AUTORITEIT
PERSOONSGEGEVENS

Toezicht op AI & Algoritmes

Autoriteit Persoonsgegevens

Over de Autoriteit Persoonsgegevens
Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

AUTORITEIT
PERSOONSGEGEVENS

Inhoudsopgave

1. Inleiding

Artificiële Intelligentie (AI) en algoritmes[1] staan volop in de aandacht van de politiek en de samenleving.[2] Deze aandacht is niet zonder reden. De inzet van algoritmes vindt inmiddels op grote schaal plaats, vaak onder de noemer van AI. Niet alleen private organisaties, maar ook steeds meer publieke organisaties op alle niveaus maker er gebruik van. De inzet van AI en algoritmes gaat samen met hoge verwachtingen, maar versterkt ook de roep om passend toezicht op systemen die gebruik maken van AI en algoritmes.

De Autoriteit Persoonsgegevens is als toezichthouder verantwoordelijk voor het toezicht op de verwerking van persoonsgegevens en daarmee ook op de toepassing van AI en algoritmes waarbij persoonsgegevens worden gebruikt. Er is een helder wettelijk Europees kader dat organisaties en ons als toezichthouder houvast biedt: de Algemene Verordening Gegevensbescherming (AVG). De AVG heeft als doel om de grondrechten en de fundamentele vrijheden van natuurlijke personen te beschermen en om regels vast te stellen betreffende het vrije verkeer van persoonsgegevens. Dit betekent in de praktijk dat de ontwikkeling en het gebruik van de meeste systemen die gebruik maken van AI en algoritmes binnen dit huidige wettelijke kader en daarmee onder het toezicht van de AP valt.

Zoals ook beschreven in het meerjarig visiedocument *Focus AP 2020-2023: 'Dataprotectie in een digitale samenleving'* is AI en algoritmes één van de drie focusgebieden in het toezicht van de AP.

In dit document lichten we het toezicht op AI en algoritmes door de AP op hoofdlijnen toe.

Dit document is opgedeeld in een viertal onderdelen:

- In hoofdstuk 2 wordt kort toegelicht wat AI en algoritmes precies zijn.
- In hoofdstuk 3 wordt het toezichtkader geschetst.
- In hoofdstuk 4 wordt toegelicht hoe de AP het toezicht inricht.
- De bijlage bevat het wettelijk kader.

[1] De technisch juiste benaming van 'algoritmische systemen' wordt vermeden met het oog op de leesbaarheid van de tekst.

[2] De afgelopen periode zijn er meerdere rapporten gepubliceerd zoals deze selectie:
Strategisch Actieplan voor Artificiële Intelligentie, Ministerie van Economische Zaken en Klimaat.
https://www.rijksoverheid.nl/documenten/beleidsnotas/2019/10/08/strategisch-actieplan-voor-artificiele-intelligentie.
Opinion of the Data Ethics Commission, Datenethikkommission.
https://www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_EN_node.html
Toezicht op het gebruik van Algoritmen en overheid. Hooghiemstra en Partners. In opdracht van het Ministerie van Binnenlandse zaken en Koninkrijksrelaties.

2. AI & Algoritmes

2.1 Wat zijn algoritmes?

Algoritmes zijn in principe niet meer dan recepten of stappenplannen en de toepassing van algoritmes is niet nieuw. De inzet van algoritmes vindt inmiddels op grote schaal plaats. Dat geldt niet alleen voor private organisaties, maar ook voor de overheid: van de belastingdienst en de politie tot verschillende gemeentes. Inzet van algoritmes kan voordelen bieden. Bedrijven en organisaties kunnen snel en efficiënt besluiten nemen door grote hoeveelheden data te analyseren. Denk aan routeplanning of dienstverlening aan klanten. Maar denk ook aan de mogelijkheden die deze technologie biedt in bijvoorbeeld de gezondheidszorg.

2.2 Wat is AI?

Het wetenschapsgebied artificiële intelligentie (AI) heeft de laatste tien jaar een enorme ontwikkeling doorgemaakt, met name op het gebied van de mogelijkheden van machine learning, neural networks en deep learning. Door deze ontwikkelingen worden algoritmische beslismodellen krachtiger en complexer. De verhoudingen tussen de mens en de machine zijn veranderd.

In de praktijk wordt veelal gesproken over de toepassing van AI-systemen. Systemen die nu getypeerd worden als 'Artificiële Intelligentie' zijn in de praktijk gebaseerd op 'Machine Learning'. Bij Machine Learning wordt, op basis van algoritmes en grote hoeveelheden voorbeelddata, een computer getraind om een bepaalde taak uit te voeren. Dit in tegenstelling tot het programmeren van een specifiek vooraf ontworpen recept of stappenplan. Belangrijke uitwerkingen van machine learning algoritmes zijn neural networks, deep learning en reinforced learning. Veel van deze systemen worden ingezet voor patroonherkenning waarbij een set voorbeelddata gebruikt wordt om het systeem te trainen.

Neural networks zijn geïnspireerd op het menselijk brein en hebben de mogelijkheid om in netwerken te leren. Deep learning zijn gelaagde netwerken waarin hiërarchie en abstracties kunnen worden geleerd. Machine Learning systemen kunnen ook zelfstandig zonder begeleiding leren, bijvoorbeeld door het systeem zelf verbanden te laten leggen. Reinforced learning betreft systemen die zelfstandig leren door te reageren op situaties en data, bijvoorbeeld autonome voertuigen maken hier gebruik van. Zo gauw een autonoom voertuig een situatie tegenkomt en daarin een keuze maakt, wordt de uitkomst van deze keuze naderhand versterkt indien het effect voldoet aan de gestelde eisen. Op deze manier leert een voertuig om objecten te ontwijken, de rijbaan te volgen, of in een file te rijden.

Het onderscheid tussen stapsgewijze en lerende algoritmes is voor de toepasselijkheid van de AVG en het toezicht van de AP verder niet relevant: zolang er persoonsgegevens worden verwerkt is de AP bevoegd om toezicht te houden.

2.3 Risico's

De inzet van AI en algoritmes kent ook risico's. Allereerst bestaat het risico van oneerlijke, bevoordeelde of zelfs discriminatoire uitkomsten bij gebruik van algoritmische systemen.[3] Dit kan verschillende oorzaken hebben.

Discriminatie kan een bewuste keuze zijn van de ontwikkelaar of van de gebruiker van een systeem. Maar de uitkomst kan ook een gevolg zijn van een slecht ontworpen stappenplan of, bij AI, van de gebruikte

[3] In de literatuur worden deze risico's samengevat onder de noemer *unfairness*.

dataset, dit zijn de (persoons)gegevens die zijn gebruikt om het algoritme te ontwikkelen ('trainen'). De dataset kan bevoordeelde, oneerlijke of discriminatoire overtuigingen of gedragingen bevatten, of simpelweg het gedrag of de voorkeuren van de meerderheid reflecteren.

Alle datasets zullen in de praktijk beperkingen kennen en waarborgen behoeven om bias en ongewenste resultaten te verminderen. Als dit soort datasets worden gebruikt om algoritmische systemen te trainen kan dit leiden tot onbehoorlijke of oneerlijke uitkomsten voor specifieke groepen of individuen. Daarnaast kan een dergelijke uitkomst de onbedoelde bijkomstigheid zijn van hoe een systeem is ontworpen of hoe deze wordt gebruikt.

Ten tweede bestaat de neiging bij het ontwikkelen en gebruiken van algoritmische systemen om zoveel mogelijk gegevens te verzamelen. Hierbij is de aanname dat hoe meer data wordt gebruikt om de systemen te trainen, hoe beter deze systemen worden. Dit betekent dat er een perverse prikkel kan ontstaan om te veel, te lang en onnodig veel data te verzamelen, bewaren en verder te verwerken.

Ten derde wordt het door de toenemende complexiteit van algoritmes steeds moeilijker om de interne logica van deze systemen te begrijpen en uit te leggen: er ontstaat een *black box*. Dit zorgt ervoor dat een betrokkene geen zicht meer heeft op wat er met zijn gegevens gebeurd. Het verlies van menselijke autonomie is een uiterste consequentie.

3. Toezichtkader AI & algoritmes

Als in een algoritme – ongeacht het type - persoonsgegevens worden gebruikt, valt deze onder het toezicht van de AP. De privacywetgeving biedt belangrijke kaders voor het toezicht op algoritmes waarin persoonsgegevens worden gebruikt.

In de Algemene verordening gegevensbescherming (AVG) zijn rechtmatigheid, behoorlijkheid en transparantie als kernbeginselen opgenomen en nader uitgewerkt in verschillende normen.

Ook is als beginsel vastgelegd dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van alle beginselen uit de AVG, en dat ook kan aantonen. Deze verantwoordingsplicht is in de AVG uitgewerkt in verschillende instrumenten, die goede handvatten bieden voor de wijze waarop de AP toezicht op algoritmes kan vormgeven. Voorbeelden van deze (verantwoordings-)instrumenten zijn het Data Protection Impact Assessment (DPIA) en de Voorafgaande Raadpleging (VR). Tot slot stelt de AVG extra eisen aan de situatie wanneer er sprake is van uitsluitend geautomatiseerde besluitvorming, dat wil zeggen zonder menselijke tussenkomst.

3.1 Rechtmatigheid, behoorlijkheid en transparantie

In het toezicht op algoritmes bieden de beginselen van 'rechtmatigheid', 'transparantie' en 'behoorlijkheid' een goed aangrijpingspunt. De AVG bevat duidelijke normen over wanneer het rechtmatig is om persoonsgegevens te verwerken. Ook schrijft de wet voor dat verwerkingsverantwoordelijke organisaties transparant moeten zijn over welke persoonsgegevens zij verwerken, met welk doel en de wijze waarop die gegevens worden verwerkt. Het begrip behoorlijkheid (fairness) kan worden ingevuld aan de hand van casuïstiek en bestaande normen.[4]

[4] In de AVG wordt het begrip 'behoorlijkheid' gebruikt. In het dagelijks taalgebruik zal er vaker worden gesproken over 'eerlijkheid'. Wij volgen in dit document de wet en spreken over 'behoorlijkheid'.

Daarnaast is er in de AVG opgenomen welke informatie er – proactief of op verzoek - moet worden gegeven over het verwerken van persoonsgegevens in algoritmes aan degenen op wie deze persoonsgegevens betrekking hebben (de 'betrokkene').[5] Zo is het onder andere verplicht om, als er sprake is van profilering en/of geautomatiseerde besluitvorming, dit kenbaar te maken. Daarbij moet in bepaalde gevallen ook nuttige informatie worden gegeven over de onderliggende logica van het algoritme, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene. In het geval van profilering heeft de betrokkene het recht om daartegen bezwaar te maken.[6]

Een algoritme beoordelen op behoorlijkheid (fairness) is op zichzelf complex maar mogelijk met de juiste middelen en kennis. De vraag of een algoritme of een uitkomst van een algoritme 'fair' of behoorlijk is, is immers sterk verweven met de omstandigheden van het geval, maar daarnaast ook met mogelijk subjectieve opvattingen over rechtvaardigheid. Een verwerkingsverantwoordelijke zal zelf actief moeten verantwoorden en motiveren waarom een algoritme fair is en het gebruik van het gekozen algoritme niet leidt tot onbehoorlijke uitkomsten.

Desalniettemin is het actief bevorderen van transparantie over algoritmes belangrijk voor onze democratische rechtsstaat. Zo bezien is transparantie niet alleen van belang voor betrokkenen zelf, maar ook voor andere partijen, zoals de media, belangenorganisaties in het maatschappelijk veld en andere toezichthouders.

3.2 Verantwoordingsplicht

Ook de verantwoordingsplicht geeft handvatten voor het toezicht op algoritmes. Zo moet een verwerkingsverantwoordelijke verplicht een register bijhouden, waarin hij activiteiten waarbij persoonsgegevens worden verwerkt, inclusief de doeleinden van die verwerkingen en de gebruikte categorieën persoonsgegevens, beschrijft.[7]

Ook moet een organisatie die algoritmes gebruikt vooraf in kaart brengen welke risico's er hierdoor voor de rechten en vrijheden van personen ontstaan. Bij het ontwerpen en bij het gebruik van algoritmische systemen moeten die risico's zoveel mogelijk worden voorkomen, onder andere door het nemen van gepaste waarborgen en maatregelen; *dataprotection by design.*

Concreet betekent dat vooraf goed nadenken over het ontwerp van het systeem: is het gekozen algoritme passend bij het doel waarvoor het wordt ingezet? Ook betekent dit het testen van de werking van het algoritme en gepaste maatregelen en waarborgen implementeren voordat het systeem gebruikt wordt. Het gaat daarbij bijvoorbeeld over wat er gebeurt wanneer algoritmes onbedoeld een verkeerde uitkomst geven en de vraag of door het gebruik van algoritmes misschien bepaalde groepen in de samenleving stelselmatig worden gediscrimineerd. De beoordeling over de risico's, maatregelen en waarborgen moet regelmatig opnieuw worden beoordeeld.

Daarnaast moet een verwerkingsverantwoordelijke voorafgaand aan een bepaalde verwerking een beoordeling uitvoeren van het effect hiervan op de bescherming van persoonsgegevens. Dit is vereist als de verwerking - gelet op de aard, de omvang, de context en de doeleinden - waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

[5] Artikel 13, 14 en 15 AVG.
[6] Artikel 21 AVG.
[7] Artikel 30 AVG.

Deze gegevensbeschermingseffectbeoordeling, ook wel Data Protection Impact Assessment (DPIA) genoemd, is bij het gebruik van algoritmische systemen veelal verplicht. In een DPIA moet de verwerkingsverantwoordelijke naast een systematische beschrijving van de beoogde verwerkingen en verwerkingsdoeleinden, bijvoorbeeld ook een beoordeling te doen van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden. Met andere woorden: de organisatie moet goed onderbouwen waarom deze bepaalde gegevens gebruikt in een algoritme, wat het doel van het gebruik van een algoritme is, maar ook waarom het nodig is te werken met het gekozen algoritme.

Een ander onderdeel van de DPIA is het beschrijven van risico's voor de rechten en vrijheden van natuurlijke personen, de vraag of deze risico's kunnen worden gemitigeerd en welke maatregelen daarvoor worden getroffen. Zoals in het vorige hoofdstuk is geschetst zouden risico's bij het gebruik van algoritmes bijvoorbeeld kunnen liggen in potentiële discriminatie, bevooroordeeldheid of andere risico's die samenhangen met de vraag of het algoritme 'fair' is. In de DPIA dient hieraan dus in elk geval aandacht te worden besteed. Kortom, de DPIA is een instrument om de verwerking op een juiste wijze te ontwikkelen, in te richten, en te verantwoorden.

Wanneer deze risico's onvoldoende kunnen worden weggenomen is het verplicht een voorafgaande raadpleging te laten doen door de AP, waarbij de AP dient te adviseren over de voorgenomen verwerking van persoonsgegevens.

3.3 Uitsluitend geautomatiseerde besluitvorming

Naast deze algemene verplichtingen, bevat de AVG een verbod op een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor de betrokkene juridische of anderszins aanmerkelijke gevolgen zijn verbonden. In andere woorden, belangrijke besluiten mogen niet worden genomen door alleen een algoritme, zonder menselijke tussenkomst. Er zijn beperkte uitzonderingen op dit verbod.

4. Organisatie van Toezicht

4.1 Toezicht van de AP

De missie van de AP stelt: *De Autoriteit Persoonsgegevens is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt.* Het toezichtveld van de AP is omvangrijk; we houden toezicht op nationale en internationale bedrijven en organisaties, de gehele overheid – inclusief politie en justitie – en ook verenigingen, scholen, stichtingen en individuele burgers. Dit doen we niet alleen in Nederland; data kennen immers geen grenzen. Het toezicht van de AP is bij uitstek grensoverschrijdend.

Het toezien op het juiste inzet van algoritmes waarbij persoonsgegevens worden gebruikt is onderdeel van het werk van de AP. In de voorgaande tekst is beschreven welke normen en kaders de AVG biedt voor deze specifieke toezichtstaak. De verantwoordingsinstrumenten en de beginselen van 'rechtmatigheid', 'behoorlijkheid' en 'transparantie' zullen een belangrijke rol spelen in het toezicht op algoritmische systemen.

Voor de komende periode onderscheidt de AP een aantal werkzaamheden. Zo zal de AP actief voorlichting geven aan de betrokkenen wiens persoonsgegevens in algoritmes worden verwerkt, maar ook aan bedrijven en overheden die algoritmes (gaan) gebruiken. Ook zal de AP voorlichting gaan richten op

Functionarissen voor de Gegevensbescherming (FG). In veel gevallen zullen organisaties die werken met algoritmes een FG moeten aanstellen die intern toezicht houdt en adviseert over verwerkingen.

Daarnaast zullen we verdere invulling geven aan een aantal specifieke verplichtingen. Dit zullen we in het bijzonder doen op het gebied van verplichtingen rondom transparantie en de verantwoordingsverplichtingen van de DPIA. Hierbij kan onderscheid worden gemaakt tussen verplichtingen bij het gebruik van algoritmes in het algemeen en lerende algoritmes, zoals toepassingen die gebruik maken van machine learning. De AP zal hierbij zoveel mogelijk aansluiten bij bestaande (inter-)nationale initiatieven, standaarden en normen.[8] Verder zal de AP de mogelijke totstandkoming van sectorspecifieke gedragscodes op het terrein van de toepassing van AI stimuleren.

Het stelsel van toezicht functioneert voor, tijdens en na een verwerking van persoonsgegevens. Verantwoordingsinstrumenten kunnen worden gecontroleerd. Zowel door bijvoorbeeld het beoordelen van en adviseren over aan de AP voorgelegde voorafgaande raadplegingen, als door het uitvoeren van controlerende onderzoeken en handhaven als er sprake is van een overtreding. Een controlerend onderzoek kan ambtshalve gedaan worden of kan bijvoorbeeld worden geïnitieerd door een klacht of een tip. Hierbij zal de AP rekening houden met het feit dat de werking en de gevolgen van een algoritme moeilijk voor burgers te beoordelen zijn.

4.2 Samenwerking met andere toezichthouders - Europees

Ook in Europees verband zal er de komende jaren worden gewerkt aan normering op het gebied van de inzet van algoritmes. Het onderwerp staat binnen het samenwerkingsverband van Europese privacy toezichthouders - de European Data Protection Board (EDPB) - hoog op de agenda. Begin 2020 heeft de EDPB de risico's van algoritmische systemen en de waarborgen die de AVG biedt, uiteengezet.[9]

De AP zal zich in de komende periode sterk maken voor een adequate en effectieve invulling van toezicht op algoritmes. De AP zet ook in op hechte samenwerking met de Europese toezichthouders, om zo ook op Europees niveau een betere invulling te kunnen geven aan toezicht.

4.3 Samenwerking met andere toezichthouders - nationaal

De AP houdt alleen toezicht op de naleving van wetgeving op het gebied van databescherming. Echter, de ontwikkeling en inzet van algoritmes kan ook gevolgen hebben voor andere (rechts)gebieden, zoals onder andere consumentenrecht, mededingingsrecht en antidiscriminatie. Om deze reden zal de AP ook met andere nationale toezichthouders gaan samenwerken op het terrein van algoritmes en AI. Zo heeft de AP in de ontwikkeling van dit document deskundigen van verschillende departementen, van andere toezichthouders en wetenschappers geraadpleegd.

[8] Bekende initiatieven zijn bijvoorbeeld: FATML: *Fairness, Accountability, and Transparency in Machine Learning*; EU: *Ethics guidelines for trustworthy AI*; AI NOW Institute: *Algorithmic Accountability Policy Toolkit*; en van het Platform voor Informatiecentrum (ECP): *AI Impact Assessment*.

[9] Beantwoording van de brief (31 juli 2019) van Europarlementariër Sophie in 't Veld. https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-mep-sophie-int-velds-letter-unfair-algorithms_en

5. Bijlage: Wettelijk kader

Bij het gebruik van persoonsgegevens in algoritmes is de AVG geheel van toepassing. Hier noemen we een aantal passages uit de AVG die specifiek van toepassing zijn bij het gebruik van algoritmes.

5.1 Beginselen (artikel 5 AVG)

De AVG geeft in het eerste lid, onder a, van artikel 5 drie beginselen weer die aangeven dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is („rechtmatigheid, behoorlijkheid en transparantie").

5.2 Verantwoording (artikel 24 en 25 AVG)

De verwerkingsverantwoordelijke is verantwoordelijk om passende technische en organisatorische maatregelen te treffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Hierbij dient de verwerkingsverantwoordelijke rekening te houden met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen. Deze maatregelen dienen te worden geëvalueerd en indien nodig te worden geactualiseerd. In beginsel dient de verwerking gegevensbescherming te bieden door het ontwerp en de standaardinstellingen.

5.3 Data Protection Impact Assessment en Voorafgaande Raadpleging (artikel 35 en 36 AVG)

Organisaties kunnen verplicht zijn om een data protection impact assessment (DPIA) uit te voeren. Dit is het geval wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt. De DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen. De verwerkingsverantwoordelijke mag in dat geval niet beginnen met het verwerken van gegevens voordat een DPIA (en indien nodig een voorafgaande raadpleging) is uitgevoerd.
Wanneer een DPIA uitwijst dat de verwerking een hoog risico oplevert indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken, dan raadpleegt de verantwoordelijke voorafgaand aan de verwerking de verantwoordelijke toezichthouder. De toezichthoudende autoriteit geeft schriftelijk advies aan de verwerkingsverantwoordelijke over de verwerking.

5.4 Profilering (artikel 4 AVG)

De definitie in artikel 4 sub 4 AVG is: "elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen."

Het gebruik van het woord "evalueren" betekent dat er bij profilering een beoordeling over een persoon gemaakt wordt.

5.5 (Uitsluitend) geautomatiseerde besluitvorming (artikel 22 AVG)

Geautomatiseerde besluiten kunnen met of zonder profilering worden genomen en profilering kan plaatsvinden met en zonder geautomatiseerde besluitvorming. *Uitsluitend* geautomatiseerde besluitvorming is het nemen van besluiten met technologische middelen en zonder menselijke tussenkomst.

5.6 Toepasselijke normen uit de AVG (artikel 2 AVG)

Bij zowel profilering als (uitsluitend) geautomatiseerde besluitvorming is sprake van 'geheel of gedeeltelijk geautomatiseerde verwerking of van de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen' (artikel 2 lid 1 AVG) dus zijn alle bepalingen in de AVG van toepassing op beiden.

5.7 Specifieke normen voor uitsluitend geautomatiseerde besluitvorming (artikel 22 AVG)

Artikel 22 AVG formuleert een verbod op volledig geautomatiseerde individuele besluitvorming die is gebaseerd op profilering als het voor de betrokkene juridische of anderszins aanmerkelijke gevolgen heeft. Het verbod is niet absoluut, lid 2 geeft drie uitzonderingsgronden op het verbod.

"1.De betrokkene heeft het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft.
2.Lid 1 geldt niet indien het besluit:
a) noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;
b) is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene; of
c) berust op de uitdrukkelijke toestemming van de betrokkene.
3.In de in lid 2, punten a) en c), bedoelde gevallen treft de verwerkingsverantwoordelijke passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene, waaronder ten minste het recht op menselijke tussenkomst van de verwerkingsverantwoordelijke, het recht om zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten.
4.De in lid 2 bedoelde besluiten worden niet gebaseerd op de in artikel 9, lid 1, bedoelde bijzondere categorieën van persoonsgegevens, tenzij artikel 9, lid 2, punt a) of g), van toepassing is en er passende maatregelen ter bescherming van de gerechtvaardigde belangen van de betrokkene zijn getroffen."

De wetgever achtte het wenselijk om van de uitzonderingsgrond lid 2 sub b gebruik te maken en heeft in artikel 40 van de UAVG het volgende opgenomen:

"1. Artikel 22, eerste lid, van de verordening geldt niet indien de in die bepaling bedoelde geautomatiseerde individuele besluitvorming, anders dan op basis van profilering, noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust of noodzakelijk is voor de vervulling van een taak van algemeen belang.
2 Bij de geautomatiseerde individuele besluitvorming, bedoeld in het eerste lid, treft de verwerkingsverantwoordelijke passende maatregelen die strekken tot bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene.

3 Indien de verwerkingsverantwoordelijke geen bestuursorgaan is, dan zijn passende maatregelen als bedoeld in het tweede lid, in ieder geval getroffen indien het recht op menselijke tussenkomst, het recht voor betrokkene om zijn standpunt kenbaar te maken en het recht om het besluit aan te vechten, zijn geborgd."

Vragen over de Algemene verordening gegevensbescherming

Op onze website autoriteitpersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de Algemene verordening gegevensbescherming (AVG). Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met het Informatie- en Meldpunt Privacy van de Autoriteit Persoonsgegevens op 088-1805 250.