale recht:

- a) AI-systemen die bedoeld zijn om door of namens bevoegde overheidsinstanties of door instellingen, organen of instanties van de Unie te worden gebruikt als leugendetector of soortgelijke hulpmiddelen;
- b) AI-systemen die bedoeld zijn om door of namens bevoegde overheidsinstanties of door instellingen, organen of instanties van de Unie te worden gebruikt om risico's te beoordelen, waaronder een veiligheidsrisico, een risico op illegale migratie of een gezondheidsrisico, uitgaat van een natuurlijke persoon die voornemens is het grondgebied van een lidstaat te betreden of dat heeft gedaan;
- c) AI-systemen die bedoeld zijn om door of namens bevoegde overheidsinstanties of door instellingen, organen of instanties van de Unie te worden gebruikt om bevoegde overheidsinstanties bij te staan bij de behandeling van aanvragen voor asiel, visa of verblijfsvergunningen en bij de behandeling van aanverwante klachten in verband met het al dan niet in aanmerking komen van de natuurlijke personen die een aanvraag voor een status indienen, met inbegrip van hieraan gerelateerde beoordelingen van de betrouwbaarheid van bewijsmateriaal;
- d) AI-systemen die bedoeld zijn om door of namens bevoegde overheidsinstanties, of door instellingen, organen of instanties van de Unie, te worden gebruikt in het kader van migratie-, asiel- of grenstoezichtbeheer, met het oog op het opsporen, herkennen of identificeren van natuurlijke personen, met uitzondering van de verificatie van reisdocumenten.

8. Rechtsbedeling en democratische processen:

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

Bijlage 6 – Verboden AI-systemen

- Subliminale technieken, manipulatie en misleiding
- Misbruik van kwetsbaarheden
- Biometrische profilering
- Sociale scoring
- Voorspellende handhaving
- Verrijking van databases voor gezichtsherkenning
- Emotieherkenning
- Real-time biometrische toepassingen

Bijlage 7 – Verboden criminele handelingen

- Terrorisme
- Seksuele misbruik van minderjarigen
- Onwettelijke handel van drugs en verdovende stoffen
- Onwettelijke handel van wapens, explosieven en munitie
- Moord of ernstige letsel
- Handel van organen en menselijke lichaamsdelen
- Onwettelijke handel van radioactieve materialen
- Gijzeling van personen
- Daden strafbaar onder de jurisdictie van de het Internationaal Strafhof
- Gijzeling van schepen en vliegtuigen
- Verkrachting
- Milieucriminaliteit
- Georganiseerde misdaad
- Sabotage
- Deelname in criminele organisaties die in één of meerdere van de bovenstaande activiteiten participeren

Verklarende begrippenlijst

Deep Learning	Onderdeel van Machine Learning, waarbij kunstmatige Neural Networks grote hoeveelheden data verwerken.
Doelspecifieke AI (Narrow AI)	Systemen die ontworpen en getraind zijn om een (aantal) specifieke functie(s) uit te voeren of die bruikbaar zijn binnen een specifiek veld/discipline.
DPIA	Data protection impact assessment. Noodzakelijk om uit te voeren bij elke toepassing waarvan het vermoeden is dat verwerking van gevoelige gegevens plaatsvindt. Een formulier om te bepalen of dat nodig is, een quickscan, is te vinden op de Sharepoint-pagina Informatie Veilig Werken.
Expert Systems	Een concept waarbij een AI-product het principe “als dit ingevoerd wordt, dan gebeurt er het volgende” gebruikt. Zo genoemd omdat de eerste modellen door menselijke experts in hun vakgebied geprogrammeerd werden.
Generalistische AI (General Purpose AI)	AI die capabel is om meerdere soorten resultaten (output) te produceren en toepassingen kent voor meerdere doeleinden en bij meerdere kennisdomeinen. Een Voorbeeld hiervan is de chatbot ChatGPT.
IAMA	Algoritme impact assessment, vergelijkbaar met een DPIA maar dan specifiek voor algoritmes.
Input	Gegevens die in een computerprogramma ingeladen worden om te verwerken. Dit leidt tot een output.
Machine Learning	Een methode om computers zelf informatie te laten associëren zonder afhankelijk te zijn van vooraf geïmplementeerde regels en condities.
Neural Networks	Een samenstelling van eenvoudige processors ('neuronen') met een hoge mate van onderlinge connectie, die informatie met elkaar uitwisselen in een manier die analoog is aan hoe het menselijke brein werkt.
Hallucineren	Het genereren van informatie middels een statistische berekening en waarschijnlijk is volgens een AI-model, maar feitelijk onjuist is.
Output	Het resultaat van een door een computerprogramma uitgevoerde verwerking van gegevens.

Bibliografie

- AIVD. (2023). *AI-systemen-ontwikkel-ze-veilig*. Opgehaald van www.aivd.nl:
<https://www.aivd.nl/documenten/publicaties/2023/02/15/ai-systemen-ontwikkel-ze-veilig>
- Center for Research on Foundation Models (CRFM). (2023). *The foundation Model Transparency Index*. Opgehaald van Stanford University: <https://crfm.stanford.edu/fmti/>
- Europees Parlement en de Raad. (2001). *Richtlijn 2001/95/EG van het Europees Parlement en de Raad inzake algemene productveiligheid*. Opgehaald van Toegang tot de wetgeving van de Europese Unie: <https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:02001L0095-20100101>
- Europese Commissie. (2023). *AI-verordening: eerste regels voor artificiële intelligentie*. Opgehaald van Europees Parlement - Nieuws:
<https://www.europarl.europa.eu/news/nl/headlines/society/20230601STO93804/ai-verordening-eerste-regels-voor-artificiele-intelligentie>
- Microsoft Corporation. (2023). *Bouw een fundament voor AI-succes: een gids voor leiders*. Microsoft Corporation.
- Miller, K. (2023). *Introducing The Foundation Model Transparency Index*. Opgehaald van Stanford University: <https://hai.stanford.edu/news/introducing-foundation-model-transparency-index>
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2019). *Beleidsbrief AI, publieke waarden en mensenrechten*. Den Haag.
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2023). *Kamerbrief over voorlopig standpunt voor Rijksorganisaties bij het gebruik van generatieve AI*. Opgehaald van Rijksoverheid.nl: <https://open.overheid.nl/documenten/814ad0a2-7e14-4fc4-8dac-1d4a3e0b02ba/file>
- Rijksoverheid. (2025). *Het overheidsbrede standpunt voor de inzet van generatieve AI*. Opgehaald van Rijksoverheid.nl:
<https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/publicaties/2025/04/22/het-overheidsbrede-standpunt-voor-de-inzet-van-generatieve-ai/Het+overheidsbrede+standpunt+voor+de+inzet+van+generatieve+AI.pdf>