AUTORITEIT
PERSOONSGEGEVENS

AP Inzet Artificial Intelligence Act

Versie 15 maart 2022

Belang van verantwoorde en veilige AI

- Van gezichtsherkenning, medische diagnoses, fraudebestrijding en het besturen van industriële processen tot de selectie van ons dagelijkse nieuws: kunstmatige intelligentie (AI) en algoritmes hebben steeds meer invloed op ons leven en onze samenleving.
- AI-systemen bieden kansen, maar ook steeds grotere risico's voor zowel de samenleving als de rechten en vrijheden van het individu.
- Mensen raken de grip op hun gegevens kwijt en groepen (kwetsbare) mensen kunnen worden gediscrimineerd of uitgesloten van bepaalde producten of diensten. Maar ook de financiële markten of de waterwerken in Nederland kunnen risico's ondervinden door ondeugdelijke werking van AI.

Proces van de AI Act

- De Europese Commissie heeft in het voorjaar 2021 een voorstel gedaan: *Proposal for a Regulation on artificial intelligence*, de Artificial Intelligence Act (AI Act).
- De AI Act wordt nu besproken in de Europese Raad en het Europees Parlement.
- De Europese privacytoezichthouders – verenigd in de European Data Protection Board (EDPB) - ondersteunen de opzet van het voorstel, maar hebben ook zorgen geuit over de AI Act.

Inzet Autoriteit Persoonsgegevens onderhandelingen AI ACT

1. Hoog risico AI-systemen vereisen strenge toetsing

- De AI Act richt zich vooral op AI-systemen met een hoog risico. Een AI-systeem krijgt het stempel 'hoog risico' als het valt onder bepaalde 'toepassingen' of 'categorieën'. Te denken valt aan: migratie- en asielsystemen, kritieke infrastructuur en opleidingen en trainingen.
- Er is onderscheid in twee soorten hoog risico:

  Lijst 1) AI toepassingen met een hoog risico waarvoor self assessment verplicht is;
  Lijst 2) AI toepassingen met een hoog risico die door een externe instantie op 'conformiteit' getoetst moeten worden.

- Voor 'biometrische systemen voor identificatie op afstand' is nu bepaald dat zij altijd door een externe instantie op conformiteit getoetst moet worden (lijst 2). Voor andere hoog risico systemen is nog niet bepaald op welke lijst zij horen. De AP adviseert dat alle AI toepassingen die een hoog risico hebben door een externe partij op conformiteit worden getoetst.
- De AI Act verbiedt ook een aantal toepassingen van AI-systemen die een onacceptabel risico vormen voor de rechten en vrijheden van het individu: denk aan social scoring en manipulatieve AI-systemen. Op dergelijke verboden, met name biometrische systemen, worden uitzonderingen geformuleerd in de AI Act. De AP vindt het van groot belang dat deze toepassingen zonder uitzondering ook echt verboden worden, en hier in de onderhandelingen niet aan wordt getornd.

2. Geef toezichthouders rol risicobepaling AI-systemen

- De Europese Commissie is in het voorstel degene die bepaalt welk (nieuw) type AI-toepassing in welke risicocategorie wordt ingedeeld. Met andere woorden, het is de Commissie die bepaalt of een hoog risico systeem aan een self assessment moet worden onderworpen of extern getoetst moet worden. De AP adviseert met klem ook de nationale toezichthoudende autoriteiten invloed op de lijst te geven en dit vast te leggen in de Act . Deze toezichthouders hebben de expertise en praktijkkennis om te beoordelen wat gevaarlijk of risicovol is voor de maatschappij en burger.
- Het voorgestelde proces om wijzigingen in de lijst aan te brengen is te traag voor deze zich snel ontwikkelende technologie. Pas na 3 jaar wordt de lijst met hoog-risico-toepassingen bijgewerkt, daarna elke 4 jaar. De AP adviseert om aanpassingen van de lijst jaarlijks mogelijk te maken.

3. Organiseer sterk toezicht op AI-systemen

- De AI Act raakt aan het toezichtveld van verschillende toezichthouders: gegevensbescherming, marktregulering, productregulering etc. Gezaghebbend en voldoende toezicht is van groot belang.
- De zorgen die bestaan over AI-systemen gaan in veel gevallen over het gebruik van persoonsgegevens. Geef privacy toezichthouders dus een belangrijke rol, in lijn met de al in de AI Act vastgelegde rol van de EDPS en de algoritmewaakhond bij de AP uit het coalitieakkoord.
- AI moet worden gezien als een systeemtechnologie met een grote impact op de samenleving en individuen. Dit vergt een gezaghebbende toezichthouder die in staat is met veel partijen samen te werken in een veld dat nog sterk in ontwikkeling is. De AP acht het huidige voorstel van maximaal 25 fte per land niet realistisch.

AUTORITEIT
PERSOONSGEGEVENS

Nadere toelichting AI Act en de AP standpunten

Belang van verantwoorde en veilige AI

Van gezichtsherkenning, medische diagnoses, fraudebestrijding, het besturen van industriële processen en de selectie van ons dagelijkse nieuws: kunstmatige intelligentie (AI) en algoritmes hebben steeds meer invloed op ons leven en onze samenleving. Niet alleen bedrijven, maar ook steeds meer publieke organisaties op alle niveaus maken er gebruik van. Dit biedt natuurlijk kansen, maar ook steeds grotere risico's voor zowel de samenleving als de rechten en vrijheden van het individu. Mogelijk raken mensen de grip op hun gegevens kwijt, worden groepen (kwetsbare) mensen gediscrimineerd of uitgesloten van bepaalde producten of diensten. Maar ook kritieke infrastructuren zoals de financiële markten of de waterwerken in Nederland kunnen risico's ondervinden door ondeugdelijke werking van AI. Goede regelgeving en gezaghebbend toezicht is daarom juist nu van groot belang.

Afgelopen voorjaar presenteerde de Europese Commissie het *Proposal for a Regulation concerning artificial intelligence*, de Artificial Intelligence Act (AI Act). Hierover wordt nu gesproken in de Europese Raad en het Europees Parlement. De Europese privacytoezichthouders – verenigd in de European Data Protection Board (EDPB) - ondersteunen de intentie van het voorstel maar hebben ook hun zorgen geuit over de AI Act. [1] [2]

In deze toelichting geeft de AP een korte beschrijving van de AI Act, tonen we de samenhang met de AVG en lichten we de voorstellen ter versterking van de AI Act toe. De AP sluit hierin aan bij de adviezen die de EDPB heeft uitgebracht.

De AI Act

- De AI Act is gericht op aanbieders, gebruikers, gemachtigden, importeurs en distributeurs van AI-systemen.
- De AI Act kijkt naar een AI-systeem als een product en past een EU standaardpakket voor markttoelating (denk aan CE markering) en productregelgeving toe op AI-systemen, denk aan regulering, uitvoering en toezicht.
- De Act maakt onderscheid tussen verschillende risicocategorieën:
    - De AI Act verbiedt een aantal toepassingen van AI-systemen die een onacceptabel risico vormen voor de rechten en vrijheden van het individu. Te denken valt aan *social scoring* en manipulatieve AI-systemen. Manipulatieve AI-systemen worden omschreven als systemen die bijvoorbeeld gebruik maken van een kwetsbaarheid van een specifieke groep personen zoals leeftijd of handicap om het gedrag op een schadelijke wijze te verstoren.
    - AI-systemen met een hoog risico krijgen een aantal nieuwe verplichtingen. Deze komen naast bestaande verplichtingen uit bijvoorbeeld de Algemene Verordening

[1] EDPB-EDPS Joint Opinion 5/2021, EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) | European Data Protection Board (europa.eu)

[2] Statement on the Digital Services Package and Data Strategy, Adopted on 18 November 2021, Statement on the Digital Services Package and Data Strategy | European Data Protection Board (europa.eu)

Gegevensbescherming (AVG). Binnen de categorie AI-systemen is er onderscheid in twee soorten hoog risico:
    - AI-toepassingen waarvoor een *self assessment* verplicht is;
    - AI-toepassingen die door een externe instantie op conformiteit getoetst moeten worden.
  - Daarnaast bevat de AI Act transparantieverplichtingen voor AI-toepassingen die een beïnvloedend karakter (kunnen) hebben zoals chatbots of deepfakes.
  - Op alle andere AI systemen die niet in de verordening worden genoemd, is er geen sprake van nieuwe verplichtingen.

- De AI Act gaat uit van een nationale toezichthoudende autoriteit die in samenwerking met nationale bevoegde autoriteiten toeziet op de naleving van de AI Act. Deze nationale toezichthoudende autoriteit neemt deel in de European AI Board (EAIB). Er blijft bestaand (sectoraal) toezicht op nationaal niveau bij de bestaande toezichthouders op grond van andere wet- en regelgeving, ook wanneer het AI-systemen betreft. Als een AI-systeem deel uitmaakt van een ander product wordt het met dat andere product 'meegecertificeerd' volgens de regels die gelden voor dat product.
- Een exploitant[3] van een AI-systeem kan een boete krijgen tot 30 miljoen euro of tot 6 procent van de wereldwijde jaaromzet bij overtreding van de AI Act.

Verhouding AI Act en AVG

Het uitgangspunt van de AVG is het grondrecht op gegevensbescherming. Hierbij is een belangrijke rol weggelegd voor de controle over de eigen persoonsgegevens. Als burger kun je dus zelf je recht uitoefenen richting partijen die jouw persoonsgegevens verwerken. De AI Act beziet een AI-systeem als een product, en kijkt dus vanuit productregulering. Dit betekent dat productveiligheid van het AI systeem centraal staat en vooraf wordt gecontroleerd. Burgers worden dus op een indirecte manier beschermd tegen ondeugdelijke AI-systemen. Dat betekent echter ook dat burgers geen expliciete rol in de AI Act hebben. Zij kunnen dus niet direct hun rechten uitoefenen, zoals zij dat wel kunnen onder de AVG. Dit is op zich ook niet nodig als ondeugdelijke AI-systemen van de markt worden geweerd en betrokkenen onverkort hun rechten onder de AVG kunnen uitoefenen. In andere woorden: wanneer het vermoeden bestaat dat persoonsgegevens worden verwerkt door een ondeugdelijk AI-systeem, kunnen burgers dus gebruik maken van hun rechten uit de AVG. Let wel: dit gaat alleen op voor AI-systemen waarin persoonsgegevens worden verwerkt. Om deze reden is het dus belangrijk dat de relatie tussen deze twee verordeningen duidelijk wordt omschreven. Samenvattend:

- De AI Act stelt conformiteitseisen aan AI-systemen gebaseerd op vooraf vastgestelde risico-categorieën.
- De AI Act verplicht het doen van een zogenaamde conformiteitsbeoordeling[4] van een AI-systeem, vóórdat deze op de markt gebracht of in gebruik gesteld wordt. Deze beoordeling heeft als doel dat er vooraf goed wordt gedacht over de kwaliteit en de toepassing van het systeem.
- De AVG reguleert het verwerken van persoonsgegevens, en ziet ook op AI toepassingen waarin persoonsgegevens worden gebruikt.

[3] Een exploitant kan zijn een aanbieder, gebruiker, gemachtigde, importeur of distributeur van een AI-systeem.
[4] AI Act: artikel 3, onder 20

- Persoonsgegevens kunnen zowel worden verwerkt bij het ontwikkelen van een AI-systeem als bij de toepassing van een AI-systeem.
- De AVG kent voor sommige toepassingen de verplichting een gegevensbeschermingseffectbeoordeling (DPIA) uit te voeren vóórdat persoonsgegevens verwerkt mogen worden. Deze verplichting geldt in veel gevallen voor AI-systemen waarin persoonsgegevens worden verwerkt. In een DPIA staan niet de risico's voorop die samenhangen met de kwaliteit van een AI-systeem, maar de risico's die samenhangen met het gebruik van persoonsgegevens.
- AI-systemen waarvoor een conformiteitsbeoordeling moet worden uitgevoerd, verwerken in veel gevallen persoonsgegevens en daarvoor geldt dus ook de DPIA-plicht. Deze twee assessments vullen elkaar aan. Dit betekent dus dat de AI Act zorg draagt voor kwalitatief goede AI-systemen, en de AVG het kader biedt voor de verwerking van persoonsgegevens. Beide verordeningen vullen elkaar dus aan.

Verduidelijk de relatie met andere wetgeving

Door de verschillende uitgangspunten - productregulering in de AI Act, grondrechten in de AVG - is het begrijpelijk dat andere rollen worden gedefinieerd in de verschillende verordeningen. Deze rollen staan vaak wel in relatie tot elkaar. Waar dit het geval is, is het wenselijk om de relatie tussen de rollen onderling te verduidelijken zodat duidelijk wordt voor wie en wanneer welke vereisten van toepassing zijn.
Een voorbeeld hiervan betreft de rollen die in de AI Act is zijn gedefinieerd zoals aanbieder, gebruiker, gemachtigde, importeur en distributeur. In de AVG wordt gesproken over verwerkingsverantwoordelijke en verwerker. De AP adviseert om in de AI Act duidelijk te maken hoe deze termen met elkaar samenhangen. Zeker voor de uitvoering van deze verplichtingen in de praktijk door bijvoorbeeld MKB en startups kan deze toelichting veel betekenen. Dit vereist geen wijziging in het voorstel, maar kan bijvoorbeeld in een overweging worden verduidelijkt.

Nadere toelichting bij de inzet AP AI ACT

1. Hoog risico AI-systemen vereisen strenge toetsing
   - De AI Act richt zich vooral op AI-systemen met een hoog risico. Een AI-systeem krijgt het stempel 'hoog risico' als het valt onder bepaalde 'toepassingen' of 'categorieën'. Te denken valt aan: migratie- en asielsystemen, kritieke infrastructuur en opleidingen en trainingen.
   - Er is onderscheid in twee soorten hoog risico:
     Lijst 1) AI toepassingen met een hoog risico waarvoor self assessment verplicht is;
     Lijst 2) AI toepassingen met een hoog risico die door een externe instantie op conformiteit getoetst moeten worden.
   - Voor 'biometrische systemen voor identificatie op afstand' is nu bepaald dat zij altijd door een externe instantie op conformiteit getoetst moet worden (lijst 2). Voor andere hoog risico systemen is nog niet bepaald op welke lijst zij horen. De AP adviseert dat alle AI toepassingen die een hoog risico hebben door een externe partij op conformiteit worden getoetst.
   - De AI Act verbiedt ook een aantal toepassingen van AI-systemen die een onacceptabel risico vormen voor de rechten en vrijheden van het individu: denk aan social scoring en manipulatieve AI-systemen. Op dergelijke verboden, met name biometrische systemen, worden uitzonderingen geformuleerd in de AI Act. De AP vindt het van groot belang dat deze toepassingen zonder uitzondering ook echt verboden worden, en hier in de onderhandelingen niet aan wordt getornd.

2. Geef toezichthouders rol risicobepaling AI-systemen

De AP vindt het opleggen van zwaardere eisen aan systemen met een hoger risico een goede zaak. Maar wij zijn ook kritisch op bepaalde voorstellen. Zo is de Europese Commissie in het voorstel degene die bepaalt welk (nieuw) type AI-toepassing in welke risico-categorie wordt ingedeeld. Met andere woorden, het is de Commissie die bepaalt of een hoog risico systeem aan een self assessment moet worden onderworpen of extern getoetst moet worden. De AP adviseert met klem ook de nationale toezichthoudende autoriteiten invloed op het samenstellen van de lijst te geven en deze bevoegdheid vast te leggen in de Act. Deze toezichthouders hebben de expertise en praktijkkennis om te beoordelen wat gevaarlijk of risicovol is voor de maatschappij en burger.

Het huidige voorstel om wijzigingen in de lijst aan te brengen is te traag voor deze snel ontwikkelende technologie. Pas na 3 jaar wordt de lijst met hoog-risico-toepassingen bijgewerkt, daarna elke 4 jaar. De AP adviseert om aanpassingen van de lijst jaarlijks mogelijk te maken. En de EAIB zou ook moeten worden geraadpleegd door de Commissie vóór elke wijziging van de lijst. Daarmee wordt geborgd dat specifieke sectorale of nationale risico's en problemen tijdig worden meegenomen in de aanpassingen.

3. Organiseer sterk toezicht op AI-systemen

De AI Act raakt aan het toezichtsveld van verschillende toezichthouders: gegevensbescherming, marktregulering, productregulering etc. Gezaghebbend en voldoende toezicht is van groot belang. In het Commissievoorstel is het toezicht op de naleving van de verordening op de volgende manier vormgegeven:

Europese AI Board (EIAB)

Er komt een Europese AI Board, onder leiding van de Europese Commissie. In de EIAB nemen de nationale toezichthoudende autoriteiten uit de lidstaten deel. Ook de European Data Protection Supervisor (EDPS) zal plaatsnemen in de EIAB. In het voorstel staat dat de Commissie de voorzitter wordt van de EIAB.

Nationaal toezicht

Het voorstel stelt dat elke lidstaat een eigen nationale toezichthoudende autoriteit aanwijst die de taken van de AI Act zal coördineren en plaats zal nemen in de EAIB. Dat kan zowel één van de nationale bevoegde autoriteiten, als een nieuw op te richten autoriteit zijn. Deze nationale toezichthoudende autoriteit zal niet automatisch het toezicht op alle onderdelen van de verordening uitvoeren. Dit moet door nationale bevoegde autoriteiten in samenwerking worden gedaan, waarbij iedere toezichthouder zijn eigen kerntaken en expertise blijft uitvoeren.

Om het systeem van toezicht succesvol te maken is goede samenwerking tussen de nationale bevoegde autoriteiten en de nationale bevoegde autoriteit dus zeer belangrijk. Op deze manier wordt er gebruikt gemaakt van bestaande sectorspecifieke expertise en krijgen ook risico's die niet samenhangen met de verwerking van persoonsgegevens voldoende aandacht. Ook de markt zal door goede samenwerking en coördinatie optimaal kunnen profiteren van de nieuwe taakverdeling.

De zorgen die bestaan over AI-systemen gaan in veel gevallen over het gebruik van persoonsgegevens. Geef privacytoezichthouders dus een belangrijke rol, in lijn met de al in de AI Act vastgelegde rol van de EDPS en in lijn met het toezicht op algoritmen bij de AP zoals bedoeld in het coalitieakkoord. Aanvullende overwegingen hiervoor zijn:

- In artikel 16 VWEU[5] staat dat bij de verwerking van persoonsgegevens onafhankelijk toezicht nodig is. In de AI act wordt niets gezegd over onafhankelijk toezicht, maar dat is dus wel noodzakelijk als het om de bescherming van persoonsgegevens bij AI systemen gaat. De AP is de onafhankelijke toezichthouder op de bescherming van persoonsgegevens en het ligt daarom voor de hand dat de AP de nationale toezichthoudende autoriteit wordt.

- De Nederlandse regering heeft bepaald dat er een toezichthouder op algoritmes bij de AP komt (de algoritmewaakhond). Het lijkt efficiënt het coördinerend toezicht op de AI Act hier ook bij te plaatsen zodat beide rollen in samenhang worden opgezet. Dit betekent vanzelfsprekend dat er bij het vormgeven van een toezichthouder op algoritmes bij de AP scherp gekeken wordt naar de samenhang met het takenpakket van de nationale toezichthoudende autoriteit op de AI Act.

Kortom: de keuze voor de nationale toezichthoudende autoriteit op de AI Act bij de AP zorgt voor een meer geharmoniseerde regelgevingsaanpak, draagt bij aan een consistente interpretatie van de bepalingen en helpt eventuele tegenstrijdigheden in de handhaving van de verordening te vermijden.

Tot slot, AI moet worden gezien als een systeemtechnologie[6] met een grote impact op de samenleving en individuen. Dit vergt een gezaghebbende toezichthouder die in staat is met veel partijen samen te werken in een veld dat nog sterk in ontwikkeling is. De AP acht het huidige voorstel van maximaal 25 fte per land niet realistisch.

Overige aandachtspunten in de AI Act

Bijzondere persoonsgegevens verwerken om vertekening tegen te gaan

In het voorstel staat dat er bijzondere persoonsgegevens mogen worden gebruikt als dit nodig is om *vertekening* in AI-systemen op te sporen of tegen te gaan. [7] Met vertekening wordt bedoeld: fouten in uitkomsten als gevolg van vooringenomenheid bij aannames of door vooroordelen in de trainingsdata.

Hoewel de intentie goed lijkt, vindt de AP dat de noodzakelijkheid van die extra verwerkingen ook echt moeten worden aangetoond. Ook moet helder moet worden gemaakt waarom alternatieve mogelijkheden met een veel kleinere inbreuk op grondrechten, zoals bijvoorbeeld het gebruik van kunstmatig gecreëerde data (zogenaamde synthetische data), geen uitkomst bieden. Uiteraard blijven de overige waarborgen uit de AVG gelden, zoals het uitvoeren van een DPIA en waar nodig het aanvragen van een Voorafgaande Raadpleging bij mogelijk hoge restrisico's.

[5] Verdrag betreffende de werking van de Europese Unie.
[6] Zie *'Opgave AI. De nieuwe systeemtechnologie'*, WRR, 2021.
[7] Artikel 10 lid 5

Heldere Definitie AI systemen

De Europese Commissie gebruikt in haar voorstel een 'brede' definitie van een *artificiële intelligentiesysteem* (AI-systeem).[8] Ook veel minder complexe geautomatiseerde of zelflerende (software)systemen vallen hierdoor onder de AI Act. Echter, de Europese Raad heeft op 29 november 2021 een voorstel gepubliceerd waarin zij een andere, smallere, definitie voorstelt. De AP stelt dat deze nieuwe definitie onduidelijk is en dat dit risico's met zich meebrengt. De AP heeft de voorkeur voor aan een brede maar heldere definitie, boven een mogelijk te nauwe definitie waardoor wellicht niet alle AI-systemen gereguleerd kunnen worden onder de AI Act.

Regulatory sandbox

De AI Act biedt de mogelijkheid voor een *regulatory sandbo*x. Een *regulatory sandbox* is een testomgeving of raamwerk waarbinnen organisaties in een gecontroleerde omgeving kunnen experimenteren, onder supervisie van een nationale bevoegde autoriteit.

Door deze regulatory sandbox creëert de AI Act een extra juridische basis[9] voor het hergebruiken van persoonsgegevens voor experimenten binnen de *regulatory sandbox,* die partijen al eerder rechtmatig voor een ander doel hadden verzameld. Binnen de sandbox mag je die gegevens gebruiken – verder verwerken – voor het trainen van, of experimenteren met AI-systemen voor het beschermen van zwaarwegend algemeen belang op verschillende terreinen. In de tekst is nu opgenomen dat wanneer het gaat om de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, de verdere verwerking gebaseerd moet zijn op het recht van de lidstaten of de Unie.
Voor het beschermen van zwaarwegend algemeen belang op gebied van de openbare veiligheid en volksgezondheid, waaronder ziektepreventie, -beheersing en –behandeling en voor de verbetering van de kwaliteit van het milieu, is niet opgenomen dat de verdere verwerking gebaseerd moet zijn op het recht van de lidstaten of de Unie. Ook voor deze terreinen moet voorzien worden in passende en voldoende waarborgen, zoals het baseren op het recht van de lidstaten of de unie.

[8] AI Act: artikel 3
[9] AI Act: artikel 54