AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens

Digitalisering, tegenmacht en de bescherming van persoonsgegevens

Oktober 2021

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.

Inleiding

Nederland loopt wereldwijd voorop op het gebied van digitalisering en innovatie. Om die digitale samenleving op een verantwoorde manier vorm te geven is de bescherming van persoonsgegevens essentieel. De bescherming van persoonsgegevens raakt immers alle aspecten van onze samenleving. Het gaat over de kansen voor onze economie, de rol van Big Tech, de fundamenten van onze rechtsstaat, over vrije verkiezingen, over de relatie van de overheid met haar burgers en over de autonomie van burgers. Niet voor niets is de bescherming van persoonsgegevens sinds 2009 een zelfstandig grondrecht, zoals benoemd in het Handvest van de grondrechten van de Europese Unie. Als Autoriteit Persoonsgegevens staan we hier pal voor.

Samenvatting

- **Digitalisering zorgt voor steeds meer data en verzameling van persoonsgegevens;**
- **Rol voor de overheid én bedrijfsleven om dat op verantwoorde manier te doen;**
- **Digitalisering vraagt om dedicated aandacht vanuit het Kabinet, en ook in Europa;**
- **Essentiele rol voor Tweede Kamer bij nieuwe wetgeving en het bieden van tegenmacht, juist ook bij algoritmes.**
- **Voor goed toezicht dient het budget van de AP te groeien van de huidige 25 miljoen naar een structurele financiering van 100 miljoen euro, vergelijkbaar met andere Nederlandse toezichthouders.**

De vaste Kamercommissie Digitale Zaken heeft een belangrijk takenpakket en hiermee een uitdagende en ook eervolle opgave. Digitalisering raakt immers alle departementen en beleidsdossiers, maar ook alle vlakken van onze samenleving. Dat weten wij als AP als geen ander. Wij zien nieuwe innovaties en slimme startups die privacy als hun *unique selling point* inzetten en zich daarmee onderscheiden, maar we zien ook grote misstanden. Van het schenden van de privacy van jonge kinderen door Big Tech, het publiceren van de woonadressen van zzp'ers in het Handelsregister van de KvK, het GGD datalek en toegang tot medische dossiers, tot de discrimerende algoritmes van de Belastingdienst waardoor tienduizenden mensen letterlijk in de knel kwamen.

Het is daarom juist nu van belang om de (publieke) waarden van onze democratie en tegenmacht centraal te zetten in alle vormen van digitalisering. Hier ligt een rol voor de AP én voor de Tweede Kamer. Alleen met instemming van de Tweede Kamer kan immers inbreuk gemaakt worden op grondrechten van burgers. De oproep van de AP is dan ook: wees kritisch, stel vragen, juist als het om heel veel gevoelige gegevens gaat. Alleen dan krijgen wij als Nederland de digitale economie en digitale democratie die we willen.

In deze schriftelijke bijdrage voor het Rondetafelgesprek maakt de AP graag van de gelegenheid gebruik om onze visie met u als Kamercommissie Digitale Zaken te delen. Dit paper gaat eerst in op de ontwikkelingen die de AP ziet, vervolgens over de rol van de AP, haar wettelijke bevoegdheden en de samenwerking met andere toezichthouders. Ook staat de AP speciaal stil bij het gebruik en de risico's van algoritmes.

1. Toekomstige ontwikkelingen

Illegale datahandel, deepfakes, gezichtsherkenning, internet of things, de inzet van algoritmes, volgsoftware, profilering, wearables en smartphonetechnologie – deze ontwikkelingen behoren allemaal tot het werkterrein van de Autoriteit Persoonsgegevens. Het werkgebied is groot en het is dan ook noodzakelijk voor de AP om keuzes te maken. In de AP Focus 2020-2023 heeft de AP haar prioriteiten tot 2023 vastgesteld. Dit betreft de focusgebieden: datahandel, digitale overheid en toezicht op AI en algoritmes. Deze focusgebieden zijn vervolgens weer onderverdeeld in aandachtsgebieden, zoals hieronder in graphic is weergegeven.

Actuele publicaties & ontwikkelingen
Gezien de razendsnelle ontwikkelingen in de digitale wereld, ontwikkelt de AP haar kennis continu. In de afgelopen periode heeft de AP richtlijnen, achtergronddocumenten en adviezen gepubliceerd over:

- de bescherming van persoonsgegevens bij Nederlandse Smart Cities;
- de inzet van gezichtsherkenning;
- guidelines over connected cars;
- targeting op sociale media;
- het gebruik van spraakassistenten;
- de bescherming van persoonsgegevens bij schuldhulpverlening;
- privacy bij verkiezingscampagnes;
- en de inzet van E-health.

Daarnaast geeft de AP onder meer 100 wetgevingsadviezen, en publiceert lasten, boetes etc.

COVID 19
Daarnaast spelen actuele maatschappelijke ontwikkelingen een grote rol. De AP heeft met spoed over een aantal belangrijke COVID -19 (wets)voorstellen geadviseerd, zoals over corona-apps, testbewijzen en veilig thuiswerken.

1.1 Datahandel

We leven in een datagedreven en techno-optimistische wereld, waarin eindeloos veel gegevens worden vastgelegd over betaaltransacties, gezondheid, mobiliteit, het gedrag van mensen etc. Deze data zijn diverser, specifieker, persoonlijker en diepgaander dan ooit tevoren. De beschikbare hoeveelheid data stijgt exponentieel door het toenemend gebruik van digitale diensten, de komst van het internet of things en de overal in verwerkte dataverzamelende sensoren. Voor veel bedrijven (zoals Big Tech) is het op grote schaal verzamelen, gebruiken (voor bijvoorbeeld gepersonaliseerde advertenties) en verkopen van persoonsgegevens een belangrijk – en soms zelfs een primair – onderdeel van hun verdienmodel. Zij verdienen hun geld dus met het gebruik en verkopen van datasets en (zeer) grote hoeveelheden persoonsgegevens.

Deze continue datahonger heeft een dataeconomie gecreëerd, waarbij grote hoeveelheden data zich concentreren bij een steeds kleinere groep spelers. Zij verkopen de data door of verwerken de gegevens tot profielen en verkopen deze door. De focus op alsmaar meer (gekoppelde) data, vaak met het idee dat dit in de toekomst 'handig' kan zijn, brengt risico's met zich mee. Zo is het zorgwekkend wanneer bedrijven de gegevens doorverkopen zonder dat mensen dat weten en zonder dat zij daarvoor toestemming hebben gegeven. Hierdoor kunnen bedrijven bijvoorbeeld ten onrechte beschikken over de medische dossiers, DNA-gegevens of betaalgegevens van mensen. Mensen verliezen dus hun grip op hun gegevens en met een beetje pech worden die gegevens ook nog tegen hun gebruikt. Te denken valt aan afpersing, (banken)fraude, discriminatie, profilering etc. Het is daarom onder andere van groot belang dat bedrijven kennis hebben over de bescherming van persoonsgegevens en verantwoorde digitalisering. Elk groot bedrijf zou een bestuurder of commissaris moeten hebben met verstand van privacy en de digitale wereld.

1.2 Digitale overheid

Naast bedrijven beschikken ook centrale en lokale overheden, uitvoeringsorganisaties en politie en justitie over veel – vaak gevoelige en bijzondere – persoonsgegevens. De AP heeft bijzondere aandacht voor de overheid omdat eenieder onder de overheid 'valt'. Een gebruiker kan immers 'nee' zeggen tegen Google door een andere zoekmachine te gebruiken en 'nee' tegen Facebook door het account op te heffen, maar de overheid wegklikken kan eenvoudigweg niet. Iedereen moet per slot van rekening belastingaangifte doen, een paspoort, zorgtoeslag of kindertoeslag aanvragen, zich inschrijven op een woonadres of zich laten testen bij de GGD. Kortom, we hebben als burger de overheid nodig om ons publieke leven te leiden. Dat betekent dat de overheid een speciale verantwoordelijkheid heeft als het gaat om de verwerking van persoonsgegevens.

Dat geldt des te meer als er bestanden gekoppeld worden. De wet ***Uitwisseling gegevensbescherming door samenwerkingsverbanden*** ligt nu voor in de Eerste Kamer. De Eerste Kamer én veel maatschappelijke organisaties, alsook de AP, zijn uitermate kritisch. Terecht, want de wet regelt niet alleen de juridische basis voor een viertal bestaande samenwerkingsverbanden, maar het zet ook de deur open naar allerlei nieuwe uitwisselingsverbanden, inclusief uitwisseling met private partijen.

Ook op Europees niveau wordt gewerkt aan nieuwe grootschalige informatiesystemen om bijvoorbeeld informatie over bepaalde reisbewegingen te verzamelen. Dit betekent dat de overheid niet alleen meer gegevens verzamelt, maar ook verdere informatie kan 'creëren' door gegevens uit databases naast elkaar te leggen. Hoewel er goede redenen kunnen zijn voor het verzamelen van bepaalde gegevens – bijvoorbeeld om zware criminaliteit te bestrijden – moet de overheid er altijd voor zorgen dat deze initiatieven daadwerkelijk noodzakelijk zijn en niet verder gaan dan nodig is.

De beveiliging van persoonsgegevens bij de overheid laat nog te vaak te wensen over. Slechte beveiliging kan leiden tot een datalek, zoals onlangs bij het UWV en de GGD. Een datalek kan er voor zorgen dat de gegevens van miljoenen Nederlanders in criminele handen terecht komen en gebruikt worden om burgers en bedrijven op te lichten of fraude te plegen. De impact van datalekken bij de overheid is vaak erg groot, omdat het meestal gaat om enorme (gekoppelde) datasets met hierin bijzondere of gevoelige persoonsgegevens. De AP ontving in 2020 maar liefst 23.976 datalekmeldingen; hierdoor zijn de gegevens van duizenden mensen op straat komen te liggen.

Het is aan de overheid om kritisch te zijn op de gegevens die zij wil verzamelen. Wees kritisch bij het vragen van meer gegevens van burgers. Worden de kernbeginselen uit de AVG - rechtmatigheid, behoorlijkheid, transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid' - nageleefd? Is het echt nodig om gegevens te verzamelen? En is het echt nodig dit weer te delen met andere instanties? En zijn onze publieke waarden voldoende geborgd? Gerichte aandacht vanuit het Kabinet en zowel de Eerste Kamer als de Tweede Kamer is hierin ook essentieel.

1.3 Toezicht op algoritmes

Algoritmes staan volop in de aandacht van de politiek en de samenleving. Deze aandacht is niet zonder reden. De inzet van algoritmes vindt inmiddels in veel sectoren plaats, vaak onder de noemer van AI. Niet alleen private organisaties, maar ook steeds meer publieke organisaties op alle niveaus maken er gebruik van. Dit biedt natuurlijk kansen, maar ook grote risico's zoals de toeslagenaffaire en het gebruik van algoritmes bij de Belastingdienst laten zien. Goed toezicht is juist in dit stadium van ontwikkeling van groot belang. Een punt van aandacht is aankomende Europese regulering, zoals de AIR.

1.3.1 Wettelijk kader voor toezicht op algoritmes

Als in een algoritme – ongeacht het type – persoonsgegevens worden gebruikt, valt deze onder het toezicht van de AP. De basis van de bescherming van persoonsgegevens is het Handvest van de grondrechten van de EU. De Algemene Verordening Gegevensbescherming (AVG) biedt het helder wettelijk Europees kader dat de burger, organisaties en ons als toezichthouder houvast biedt. In de AVG zijn rechtmatigheid, behoorlijkheid, transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid als kernbeginselen opgenomen en nader uitgewerkt. Ook is als beginsel vastgelegd dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van alle beginselen uit de AVG, en dat ook kan aantonen aan de burger en de toezichthouder. Voorbeelden van deze (verantwoordings-)instrumenten zijn het Data Protection Impact Assessment (DPIA) en de Voorafgaande Raadpleging (VR). De AVG stelt extra eisen aan de situatie wanneer er sprake is van uitsluitend geautomatiseerde besluitvorming, dat wil zeggen zonder menselijke tussenkomst.

Ook moet een organisatie die algoritmes gebruikt voorafin 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 gebruik van zo minimaal mogelijk persoonsgegevens en het nemen van gepaste waarborgen en maatregelen; *data protection by design*. Concreet betekent dat vooraf goed nadenken over het ontwerp van het systeem: waarom gebruik ik een algoritme? Is het gekozen algoritme passend bij het doel waarvoor het wordt ingezet? Is het gebruik van dit algoritme noodzakelijk? Op welke data is dit algoritme gebaseerd? Wanneer risico's onvoldoende kunnen worden weggenomen is het verplicht een voorafgaande raadpleging te laten doen door de AP.

1.3.2 Samenwerking met andere toezichthouders

Algoritmische systemen worden toegepast in steeds meer sectoren en voor steeds meer toepassingen. Dit creëert per definitie risico's voor gegevensbescherming, maar ook voor meer sectorspecifieke vraagstukken zoals cybersecurity, consumentenrecht, mededingingsrecht en antidiscriminatie. Toezicht op algoritmes is dan ook bij uitstek een onderwerp waar de AP veel samenwerkt met andere toezichthouders. Toezicht op AI en algoritmes staat of valt bij de coördinatie vanuit de verschillende expertises (zie ook hoofdstuk 2.3).

2. De AP als toezichthouder

Het werkgebied van de Autoriteit Persoonsgegevens is ongekend groot en heeft ook een internationale dimensie. De basis van de bescherming van persoonsgegevens is het Handvest van de grondrechten van de Europese Unie. De bescherming van persoonsgegevens is dus een grondrecht, zoals ook bijvoorbeeld het recht op vrijheid en veiligheid. Uit het grondrecht volgt de andere wetgeving. Alle organisaties die in Nederland persoonsgegevens verwerken moeten voldoen aan de eisen die de AVG, UAVG, Wpg[1], Wjsg[2], en BRP[3] stellen.

De AP houdt toezicht op:

- 1,8 miljoen bedrijven in Nederland, waarvan 1,3 miljoen met één werkzaam persoon en 500.000 met meer dan één werkzaam persoon;
- Circa 500 overheidsinstellingen – zowel centraal als decentraal –, zoals ministeries, gemeenten, politie en justitie, uitvoeringsorganisaties en andere toezichthouders;
- 7000 scholen primair onderwijs, 1400 scholen voortgezet onderwijs, 65 ROC's, 30 hogescholen en 20 universiteiten;
- en 50.000 zorginstellingen, waaronder fysiocentra, huisartsenpraktijken en ziekenhuizen.

Verder houdt de AP toezicht op '**grenzen en veiligheid**', op basis van de Richtlijn gegevensbescherming politie & justitie. Het gaat hierbij om grote (EU) systemen, zoals het Schengen-informatiesysteem en het Visum Informatie Systeem, die gebruikt worden door politie, OM, douane, Europol etc. Het betreft hier veel gevoelige gegevens, waarbij fouten grote consequenties hebben voor individuen en de samenleving. Het gaat om gegevens van:

- Miljoenen reizigers naar de EU (Entry Exit, VIS, ETIAS), denk aan:
  - vakantiegangers;
  - zakenreizigers;
  - schatting: >700 miljoen reizigers naar EU voorafgaand aan corona
- Verdachten;
- Veroordeelde personen;
- Gezochte of vermiste personen, waaronder minderjarigen;
- Asielzoekers;
- Staatlozen.

2.1 Bevoegdheden

De AP heeft een breed scala aan bevoegdheden om toe te zien op de bescherming van persoonsgegevens. Enkele van deze bevoegdheden zijn:

- Het geven van voorlichting;
- Het geven van gevraagde en ongevraagde adviezen, waaronder het adviseren over (nieuwe) wet- en regelgeving waarin verwerking van persoonsgegevens aan de orde komt;
- Het beoordelen van een gedragscode;
- De verwerkingsverantwoordelijke of de verwerker te gelasten alle benodigde informatie te verstrekken of toegang te verkrijgen tot alle benodigde persoonsgegevens en informatie;
- Het doen van onderzoek;

[1] Wet politiegegevens
[2] Wet justitiële en strafvorderlijke gegevens
[3] Basisregistratie Personen

- Het opleggen van een verwerkingsverbod;
- Handhavend optreden, zoals het opleggen van een last onder dwangsom of een boete.

Door dit uitgebreide arsenaal aan bevoegdheden is de AP voldoende toegerust om passend te kunnen optreden als het gaat om de toepassing van digitale technologieën door de overheid, bedrijven en burgers. De bevoegdheden van de AP zijn daarmee toereikend.

2.2 Europees toezicht

Het toezicht van de AP is bij uitstek internationaal van aard. De samenwerking met andere Europese toezichthouders is uniek. Gezien de relatief korte termijn sinds de inwerkingtreding van de AVG, zijn er al grote stappen gemaakt. Te denken valt aan de recente boetes voor Amazon en WhatsApp, maar ook de gezamenlijke statements over de zeer impactvolle EU-verordeningen DSA, DMA, DGA en AIR.

Europese samenwerking is een must, zowel vanuit juridisch oogpunt als vanuit praktisch oogpunt. Grote techbedrijven en andere grote bedrijven opereren nu eenmaal internationaal, en verwerken persoonsgegevens van nagenoeg alle Europese burgers. Juridisch gezien schrijft de AVG een verdeelsysteem voor grote zaken voor: het is een-loketmechanisme. Daar waar het hoofdkwartier van het betrokken bedrijf zit, daar zit de bevoegdheid om tegen dit bedrijf op te treden. Om in dat krachtenveld effectief te kunnen zijn, moeten de Europese toezichthouders kun krachten dus bundelen. De European Data Protection Board (EDPB) is het forum waarbinnen deze samenwerking plaatsvindt. De AP is vicevoorzitter van de EDPB en is bovendien een actieve speler in Europees verband.

Nederland is bovengemiddeld gedigitaliseerd en huisvest daarmee veel grote internationale bedrijven en hoofdkantoren. Daarmee is de AP relatief vaak aanzet om onderzoek te doen naar gegevensverwerking door internationale spelers als Uber, Netflix of Booking. De AP werkt in onderzoeken actief samen met haar Europese collega's, omdat zij zich volgens de AVG ook mogen uitspreken over de besluiten die de AP neemt. Andersom werkt dit natuurlijk ook zo. De AP kijkt mee met de onderzoeken van haar Europese collega's die gaan over bedrijven die niet in Nederland gevestigd zijn. Zo kan de AP invloed uitoefenen op de manier waarop er door onze Europese collega's opgetreden wordt.

Een belangrijk onderdeel is ook het zorgen voor een gelijk speelveld binnen Europa. Dit doet de EDPB door handreikingen te schrijven over de uitleg van de AVG en de Richtlijn politie & justitie, in gesprek te gaan met belangrijke stakeholders en waar nodig de Europese politiek in beweging te krijgen. De AP investeert in haar rol in Europa, omdat dit haar slagkracht en effectiviteit vergroot.

2.3 Samenwerking met andere toezichthouders

Zoals vermeld, raakt digitalisering alle takken van onze samenleving. Van de financiële sector, tot de zorg, het onderwijs, de energiesector, horeca, veiligheid etc. Dat vraagt dus ook een gecoördineerde toezichtsaanpak, vanuit de verschillende expertise en met respect voor de verschillende bevoegdheden. Samenwerking met anderen is onontbeerlijk, ook met oog op efficiency voor ondertoezichtsstaanden. De samenwerking neemt daarom steeds verder toe. Zo werkt de AP intensief samen met verschillende toezichthouders. Met de Inspectie Gezondheidszorg en Jeugd (IGJ) en de Nederlandse Zorgautoriteit (NZA) werken we samen op zorgvraagstukken, met de Autoriteit Financiële Markten (AFM) als het gaat om vragen over digitalisering in het bankwezen en met het Agentschap Telecom (AT) kijken we naar de gezamenlijke aanpak van algoritmes. Met onder andere de Autoriteit Consument en Markt (ACM) wordt momenteel gekeken naar intensivering van samenwerking op het onderwerp digitale economie.

3. Noodzakelijke groei van de AP voor het bedrijfsleven en burgers

Digitalisering en het gebruik van persoonsgegevens gaan niet meer weg. Integendeel, deze ontwikkelingen zullen alleen maar sterker en omvangrijker worden. Dat merken wij als AP iedere dag opnieuw. Het aantal incidenten neemt daarbij ook toe. Van de explosieve toename van datahandel en datadiefstal, zoals onlangs bij de GGD, tot het gebruik van persoonsgegevens door de NCTV. Met het aantal misstanden neemt ook bewustzijn van burgers toe – wij ontvangen meer dan 20.000 klachten per jaar. Tegelijkertijd krijgen wij veel vragen van bedrijven en organisaties over hoe zij hun datahuishouding het beste kunnen vormgeven.

Deze impactvolle ontwikkelingen vragen om een toezichthouder die daar voldoende op toegerust is. Door het achterblijven van budget komt dit niet genoeg van de grond. De AP voldoet nu niet aan haar wettelijke taken als toezichthouder en komt niet toe aan de uitvoering van haar strategische prioriteiten. Dit geldt overigens ook voor de andere Europese privacy toezichthouders; allen kampen met zeer krappe budgetten.

3.1 Stappen voorwaarts naar een toekomstbestendige toezichthouder

In een vrije, democratische samenleving moeten mensen erop kunnen vertrouwen dat organisaties zorgvuldig omgaan met hun gegevens, nu en in de toekomst. De groei van de AP is noodzakelijk voor burgers en het bedrijfsleven in onze snel digitaliserende samenleving. Alleen dan kan Nederland verantwoord economisch blijven groeien en verder digitaliseren. En kan Nederland de voortrekkersrol vervullen die bij ons past – als een van de meest gedigitaliseerde én innovatieve landen ter wereld.
Het budget van de AP moet daarvoor groeien van het huidige 25 miljoen naar een structurele financiering van 100 miljoen euro, vergelijkbaar met andere Nederlandse toezichthouders.

De vraag om groei is in lijn met een drietal moties aangenomen door de Tweede Kamer. De motie Klaver/Ploumen benadrukt een sterke AP in het kader van tegenmacht en het beschermen van de burgers tegen discriminerende algoritmes. De motie Hijink pleit voor een verhoging van het budget van de AP, om onder meer de steeds verder groeiende aantal datalekken en problematiek aan te pakken. De motie Beukering-Huijbregts verzoekt het kabinet te onderzoeken hoe de capaciteit en middelen van de AP vanaf 2022 structureel op een afdoende niveau kunnen komen. De AP kan door uitbreiding van het budget tegenmacht bieden en een essentiële bijdrage leveren inzake digitalisering en de bescherming van persoonsgegevens. Hiermee krijgen wij als Nederland de digitale economie en digitale democratie die we willen.