AUTORITEIT
PERSOONSGEGEVENS

Focus AP 2020-2023

Dataprotectie in een digitale samenleving

Inhoud

Voorwoord

Leven in een vrij en democratisch land als Nederland is een groot goed. Velen van ons kunnen iedere dag naar hun werk, volgen onderwijs, spreken af met vrienden en familie, gaan er in het weekend op uit of kijken geregeld een serie.

Veel van het gemak in ons leven komt door technologie en digitalisering. We hebben allemaal een *smart phone* in onze broekzak en steeds meer mensen maken gebruik van een slimme meter, hebben slimme speakers en apparaten met stemherkenning. Ook onze diensten regelen we steeds meer online; van onze bankzaken tot de aangifte van onze belasting tot het vinden van een partner.

Al deze apparaten en diensten verzamelen persoonlijke gegevens waardoor ze steeds meer van ons weten. Niets voor niets wordt inmiddels gezegd dat zoekmachines en sociale media op basis van onze zoekgegevens en berichten ons beter kennen dan onze naasten. Uit de grote hoeveelheid data kun je immers afleiden wat onze seksuele voorkeur is, op welke partij we stemmen, hoe vaak we onze huisarts of specialist hebben bezocht en waar we ons geld aan uitgeven. Anders gezegd, er wordt steeds meer over ons vastgelegd, ons leven wordt steeds beter gedocumenteerd zonder dat we precies weten wat er met die gegevens gebeurt en wie er toegang toe heeft. Dit maakt ons en onze democratische rechtstaat kwetsbaar.

In deze digitale samenleving is de bescherming van persoonsgegevens (dataprotectie) essentieel. Daarom is het recht op gegevensbescherming opgenomen in het Handvest van de grondrechten van de Europese Unie. Het is een belangrijk grondrecht dat er is om ons tegen misbruik te beschermen. Het gaat in de kern over zeggenschap, over autonomie, over dat wij als burgers zelf gaan over wat we met wie delen. Kortom, het fundamentele recht op bescherming van privacy moet voorkomen dat de fundamenten van onze rechtsorde, vrije wil en onze autonomie eroderen.

De Autoriteit Persoonsgegevens (AP) heeft hierin een belangrijke taak. De AP is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt. Wij zijn onderdeel van een Europees samenwerkingsverband van toezichthouders. Ons toezichtveld is omvangrijk: 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 daarom bij uitstek grensoverschrijdend. Samen met onze Europese collega-toezichthouders geven we voorlichting, doen we onderzoek en delen we boetes uit aan bedrijven en organisaties die zich niet aan de wet houden.

In het document *Focus AP 2020-2023* leest u welke ontwikkelingen en risico's wij zien en waar wij de komende periode onze aandacht aan besteden om de bescherming van persoonsgegevens te borgen. Van *smart cities* tot *internet of things*, van het toezicht op algoritmes tot de aanpak van illegale datahandel. Impactvolle onderwerpen waar bedrijven en organisaties dagelijks mee bezig zijn en thema's die burgers dagelijks beïnvloeden.

We kiezen in ons werk voor een balans tussen bevorderen en bewaken, zoals ook in onze missie naar voren komt. Dat betekent dat we inzicht hebben in de manieren waarop bedrijven en organisaties persoonsgegevens verwerken, we hen aanspreken op hun verantwoordelijkheid en we ingrijpen als het mis gaat. Ons werk gebeurt enerzijds reactief – wij krijgen bijvoorbeeld veel klachten van burgers, behandelen voorafgaande raadplegingen, geven wetgevingsadviezen en ondersteunen functionarissen gegevensbescherming – en anderzijds proactief.

Tegelijkertijd willen we innovatie de ruimte geven, om gemak en welvaart te stimuleren. Innovatie moet en kan hand in hand gaan met de bescherming van persoonsgegevens. Bij nieuwe technologieën bevordert de AP daarom *privacy by design* en *privacy by default.*

De komende vier jaar gaan we als AP hard aan de slag met *dataprotectie in een digitale samenleving.*
Gezien de snelle ontwikkelingen in ons toezichtveld, houden wij daarnaast voldoende ruimte om op die ontwikkelingen in te spelen.

Katja Mur, Monique Verdier en Aleid Wolfsen
Bestuur Autoriteit Persoonsgegevens

Managementsamenvatting

De bescherming van je persoonsgegevens is een grondrecht van iedere Nederlander. De Autoriteit Persoonsgegevens (AP) is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt. Wij zijn onderdeel van een Europees samenwerkingsverband van toezichthouders. Ons toezichtveld is omvangrijk: internationale en nationale bedrijven en organisaties, de gehele overheid, inclusief politie en justitie en ook verenigingen, scholen, stichtingen en individuele burgers.

Met *Focus AP 2020-2023* delen wij met u wat u de komende jaren in ieder geval van de AP kunt verwachten.

De wereld om ons heen

De AP werkt in een wereld die volop in verandering is. Van alle ontwikkelingen heeft vooral digitalisering een grote impact op onze toezichtstaak. Wij onderscheiden 3 trends die voor het werk van de AP van belang zijn. Deze trends staan niet los van elkaar, maar hangen op een logische manier met elkaar samen.

1. Doorgroei van de datasamenleving

De samenleving is de afgelopen jaren wezenlijk veranderd door digitalisering en technologische innovatie. Er is sprake van een datagedreven wereld, waarin doorlopend gegevens worden vastgelegd over bijvoorbeeld betaaltransacties, gezondheid, mobiliteit en ook gedrag van mensen. Er zijn hierdoor niet alleen veel meer data dan ooit tevoren beschikbaar, de data zijn ook diverser, veel specifieker, persoonlijker en diepgaander. Dit komt tot uiting in een aantal gebieden: data als businessmodel, het rechtsbestel, marktconcentraties en internationalisering.

2. Toename van digitaal onrecht

In deze digitale samenleving is de bescherming van persoonsgegevens essentieel. Privacy en de bescherming van persoonsgegevens zijn een grondrecht en een voorwaarde om vrij te zijn in wie je bent en wat je doet en jezelf verder te ontwikkelen. Privacy gaat erover dat burgers regie houden over hun gegevens: weten welke organisatie welke gegevens verzamelt, wat daarmee gebeurt, hoe lang ze worden bewaard en of ze goed beveiligd zijn. Maar ook dat mensen onbespied over straat kunnen of op internet kunnen surfen. En dat bedrijven, organisaties en overheden hen niet oneerlijk behandelen door profilering op basis van hun persoonsgegevens. Met andere woorden: bescherming van persoonsgegevens is een voorwaarde voor het functioneren van onze democratische rechtsorde.

Omdat de digitalisering verder zal toenemen en de dataeconomie als geheel sterk zal groeien, verwachten wij een toename van digitaal onrecht. Voorbeelden hiervan zijn illegale datahandel, gebrekkige beveiliging, discriminatie en ondermijning van de democratische rechtsorde. De overheid heeft hierin een bijzondere positie omdat zij over veel gevoelige persoonsgegevens beschikt en deze vaak koppelt, waardoor mensen in de knel kunnen komen.

3. Toename van privacybewustzijn

Mede door de komst van de AVG en de Richtlijn politie & justitie ziet de AP dat bedrijven, organisaties en burgers zich langzaamaan meer bewust worden van de privacyrisico's en grip willen krijgen op hun persoonsgegevens. Het is van groot belang dat organisaties hun verantwoordelijkheid nemen. We zien dat zowel bedrijven als overheden de omgang met privacy en de beveiliging van persoonsgegevens opnemen in hun reguliere werkzaamheden. Het toepassen van *privacy by design* en *privacy by default* is noodzakelijk in

een datasamenleving waarin continu nieuwe producten en diensten worden ontwikkeld. Dit betekent bijvoorbeeld dat bij het ontwerpen van systemen wordt geborgd dat zo min mogelijk persoonsgegevens worden verzameld (dataminimalisatie).

Ook burgers worden zich langzaamaan steeds meer bewust van hun privacy. Maar het blijft voor individuele consumenten lastig te overzien wat de gevolgen zijn van keuzes, zoals toestemming geven voor het gebruik van hun persoonsgegevens.

Onze focusgebieden

De risico's van de digitaliserende samenleving voor de bescherming van persoonsgegevens zijn groot, divers en complex. Het is noodzakelijk om te kiezen. Om als toezichthouder onze missie en ambities waar te maken, kiezen wij voor drie focusgebieden. De focusgebieden krijgen de komende jaren extra nadruk in ons toezicht. Daarnaast hebben wij veel reguliere werkzaamheden, zoals het behandelen van klachten van burgers, het verwerken van datalekmeldingen, het ondersteunen van functionarissen gegevensbescherming en het geven van wetgevingsadviezen. Ook daar brengen wij prioritering in aan. Binnen de focusgebieden spitsen wij ons toe op een aantal aandachtsgebieden.

1. Datahandel

Data maken producten en diensten steeds slimmer en deze producten en diensten creëren vervolgens weer meer data. Dit heeft voordelen; de data kunnen worden gebruikt om bijvoorbeeld gericht producten en diensten aan te bieden. Maar ook nadelen: er vindt steeds meer ongeoorloofde doorverkoop van persoonsgegevens aan derden plaats, die vervolgens kunnen worden gebruikt om ons te beïnvloeden en te sturen. Dit vindt zowel nationaal als internationaal plaats.

Aandachtsgebieden: toezicht op doorverkoop data, *internet of things,* profilering, *behaviorial advertising*.

2. Digitale overheid

Centrale en lokale overheden, uitvoeringsorganisaties en politie en justitie beschikken over een grote hoeveelheid – vaak gevoelige en bijzondere – persoonsgegevens. De overheid werkt gericht aan het inzetten van persoonsgegevens. Dit is ook nodig; de overheid kan niet achterblijven in digitalisering. Het is noodzakelijk om maatschappelijke en economische kansen te creëren. Maar er zijn ook risico's.
De AP vindt het belangrijk dat de overheid verantwoordelijk omgaat met persoonsgegevens.

Aandachtsgebieden: databeveiliging, *smart cities*, samenwerkingsverbanden, verkiezingen en *microtargeting.*

3. Artificiële Intelligentie & algoritmes

Steeds meer bedrijven en organisaties maken gebruik van algoritmes en AI. Dit biedt voordelen en leidt tot nieuwe nuttige toepassingen. Maar de inzet van AI en algoritmes kent ook risico´s en schadelijke effecten. Als AP zijn wij verantwoordelijk voor het toezicht op persoonsgegevens en daarmee ook op de toepassing van AI en algoritmes waarbij persoonsgegevens worden gebruikt. De AVG biedt ook een belangrijke wettelijke basis voor het toezicht op AI en algoritmes. Hierdoor kan de AP ook op dit gebied haar toezicht uitoefenen.

Aandachtsgebied: stelsel van toezicht.

Hoe gaan we dit doen?

Om de juiste problemen aan te kunnen pakken houdt de AP risicogestuurd toezicht. Dat betekent dat de AP op een methodische en weloverwogen wijze aan oordeelsvorming en besluitvorming doet in haar toezichtactiviteiten. Daarbij is het uitgangspunt dat de AP gespitst is op onderwerpen met een groot risico voor burgers. Daarbij wegen we onder andere af om hoeveel data het gaat en hoe gevoelig die data zijn.

Goed toezicht vergt dat wij de juiste balans hanteren tussen bevorderen en bewaken. Of anders gezegd: tussen het stimuleren van 'goed' gedrag en handhavend optreden waar nodig. Zo bevorderen wij – bijvoorbeeld met voorlichtingscampagnes - dat organisaties hun verantwoordelijkheid nemen om rechtmatig persoonsgegevens te verwerken en deze gegevens te beschermen. Innovatie en privacy gaan daarbij wat ons betreft hand in hand. Ook stimuleren wij op verschillende manieren dat ook mensen zelf hun verantwoordelijkheid nemen. Daarnaast bewaken wij de naleving van privacyregels door onafhankelijk onderzoek te doen naar (mogelijke) overtredingen door de overheid en het bedrijfsleven. Dit geldt voor nationale partijen, maar juist ook voor internationale bedrijven en organisaties. Als het nodig is, treden wij handhavend op.

Onze eigen organisatie

De AP houdt toezicht op het gedrag en handelen van heel veel bedrijven en organisaties. Deze taak en verantwoordelijkheid vragen ook onberispelijk en onbesproken gedrag van onszelf. We passen daarom in de hele organisatie de *good governance*-principes toe in onze manier van werken.

Wij zien onze kernwaarden – open, onafhankelijk, deskundig en effectief – als kompas in ons handelen en spreken elkaar daar ook actief op aan.

Focus Autoriteit Persoonsgegevens 2020-2023

Dataprotectie in een digitale samenleving

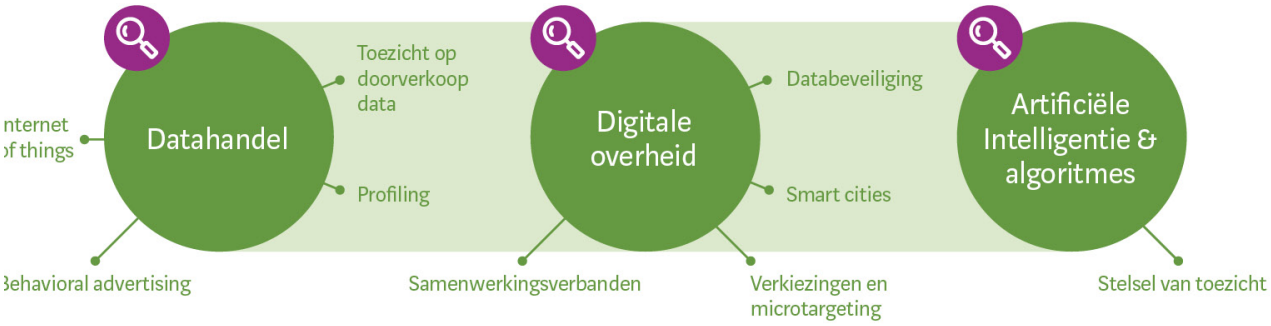
De Autoriteit Persoonsgegevens (AP) is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt.

Welke ontwikkelingen zien wij?

- Doorgroei van de data-samenleving
- Toename van digitaal onrecht
- Toename van privacy-bewustzijn

Wat worden onze focusgebieden?

Wij kiezen voor drie focusgebieden. Thema's die direct raken aan de missie van de AP en passen binnen de beschreven trends. En thema's die een zekere breedheid kennen, die in meerdere sectoren spelen en waar de AP het verschil kan maken door grenzen te markeren ten aanzien van wat wel of niet kan onder de AVG. De focusgebieden krijgen de komende jaren extra nadruk in ons toezicht, waarbij wij andere ontwikkelingen en onze wettelijke taak niet uit het oog verliezen.



Datahandel
Data maken producten en diensten steeds slimmer en deze producten en diensten creëren vervolgens weer meer data. Dit heeft voordelen maar ook nadelen: er vindt steeds meer ongeoorloofde doorverkoop van persoonsgegevens aan derden plaats.

Digitale overheid
Centrale en lokale overheden, uitvoeringsorganisaties en politie en justitie beschikken over een grote hoeveelheid – vaak gevoelige en bijzondere – persoonsgegevens. De overheid werkt gericht aan het inzetten van persoonsgegevens. Het is van belang dat de overheid verantwoordelijk omgaat met persoonsgegevens.

AI & algoritmes
Steeds meer bedrijven en organisaties maken gebruik van algoritmes en AI. Dit biedt voordelen en leidt tot nieuwe nuttige toepassingen. Maar de inzet van AI en algoritmes kent ook risico's en schadelijke effecten.

Hoe gaan wij dit doen?

Om de juiste problemen aan te kunnen pakken houdt de AP risicogestuurd toezicht. Dat betekent dat de AP op methodische en weloverwogen wijze aan oordeelsvorming en besluitvorming doet in haar toezichtactiviteiten. De AP is gespitst op onderwerpen met een groot risico voor burgers. Daarbij wegen we onder andere af om hoeveel data het gaat en hoe gevoelig die data zijn. Op basis daarvan gebruiken we een of meerdere toezichtsinstrumenten, zoals normuitleg, wetgevingsadvies, voorlichting of handhaving. Dit doen we in samenwerking met onze Europese collega's.

1. Inleiding

Als toezichthouder krijgen wij vaak de vraag waaraan wij aandacht gaan besteden en hoe wij ons toezicht vormgeven. Met *Focus AP 2020-2023* willen wij delen wat u de komende jaren in ieder geval van de Autoriteit Persoonsgegevens (AP) kunt verwachten.

1.1 Missie Autoriteit Persoonsgegevens

De missie van de AP stelt: de Autoriteit Persoonsgegevens is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt.

Door de digitalisering van onze samenleving is deze missie uitdagender dan ooit. Immers, in een datagedreven en open samenleving zoals Nederland worden overal persoonsgegevens (data) verzameld en vastgelegd en verder verwerkt. Ons land behoort bovendien tot een van de meest gedigitaliseerde landen van Europa. We hebben een open economie en een (internationaal) bedrijfsleven dat volop digitale technologie gebruikt. Bovendien is bijna ieder huishouden verbonden met internet. De maatschappelijke opgave om burgers en hun persoonsgegevens in een digitale samenleving te beschermen, is hierdoor omvangrijk en complex.[1]

[1] *Index van de digitale economie en maatschappij (DESI). Landverslag 2019. Nederland.* Europese Commissie.

1.2 Focus AP 2020-2023

Met *Focus AP 2020-2023* bouwen wij voort op ons *Toezichtkader 2018-2019*. Wij bieden hiermee inzicht in hoe wij invulling geven aan onze missie en ambities en beschrijven de onderwerpen die de komende vier jaar dringend aandacht nodig hebben. Het document is bedoeld als startpunt van (sectorale) toezichtactiviteiten voor de komende periode.

Bij de totstandkoming van *Focus AP 2020-2023* hebben wij met een groot aantal partijen gesproken, zoals stakeholders, FG's en andere toezichthouders. Daarnaast hebben wij geput uit de kennis en ervaring van onze medewerkers en hebben we gekeken naar onderwerpen die in internationaal verband aan de orde zijn.

Focus AP 2020-2023 bestaat uit de volgende onderdelen:

- Hoofdstuk 2: De wereld om ons heen. Welke ontwikkelingen zien wij bij digitalisering, data en persoonsgegevens?
- Hoofdstuk 3: Focusgebieden. Welke focusgebieden hebben wij gekozen? Dit zijn thema's waarbij wij risico's zien en waarmee wij aan de slag gaan in de komende vier jaar.
- Hoofdstuk 4: Strategie. Hoe hebben wij ons toezicht ingericht en hoe pakken wij problemen aan?
- Hoofdstuk 5: Interne organisatie. Hoe ziet onze organisatie eruit?

2. De wereld om ons heen

De Autoriteit Persoonsgegevens (AP) werkt in een wereld die volop in verandering is. Van alle ontwikkelingen heeft vooral digitalisering een grote impact op onze toezichtstaak. Als wij effectief willen optreden als toezichthouder, is het van belang om meer inzicht te krijgen in de precieze uitwerking en ontwikkeling van digitalisering.

In dit hoofdstuk onderscheiden wij drie trends die voor het werk van de AP van belang zijn:

1. Doorgroei van de datasamenleving;
2. Toename van digitaal onrecht;
3. Toename van privacy bewustzijn.

Deze drie trends zijn niet los van elkaar te zien. Zo is de opkomst van digitaal onrecht een direct gevolg van de digitalisering van de samenleving. En de toename van digitaal onrecht voedt het privacybewustzijn in de samenleving.

Bij elke trend schetsen wij de onderliggende ontwikkelingen. De analyse hiervan legt de basis voor de focusgebieden van de AP in 2020-2023, zoals beschreven in hoofdstuk 3.

2.1 Trend: doorgroei van de datasamenleving

De samenleving is de afgelopen jaren wezenlijk veranderd door digitalisering en technologische innovatie. Er is sprake van een datagedreven wereld, waarin doorlopend gegevens worden vastgelegd over

bijvoorbeeld betaaltransacties, gezondheid, mobiliteit en ook gedrag van mensen. Er zijn hierdoor niet alleen veel meer data dan ooit tevoren beschikbaar, de data zijn ook diverser, veel specifieker, persoonlijker en diepgaander.

Bedrijven zijn ook bereid veel geld te betalen voor persoonsgegevens die nieuwe kansen bieden, marktvraag en -aanbod dichter bij elkaar brengen en toepassingen opleveren die voorheen ondenkbaar waren. Deze toepassingen bieden vaak voordelen en gemak voor bedrijven, organisaties en burgers. Ook burgers beschikken over steeds meer mogelijkheden waarmee zij de persoonsgegevens van andere personen kunnen verwerken, waaronder verder verspreiden.

In deze dataeconomie is het logisch om zo veel mogelijk persoonsgegevens en digitale 'sporen' te verwerken, zodat de digitale producten en diensten nog slimmer, persoonlijker en efficiënter worden. De EU ziet het stimuleren van de digitale dataeconomie als prioriteit.

Op vier deelontwikkelingen gaan we hieronder verder in.

Data als businessmodel

(Internationale) bedrijven ontwikkelen steeds meer manieren om data binnen te halen, te beheren, te analyseren en te gebruiken. Voor veel bedrijven is het op grote schaal verzamelen, gebruiken (voor bijvoorbeeld gepersonaliseerde advertenties) en verkopen van persoonsgegevens inmiddels een belangrijk – en soms zelfs een primair – onderdeel van hun verdienmodel. Zij verdienen hun geld dus met het gebruik van datasets en (zeer) grote hoeveelheden persoonsgegevens.

Dit kan voor burgers voordelen en gemak bieden. Zo mag een winkel klantgegevens gebruiken om consumenten gericht van dienst te zijn, mits zij daarvoor toestemming hebben gegeven. Data-analyse kan ook innovatieve oplossingen bieden die onze samenleving positief beïnvloeden. Denk aan kostenefficiënte gezondheidszorg, waardoor bijvoorbeeld een consult met een arts ook via een videoverbinding kan, of aan apps die de beweging of bloeddruk van mensen meten (*eHealth*). Maar ook gemeenten die met mobiliteitsgegevens groeiende verkeerstromen reguleren, wat in drukke steden een uitkomst kan zijn (*smart cities*). Deze dataeconomie zal zich naar verwachting verder ontwikkelen door gebruik van artificiële intelligentie en ontwikkelingen in de biotechnologie.[2]

De dataeconomie brengt ook risico's met zich mee. Bedrijven verzamelen gegevens over burgers en consumenten (het 'oogsten' van informatie) en gebruiken deze voor marketingdoeleinden, ze verkopen de data door (het 'vermarkten' van informatie) of verwerken de gegevens tot profielen en verkopen deze door, en zetten deze gegevens in om geautomatiseerd besluiten te nemen. Dit is zorgwekkend wanneer bedrijven de gegevens doorverkopen zonder dat mensen dat weten en zonder dat zij daarvoor toestemming hebben gegeven. Zo kunnen bedrijven bijvoorbeeld ten onrechte beschikken over de medische gegevens, DNA-gegevens of betaalgegevens van mensen. Deze data kunnen bedrijven, zeker als ze die combineren, gebruiken om gericht gedrag te beïnvloeden. Ook kunnen de gegevens onbedoeld 'wegstromen' (datalekken), bijvoorbeeld door gebrekkige beveiliging.

Deze ontwikkelingen zorgen ervoor dat het bijna onmogelijk wordt om je als individu aan digitalisering en dataficatie te onttrekken. Dit noemen we ook wel systeemdwang. Persoonsgegevens worden overal vastgelegd en fysieke en digitale bewegingen van mensen worden zowel in het openbaar als in de privésfeer vastgelegd, ook als zij dat niet willen.

[2] Silke den Hartog- de Wilde, *Vooruitkijken naar 2050. Trends die de toekomst van de Nederlandse economie beïnvloeden.* Den Haag: Stichting Toekomstbeeld der Techniek, 2018.

Het rechtsbestel in een datasamenleving

De rechtsstaat ontwikkelt mee als een reactie op de digitalisering van de samenleving en het ontstaan van een dataeconomie. Om de ontwikkeling van de digitale datasamenleving in goede banen te leiden, zijn onder meer de Algemene verordening gegevensbescherming (AVG) en de Richtlijn politie & justitie geïntroduceerd.[3] Deze wetten waarborgen het grondwettelijk recht op privacy en zorgen voor spelregels op de markt van persoonsgegevens. Uitgangspunt is de bescherming van persoonsgegevens, waardoor in de nieuwe Europese, digitale economie gegevens vrijelijk moeten kunnen stromen. In deze context is een nieuw Europees orgaan van privacytoezichthouders opgericht, waarvan de AP deel uitmaakt: de European Data Protection Board (EDPB).

De AVG heeft als doel om het grondrecht op privacy en rechtszekerheid in de hele EU te stimuleren in de digitale datamarkt,[4] schenders van privacy aan te pakken en een hoog niveau van dataprotectie te borgen.[5]

Er is bij het opstellen van de AVG bewust voor gekozen om niet louter 'van bovenaf' gedetailleerde regels op te leggen. De AVG is *principle-based*, biedt de ruimte om mee te groeien met de stand van de techniek en verlangt dat bedrijven en organisaties het beschermen van privacy zelf vormgeven. Dit doen zij met instrumenten als een verwerkingsregister, *privacy by design*, *self-assesments* (*data protection impact assessments*) en intern toezicht (functionaris gegevensbescherming). Bedrijven en organisaties moeten dus zelf aan de slag om met eigen kennis en kunde het beste resultaat te bereiken en dat te verantwoorden.

Marktconcentraties

Een kenmerk van de groeiende dataeconomie is het ontstaan van marktconcentraties. De beschikbare hoeveelheid te verhandelen data stijgt exponentieel door het toenemend gebruik van digitale diensten, de komst van het *internet of things* (IoT) en de alomtegenwoordigheid van dataverzamelende sensoren. Apparaten – van koelkast tot schoen tot bril – maar bijvoorbeeld ook stoffen zijn 'datadragers' geworden. Met zo veel mogelijk data en met gebruik van artificiële intelligentie worden innovatieve toepassingen ontwikkeld.

Grote hoeveelheden data komen in toenemende mate terecht bij een selecte groep van machtige spelers. Grote (tech)bedrijven kopen succesvolle *start-ups* op en blijven hierdoor de markt domineren. Door netwerkeffecten vindt concentratie plaats van diensten, technologie, kennis en data. Grote bedrijven en organisaties groeien verder door, en krijgen macht ten nadele van nieuwe spelers. De individuele keuzevrijheid van consumenten en burgers kan hierdoor onder druk komen te staan. Ook bestaat het risico op ongeoorloofde marktconcentratie en mogelijk misbruik van die machtposities. Dit kan steeds vaker leiden tot een samenloop van vragen over privacy en mededinging.

Internationalisering

De digitale dataeconomie onttrekt zich meer dan de conventionele diensteneconomie aan landsgrenzen. Dit kan het privacytoezicht bemoeilijken. Immers, data kunnen makkelijk over grenzen worden verplaatst en de digitale wereld kent geen fysieke landsgrenzen. Bij gegevensverwerkingen in verschillende Europese landen werken de Europese toezichthouders met elkaar samen. Dit wordt het samenwerkings- en coherentiemechanisme genoemd. De AP hecht veel waarde aan een effectieve samenwerking tussen de Europese toezichthouders. Niet alleen omdat burgers hierbij gebaat zijn – gegevensbescherming moet immers niet bij de Nederlandse grens ophouden – maar ook omdat gezamenlijke Europese normuitleg de meeste duidelijkheid biedt aan bedrijven en organisaties die actief zijn in verschillende landen.

[3] Voor de AVG gold de Wet bescherming persoonsgegevens.

[4] Bijvoorbeeld door een minimumstandaard van beveiligingsniveau bij bijzondere data te eisen en aan te sluiten op NEN- en ISO-normering.

[5] Zie ook het *Framework for the free flow of non personal data in the European Union* van de Europese Commissie (mei 2019).

Het is voor de AP én de Nederlandse economie bovendien van groot belang om juist de komende periode – waarin we de eerste resultaten van grote internationale onderzoeken verwachten – een actieve bijdrage te kunnen leveren aan de interpretatie, toepassing en handhaving van de nieuwe AVG-normen.

Een aandachtspunt is dat persoonsgegevens van Nederlandse burgers ook buiten de EU kunnen worden verwerkt en dat burgers zich daarvan vaak niet bewust zijn. Dit is een risico wanneer het gaat om landen die geen, of een minder hoog, beschermingsniveau van persoonsgegevens bieden ('dataparadijzen'). Ook in deze gevallen kan de AVG echter van toepassing zijn. Het verschil met landen buiten de EU zonder een hoog dataprotectieniveau kan steeds groter worden. Dit kan bijvoorbeeld tot gevolg hebben dat nieuwe IoT- producten afkomstig uit dergelijke landen – zoals een knuffelbeer met camera's en sensoren – niet zonder meer op de Europese markt verkrijgbaar zouden mogen zijn.

Handhaving van dit soort gevallen blijft echter een complex proces. Hoewel de samenwerking tussen de EU-toezichthouders met de komst van de AVG goed is georganiseerd, verwachten wij dat (dataprotectie)-wetgeving nog verder zal (moeten) internationaliseren om de rechten van Nederlandse burgers ook bij verwerkingen buiten de EU goed te kunnen beschermen.

2.2 Trend: toename van digitaal onrecht

In een digitale samenleving is de bescherming van persoonsgegevens essentieel. Privacy en de bescherming van persoonsgegevens zijn een grondrecht. In toenemende mate is het ook verweven met de bescherming van andere grondrechten, zoals het recht op gelijke behandeling en het kiesrecht. Privacy is dus een voorwaarde om vrij te zijn in wie je bent en wat je doet en jezelf verder te ontwikkelen. Privacy gaat erover dat burgers regie houden over hun gegevens: weten welke organisatie welke gegevens verzamelt, wat daarmee gebeurt, hoe lang ze worden bewaard en of ze goed beveiligd zijn. Maar ook dat mensen onbespied over straat kunnen of op internet kunnen surfen. En dat bedrijven en organisaties hen niet oneerlijk behandelen door profilering op basis van hun persoonsgegevens. Met andere woorden: bescherming van persoonsgegevens is een voorwaarde voor het functioneren van onze democratische rechtsorde.

Omdat de digitalisering verder zal toenemen en de dataeconomie als geheel sterk zal groeien, verwachten wij een toename van digitaal onrecht. Voorbeelden hiervan zijn geautomatiseerde besluitvorming waardoor burgers ten onrechte in de knel komen of kunnen worden buitengesloten, illegale datahandel, *hacking* en discriminatie als gevolg van profilering. Door deze praktijken bestaat de kans op ondermijning van de solidariteit en gelijkheid binnen onze rechtsorde (artikel 1 Grondwet). Vooral mensen die digitaal minder vaardig of bewust zijn, zullen in hun grondrechten aangetast worden en slachtoffer worden van de negatieve kanten van digitalisering.

Illegale datahandel

Hoe meer data bij elkaar gebracht worden – en dus kunnen worden gecombineerd – des te hoger de waarde van die data. Het oogsten en doorverkopen van persoonsgegevens kan hierdoor sterk toenemen. Dit leidt tot potentiële gevaren op de (internationale) digitale markt. Zoals persoonsgegevens verkopen zonder toestemming. Ook sluiten wij niet uit dat er misbruik gemaakt kan worden van 'kwaadaardige' apps en websites die grote hoeveelheden data afvangen en stelen om vervolgens door te verkopen (datadiefstal en illegale datahandel).

Gebrekkige beveiliging

In een dataeconomie is het goed beveiligen van allerhande gegevens essentieel. Het uitvallen van kritieke infrastructuren door gebrekkige beveiliging is een erkend gevaar. *Hacking*, het ongeoorloofd binnendringen in een computersysteem, komt ook veelvuldig voor. Daarbij worden vaak persoonsgegevens buitgemaakt,

zoals inloggegevens. Ook menselijke fouten kunnen ertoe leiden dat gegevens uit computersystemen onbedoeld op straat komen te liggen. De datalekken door *hacking* of menselijke fouten kunnen niet alleen leiden tot grote economische schade voor bedrijven of organisaties, maar kunnen ook een ernstige inbreuk vormen op de grondrechten van mensen. Bijvoorbeeld doordat gegevens over gezondheid, politieke activiteiten en seksuele voorkeur op straat komen te liggen.

Naast economische schade zorgt een succesvolle hack ook voor een vorm van digitale onmacht. Burgers van wie gegevens door een hack op straat komen te liggen, kunnen daar immers nauwelijks iets tegen doen (denk aan identiteitsfraude). Als bedrijf of organisatie kun je je dergelijke bedrijfsrisico's niet veroorloven. Het beveiligen van data (*cybersecurity*) is daarom een belangrijk onderwerp op de strategische agenda van bestuurders en organisaties.

Discriminatie

Steeds meer bedrijven en organisaties gebruiken data om profielen te maken van mensen. Dit heet profilering. Vervolgens kunnen zij gericht producten en diensten aanbieden. Het profiel en de bijbehorende score bepalen op welke manier zij mensen behandelen of benaderen.

Profilering kent verschillende risico's. Vervuilde, verouderde of foutieve data kunnen resulteren in onjuiste beslissingen voor betrokkenen. Profilering kan daarnaast tot discriminatie leiden. Beslissingen kunnen vooroordelen bevatten als zelflerende algoritmes getraind worden met datasets die objectief correct zijn, maar inherent vooroordelen bevatten. Maar ook ontwerpkeuzes van makers van algoritmen kunnen (onbedoelde) vooroordelen bevatten. Zo kan bijvoorbeeld een correlatie tussen bepaalde variabelen opgevat worden als een causaal verband, terwijl dat causale verband niet hoeft te bestaan.

Bekend is bijvoorbeeld dat vrouwen en etnische minderheden door verkeerd getrainde algoritmes niet uitgenodigd worden voor een sollicitatiegesprek bij een geautomatiseerde briefselectie. Of überhaupt de vacatures niet te zien krijgen op een website die zich volautomatisch aanpast aan de gebruiker. Door toepassingen van artificiële intelligentie als *predictive policing* kunnen mensen met bepaalde kenmerken, bijvoorbeeld huidskleur, worden ingeschat als individu met een hogere kans op misdadig gedrag (digitaal etnisch profileren).

In een dataeconomie waarin profilering en scoring vanzelfsprekend zijn, ontstaat als vanzelf een indeling van mensen in verschillende groepen. Een bijkomend gevolg van het verregaand scoren en profileren van individuen is een mogelijke ondermijning van solidariteit en sociale zekerheid. Zo bestaat bijvoorbeeld het risico dat bepaalde groepen geen verzekering of woning kunnen krijgen door een lage score. Dit leidt tot tweedeling en polarisatie in de samenleving. Uitgangspunt zou moeten zijn dat iedereen zich kan verweren tegen een lage score, bijvoorbeeld door een beroep op het recht op vergetelheid of een correctierecht. Maar ook dat bedrijven en organisaties transparant zijn over het gebruik en de werking van dit soort technieken. Wij verwachten dat mensen steeds vaker een beroep zullen doen op deze rechten. Dit zien wij ook in de privacyklachten die wij ontvangen.

Ook de mogelijkheid om te betalen met je data kan leiden tot een tweedeling in de samenleving. De verwachting is dat armere mensen eerder bereid zijn hun privacy op te geven en hun persoonsgegevens te gelde te maken, bijvoorbeeld door kortingen te accepteren in ruil voor data.

Ondermijning democratische normen

Een specifieke vorm van digitaal onrecht is het bewust of onbewust manipuleren van mensen in hun democratisch recht om vrij te stemmen. Het zal niemand ontgaan zijn dat schending van privacy en beïnvloeding van verkiezingen inmiddels nauw met elkaar samenhangen. Het recente schandaal met Cambridge Analytica is alom bekend. Maar dit soort praktijken zijn niet voorbehouden aan landen buiten de EU. Ook in Nederland is beïnvloeding van het democratisch bestel een reëel risico. De vraag is in hoeverre burgers nog een echt vrije keuze hebben als zij doorlopend beïnvloed worden door of via grote en

machtige partijen. We zien steeds vaker dat politieke partijen met *microtargeting* groepen kiezers proberen te beïnvloeden, veelal via diensten van derde partijen. Verleiden is uiteraard van alle tijden, maar transparantie en een gelijk speelveld zijn cruciaal voor vrije verkiezingen.

De overheid en (gevoelige) persoonsgegevens

Naast bedrijven beschikken centrale en lokale overheden, uitvoeringsorganisaties en politie en justitie over veel – vaak gevoelige en bijzondere – persoonsgegevens. Mensen zijn meestal verplicht om hun persoonsgegevens af te geven aan de overheid. Daarom moet iedereen erop kunnen vertrouwen dat de overheid zorgvuldig met deze gegevens omgaat en inzicht biedt in wat er met deze gegevens gebeurt. De overheid verwerkt persoonsgegevens op basis van specifieke wetgeving die als doel heeft dat de overheid niet meer persoonsgegevens verwerkt dan noodzakelijk is. Daarnaast moet ook de overheid uiteraard aan de AVG voldoen en bijvoorbeeld gegevens goed beveiligen en transparant zijn over het gebruik van gegevens. We zien nog te vaak dat dit niet goed gaat, terwijl de burger juist van de overheid – als hoeder van de rechtsstaat – het goede voorbeeld zou mogen verwachten.

Het koppelen van bestanden en geautomatiseerd analyseren van grote hoeveelheden gegevens is een belangrijke ontwikkeling voor de overheid de komende jaren, zowel binnen Nederland als binnen Europa. Zo wordt er op Europees niveau 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 dat de overheid 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.

Daarnaast kunnen overheidsorganisaties profielen van burgers opstellen op basis van informatie over bijvoorbeeld hun economische situatie, gezondheid en locatie. Hierdoor kan de overheid het mogelijk handelen van deze personen voorspellen, bijvoorbeeld om fraude met uitkeringen op te sporen en te voorkomen. Dit soort '*big nudge*' of voorspellingssystemen gebruiken en ermee experimenteren – al dan niet in samenwerkingsverbanden – is niet zonder risico's. Het kan leiden tot onjuiste beslissingen, discriminatie en buitenwettelijk overheidshandelen.

Wij verwachten dat functionarissen gegevensbescherming (FG's) binnen overheidsorganisaties steeds vaker de vraag zullen krijgen of zij dit soort ontwikkelingen toelaatbaar vinden. (Lokale) politici en overheidsbestuurders zullen steeds vaker geconfronteerd worden met technische en ethische vraagstukken die te maken hebben met de digitale datasamenleving. Daarbij zullen spanningen ontstaan tussen effectiviteit, rechtmatigheid en behoorlijkheid van het overheidshandelen.

2.3 Trend: toename van privacybewustzijn

Mede door de komst van de AVG en de Richtlijn politie& justitie ziet de AP dat bedrijven, organisaties en burgers zich langzaamaan meer bewust worden van de privacyrisico's en daar ook grip op willen krijgen.

Verantwoordelijkheid stimuleren

Veel organisaties willen werk maken van de AVG, ook al gaat dat niet altijd zonder slag of stoot. Onze Britse toezichtcollega, de Information Commissioner's Office (ICO), spreekt over het creëren van 'a culture of accountability', die de verantwoordelijkheid van bedrijven, organisaties en burgers benadrukt. We zien dat zowel bedrijven als overheidsorganisaties de omgang met privacy en de beveiliging van persoonsgegevens opnemen in hun reguliere compliancebeleid of onderdeel maken van maatschappelijk verantwoord ondernemen. Accountants toetsen ook steeds vaker compliancerisico's. Privacy en gegevensbescherming worden naar onze verwachting een *unique sellingpoint* van organisaties, zowel in de zakelijke sector als in de consumentenmarkt.

Privacy by design / privacy in de haarvaten

De AVG schrijft voor dat bedrijven en organisaties standaard rekening moeten houden met privacy en gegevensbescherming wanneer zij diensten en producten ontwerpen. In hoeverre dit al staande praktijk is, valt nog moeilijk te zeggen. Het toepassen van *privacy by design* en *privacy by default* is echter wel noodzakelijk in een datasamenleving. Dit betekent bijvoorbeeld dat er bij het ontwerp van systemen zo min mogelijk persoonsgegevens worden verzameld (dataminimalisatie) (*by design*). En dat bijvoorbeeld bij (IoT)-producten automatisch de meest privacyvriendelijke optie wordt gebruikt (*by default*).

Privacy by design vraagt dat zowel private als publieke partijen verantwoordelijkheid nemen en dit principe toepassen. Zoals ook de wet voorschrijft, ligt de verantwoordelijkheid bij bedrijven en organisaties om aan te tonen dat zij aan de privacyregels voldoen. In de private sfeer zullen de bedrijven die nu verantwoordelijkheid nemen, een competitieve voorsprong hebben op die sectoren en branches die zich tegen de AVG-regels proberen te verzetten.

Privacybewustzijn bij burgers

Burgers worden zich langzaamaan steeds meer bewust van hun privacy. Nederland scoort in Europees verband zeer hoog als het gaat om de bekendheid met de AVG en de privacytoezichthouder.[6] Ook maakt 94% van de Nederlanders zich zorgen over de bescherming van zijn of haar persoonsgegevens. 88% zegt echter nog nooit gebruik te hebben gemaakt van zijn privacyrechten. Een deel weet niet hoe dat moet of vindt het 'gedoe'.[7] Voor individuele consumenten is het bovendien vaak lastig te overzien wat de gevolgen zijn van keuzes, zoals toestemming geven voor het gebruik van persoonlijke gegevens. In de praktijk zijn veel van deze keuzes noch een bewuste of echte keuze, noch een vrije keuze.

Op dit moment ervaren burgers dus nog onvoldoende handelingsperspectief om zelf het heft in handen te nemen. Ze voelen zich onvoldoende in staat om verantwoordelijkheid te nemen. De uitdaging voor consumenten wordt om de komende jaren meer privacybewust te worden. Dat gebeurt al, maar kan nog meer. Zo geven bepaalde scholen al lessen om kinderen al jong *privacy smart* te maken.

[6] Europese Barometer, juni 2019, https://www.privacy-web.nl/cms/files/2019-06/ebs487a-en.pdf
[7] Onderzoek in opdracht van de AP.

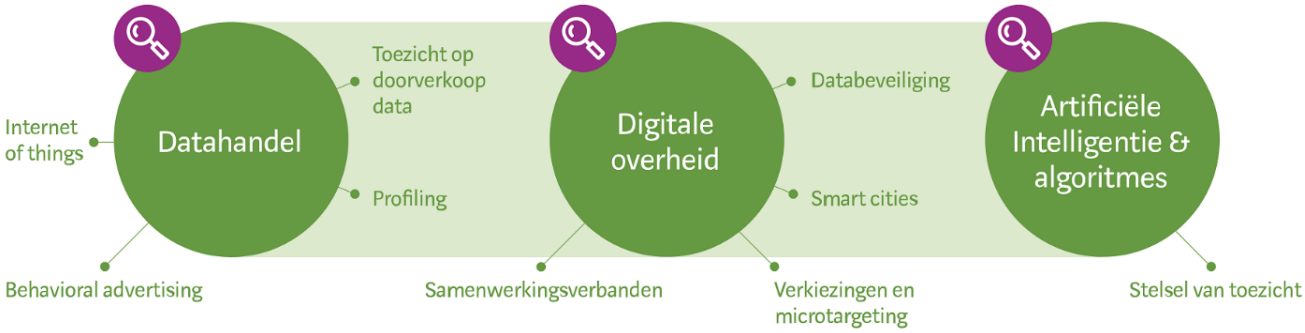
3. Focusgebieden

Het voorgaande hoofdstuk laat zien hoe groot, divers en complex de risico's van de digitaliserende samenleving zijn voor de bescherming van persoonsgegevens. Het is noodzakelijk om te kiezen. Om de juiste problemen aan te kunnen pakken houdt de AP risicogestuurd toezicht. Dat betekent dat de AP toezicht houdt door altijd op een methodische, kennisrijke en beheerste manier een beeld, oordeel en besluit te vormen. Daarbij is het uitgangspunt dat de AP gespitst is op onderwerpen met een groot risico voor burgers.[8]

Om als toezichthouder onze missie en ambities waar te maken en de trends zoals hiervoor beschreven te beïnvloeden, kiezen wij voor drie focusgebieden. De keuze voor deze focusgebieden is ingegeven door een aantal criteria. Het gaat om thema's die breed genoeg zijn, die in meerdere sectoren spelen en waarbij de AP het verschil kan maken door grenzen te markeren: wat kan wel of niet onder de AVG. Het gaat daarnaast om focusgebieden die direct raken aan de missie van de AP en die passen binnen de trends zoals hiervoor geschetst. De onderstaande drie gebieden krijgen de komende jaren extra nadruk in ons toezicht, zonder andere ontwikkelingen en de werkzaamheden die voortkomen uit onze wettelijke taak uit het oog te verliezen. De focusgebieden voor de komende jaren zijn:

- Datahandel
- Digitale overheid
- Algoritmes & AI

8 Voor een uitgebreidere toelichting op risicogestuurd toezicht zie hoofdstuk 4.



Datahandel
Data maken producten en diensten steeds slimmer en deze producten en diensten creëren vervolgens weer meer data. Dit heeft voordelen maar ook nadelen: er vindt steeds meer ongeoorloofde doorverkoop van persoonsgegevens aan derden plaats.

Digitale overheid
Centrale en lokale overheden, uitvoeringsorganisaties en politie en justitie beschikken over een grote hoeveelheid – vaak gevoelige en bijzondere – persoonsgegevens. De overheid werkt gericht aan het inzetten van persoons gegevens. Het is van belang dat de overheid verantwoordelijk omgaat met persoonsgegevens.

AI & algoritmes
Steeds meer bedrijven en organisaties maken gebruik van algoritmes en AI. Dit biedt voordelen en leidt tot nieuwe nuttige toepassingen. Maar de inzet van AI en algoritmes kent ook risico's en schadelijke effecten.

3.1 Focusgebied Datahandel

Zoals beschreven in hoofdstuk 2, worden er steeds meer (persoons)gegevens verwerkt en blijft de datastroom toenemen. In feite is het een vicieuze cirkel: data maken producten en diensten steeds slimmer en deze producten en diensten creëren vervolgens weer meer data. Dit heeft voordelen: de data kunnen worden gebruikt om bijvoorbeeld gericht producten en diensten aan te bieden.

De AP ziet echter ook dat er steeds meer ongeoorloofde doorverkoop van persoonsgegevens aan derden plaatsvindt: illegale datahandel. We onderscheiden hierin enerzijds de datahandelaren (*brokers*). Dit zijn ondernemingen die hun geld enkel en alleen verdienen met de (internationale) doorverkoop van gegevens. Anderzijds zien we dat steeds meer 'normale' bedrijven ook gegevens doorverkopen. Bijvoorbeeld een bedrijf dat de gegevens (resultaten) uit een stappenteller-app zonder toestemming verkoopt aan een verzekeraar. De verzekeraar gebruikt deze gegevens om iemand een profiel en score op te leggen en daar een risico- en premieklasse aan te koppelen. Mensen verliezen hierdoor de grip op hun data en kunnen ook hun rechten niet meer uitoefenen.

Mensen moeten erop kunnen vertrouwen dat organisaties niet zomaar persoonsgegevens doorgeven, zonder dat zij dat weten of ermee instemmen. Zoals de AVG stelt: mensen hebben 'informationele zeggenschap' over hun eigen persoonsgegevens. Dit betekent dat het vrije verkeer van persoonsgegevens alleen vrij is zolang aan die zeggenschap recht wordt gedaan. De AP is de grondrechtenbeschermer op deze grensoverschrijdende datamarkt. In samenwerking met onze EU-collega's geven we grenzen aan, stimuleren we eerlijke datahandel en treden we op tegen overtredingen. Op die manier kan de internationale digitale dataeconomie duurzaam tot bloei komen.

De AP streeft ernaar dat verantwoord datagebruik een onderdeel wordt van beleid voor maatschappelijk verantwoord ondernemen (MVO) en van de *Corporate Governance Code*. Waar de vragen in de bestuurskamers zich eerst richtten op de vraag óf de AVG geïmplementeerd is, zoals óf er een verwerkingenregister is, zullen de vragen de komende periode verschuiven naar de vraag of de grondslag voor de verwerking wel op orde is en naar risicobeheersing: hoe voorkomen wij een datalek? En welk niveau van risicoacceptatie vinden wij verantwoord in onze sector?

Het focusgebied Datahandel wordt programmatisch aangepakt. De belangrijkste aandachtsgebieden binnen Datahandel zijn:

- Toezicht op doorverkoop data
- Internet of things (IoT)
- Profilering
- Behavioral advertising

Aandachtsgebied Toezicht op doorverkoop data

Datahandelaren verzamelen op grote schaal persoonsgegevens van consumenten via verschillende online en offline bronnen. Zij verwerken de gegevens tot profielen en verkopen deze door. Dit kan leiden tot ongemerkte sturing en ongevraagde advertenties. Ook bestaat het risico dat onjuiste data worden doorverkocht.

De AP wil dat de handel in persoonsgegevens zich op een manier ontwikkelt die recht doet aan de zeggenschap van burgers over hun data. Om effectief te kunnen optreden, is het van belang om datastromen bloot te leggen en de directe en indirecte gevolgen in kaart te brengen. We volgen daarnaast de grote partijen – datahandelaren en bedrijven met grote hoeveelheden data, zoals technologiebedrijven – op de voet om inzicht te krijgen in de bedrijfsprocessen.

We maken duidelijk: de verantwoordelijkheid voor het rechtmatig, behoorlijk en transparant verzamelen en doorverkopen van gegevens ligt bij de datahandelaren. De aanpak van de AP omvat dat wij rechtmatig datamarktgedrag bevorderden en de eigen verantwoordelijkheid van bedrijven stimuleren. De AP treedt handhavend op tegen bedrijven die zich niet aan de wet houden.

De AP vindt het daarnaast belangrijk dat mensen zicht hebben op de vele verschillende datastromen die onze samenleving doorboren. Dat is op dit moment nog niet het geval. Mensen lijken zich daarnaast weinig bewust van hun privacyrechten. Zij moeten de kans krijgen om hun rechten uit te oefenen. Dit betekent enerzijds dat bedrijven vooraf actief en op toegankelijke wijze duidelijk moeten maken wat zij doen. Tegelijkertijd zullen mensen, daar waar dat kan, zelf verantwoordelijkheid moeten nemen. De rol van de AP is hier om voorlichting te geven, met als doel dat mensen ook echt in actie kunnen komen. Het uiteindelijke doel is een duurzame cultuurverandering bij zowel bedrijven als mensen in de hele Europese Unie.

Aandachtsgebied Internet of things (IoT)

Het aantal huishoudens, organisaties en personen dat gebruik maakt van IoT-apparaten groeit aanzienlijk; van kinderen (knuffels, speelgoed, tablets), ouderen (camera's, sensoren, zorgrobots) tot patiënten (*pacemakers*, insulinepompen, gehoorimplantaten). Het gaat hier zowel om apparaten in het publieke domein – *smart cities*, surveillance – als apparaten in het privédomein – *eHealth*, spraakassistenten, *smart home*. Deze apparaten zijn veelal het startpunt van een enorme dataverzameling. Deze verzameling biedt – als deze groot genoeg wordt en met voldoende rekenkracht – niet alleen marktmacht, maar ook geopolitieke macht. Denk bijvoorbeeld aan een niet-Europese producent die miljoenen apparaten maakt die ook op de Nederlandse en Europese markt terechtkomen. Deze producent kan zo beschikken over gevoelige gegevens over en van burgers uit andere landen.

De AP vindt het van belang dat de IoT-markt zich de komende jaren goed, duurzaam en beheersbaar ontwikkelt. Daarbij zijn wij ons ook bewust van de geopolitieke aspecten van deze ontwikkeling. De AP verwacht van aanbieders, zowel publiek als privaat, dat zij voldoende transparant zijn over welke gegevens er worden verzameld en welke risico's er kleven aan het gebruik van de verschillende apparaten. De hoeveelheid data minimaliseren en goed omgaan met de verzamelde gegevens kan de steeds groter wordende problemen verderop in de dataketen voorkomen. Ook verwacht de AP dat IoT-apparaten voldoende beveiligd worden. De AP pakt bedrijven aan die de wet niet naleven.

De AP stimuleert in de komende periode het ontwikkelen van productiestandaarden voor IoT-producten en het AVG-certificeren hiervan. Samenwerking met andere toezichthouders ligt hier voor de hand. Ook wil de AP zich actief mengen in het debat over de ontwikkeling van duurzame, maatschappelijk verantwoorde IoT. Dataminimalisatie, *privacy by design* en *privacy by default* zullen hierbij belangrijke onderwerpen zijn.

Aandachtsgebied Profilering

Naast het feit dat er veel meer data worden gegenereerd, verzameld en vastgelegd, worden er op basis van die data profielen gemaakt. Steeds meer bedrijven en organisaties gebruiken die profielen om gericht diensten en producten aan te bieden. Ons profiel en bijbehorende score bepalen vervolgens op welke manier zij ons behandelen of benaderen of juist niet benaderen. Deze profilering kan een zodanig karakter krijgen dat sommige groepen mensen gediscrimineerd en uitgesloten kunnen worden.

De AP streeft ernaar dat bedrijven en organisaties profilering zo toepassen dat zij de rechten van mensen niet schenden en discriminatie voorkomen. De AVG schrijft voor dat bedrijven en organisaties data eerlijk moeten verwerken en dat zij transparant moeten zijn over hoe ze profielen samenstellenen hoe ze profilering inzetten. De AP ziet hierop toe.

Aandachtsgebied 'Behavioral advertising'

De online advertentie business heeft met het internet een grote vlucht genomen. De technische mogelijkheden om mensen te volgen, profielen op te stellen en deze in korte tijd op online markten te verkopen, zijn volop in gebruik.

De AP zal aansturen op nieuwe gedragscodes die recht doen aan de eisen van onder meer transparantie en toestemming. Verschillende sector- en brancheorganisaties zijn hier al mee bezig; positieve initiatieven verdienen het om onder de aandacht gebracht te worden. Ook legt de AP het onbeperkt en zonder wettelijke basis volgen van persoonlijk surfgedrag en het doorverkopen daarvan aan banden. De AP treedt handhavend op als dat nodig is.

3.2 Focusgebied Digitale overheid

Naast bedrijven beschikken centrale en lokale overheden, uitvoeringsorganisaties en politie en justitie over veel – vaak gevoelige en bijzondere – persoonsgegevens. De overheid werkt ook gericht aan het inzetten van gegevens.[9] Dit is ook nodig; de overheid kan niet achterblijven in digitalisering. Het is noodzakelijk om maatschappelijke en economische kansen te creëren. Ook op het gebied van veiligheid en terrorismebestrijding kunnen data een belangrijke rol spelen.

[9] Recente publicaties zoals *Nederlandse Digitaliseringsstrategie voor 2018-2021*, de *Data agenda* en het rapport *Nederland digitaal* bewijzen dit.

Het focusgebied wordt programmatisch aangepakt. De belangrijkste aandachtsgebieden binnen Digitale overheid zijn:

- Databeveiliging
- *Smart cities*
- Samenwerkingsverbanden / ongeoorloofd delen
- Verkiezingen en *microtargeting*

Overheidsorganisaties hebben een bijzondere positie doordat zij over zoveel (gevoelige) persoonsgegevens beschikken. De AP vindt het belangrijk dat de overheid verantwoordelijk omgaat met persoonsgegevens.

Aandachtsgebied Databeveiliging

De beveiliging van persoonsgegevens bij de overheid laat nog vaak te wensen over. Slechte beveiliging kan leiden tot een datalek. De impact van datalekken bij de overheid kan erg groot zijn, omdat het vaak gaat om enorme hoeveelheden bijzondere of gevoelige persoonsgegevens. Het is daarom belangrijk dat overheidsorganisaties aandacht hebben voor de beveiliging van gegevens. Zeker als het gaat om zeer gevoelige dossiers, zoals in de jeugdzorg of bij politie en justitie.

De AP verwacht van overheidsorganisaties dat zij structureel en op toereikende wijze investeren in hun informatiebeveiliging. De komende jaren wil de AP overheidsorganisaties controleren op hun beveiligingsniveau en hen stimuleren om werk te maken van een sterke IT- en datahuishouding. De AP wil bevorderen dat overheidsorganisaties behendig worden in privacyrisicomanagement en hun IT-systemen laten *auditen* als onderdeel van hun databoekhouding.

Aandachtsgebied *Smart cities*

Steden, stedelijke gebieden en gemeenten zijn steeds vaker op zoek naar slimme oplossingen voor vraagstukken op het gebied van mobiliteit, energie, veiligheid en huisvesting. Deze slimme oplossingen vinden zij in sensoren en data. Ondersteund door technologieën zoals *machine learning* proberen steden data te verzamelen of slim data te combineren over bijvoorbeeld afvalstromen, energiegebruik of stromen van mensen. Door slim gebruik van de data kunnen bewoners 'verleiden' tot betere keuzes en het gebruik van de openbare ruimte optimaliseren. Hiermee raken steden en gemeenten aan de grenzen tussen het openbaar belang en de privacy van bewoners.

De alomtegenwoordigheid van sensoren heeft ook grote risico's. Mensen worden overal gevolgd, of geïdentificeerd, en kunnen zich niet onttrekken aan sensoren – je weet immers niet waar ze zitten. Op die manier sturen en beïnvloeden steden en gemeenten hun inwoners.

De AP vindt het belangrijk dat overheidsorganisaties vroegtijdig in hun processen stilstaan bij de grondrechten en keuzevrijheden van mensen. Zeker ook omdat in de praktijk van *smart cities* niet alleen gemeenten een rol spelen, maar ook bedrijven en dat tegen die achtergrond publieke belangen soms verweven kunnen raken met private belangen. De AP spreekt overheidsorganisaties erop aan dat zij hun processen zodanig inrichten dat zij zo min mogelijk persoonsgegevens verzamelen (*privacy by design*). De AP zal de ontwikkelingen op dit terrein volgen en in kaart brengen. Waar nodig treedt de AP handhavend

op. De aandacht van de AP gaat in eerste instantie uit naar de ontwikkeling van *smart city*-projecten door de overheid en naar de rechten van burgers.

Aandachtsgebied Samenwerkingsverbanden / ongeoorloofd delen

Steeds vaker deelt en koppelt de overheid bestanden; van centraal tot lokaal, al dan niet in Europees verband. Dit gebeurt zowel tussen overheidsorganisaties onderling als tussen de overheid en de private sector. Het uitwisselen van gegevens gebeurt binnen samenwerkingsverbanden. De overheid doet dit bijvoorbeeld om de publieke dienstverlening beter te maken, misbruik van publieke middelen tegen te gaan en zware criminaliteit op te sporen. Zo kijkt de overheid naar data om bijvoorbeeld eerder problematische schulden te ontdekken of om te voorspellen of iemand radicaliseert.

Hoewel de intenties vaak goed zijn, kan het delen en koppelen van bestanden een schending zijn van het wettelijke beginsel van doelbinding. Dit principe houdt in dat gegevens die voor een bepaald doel zijn verzameld, niet voor een ander doel gebruikt mogen worden. Tenzij in wet- of regelgeving duidelijk en nauwkeurig is vastgelegd dat het voor een bepaald doel mag en waarbij de toepassing dan voldoende voorspelbaar is. De overheid moet daarom voorzichtig zijn met bestanden aan elkaar koppelen, zelfs als dat kostentechnisch voor de hand ligt. De gedachte hierachter is dat een lagere prijs voor verbeterde publieke dienstverlening niet ten koste mag gaan van vrijheid. Ook moet de overheid vanuit behoorlijkheid handelen en kunnen instaan voor de juistheid van de data en modellen.

De AP verwacht dat overheidsorganisaties terughoudend zijn met het delen van bestanden. Het is aan overheidsbestuurders en aan de wetgever om een goede afweging te maken over het nut en de noodzaak van het gebruik van data en nieuwe verwerkingen. De AP spreekt bestuurders hierop aan. Schending van het beginsel van doelbinding pakt de AP zo nodig aan. Dit betekent ook dat de wetgever het beginsel van doelbinding in acht moet houden bij het opstellen van nieuwe wetgeving, zowel op nationaal als op Europees niveau.

Aandachtsgebied Verkiezingen en *microtargeting*

Politieke partijen verwerken en gebruiken steeds vaker persoonsgegevens, met als doel zo gericht mogelijk hun leden te bereiken. Ook maken zij gebruik van externe partijen om dit werk voor hen te doen. De Europese wetgever heeft aangegeven dat dit op grond van een algemeen belang is toegestaan, maar dat er wel waarborgen worden vastgesteld. Een rechtmatige, behoorlijke en transparante verwerking is belangrijk om vrije verkiezingen in een open samenleving te waarborgen. Dat heeft de zaak rondom Cambridge Analytica wel duidelijk gemaakt. Hierbij zijn gegevens gebruikt van miljoenen mensen, waaronder niet-leden, zonder hun toestemming. Verschillende instanties binnen en buiten Nederland hebben dergelijke ontwikkelingen onderzocht.

De AP houdt toezicht op de naleving van de AVG door politieke partijen. Dit doet de AP door verkennend onderzoek te doen, nadere normen te formuleren, zelfregulering te stimuleren en eventueel te handhaven. De AP hecht hierbij veel waarde aan samenwerking met de Europese collega's.

3.3 Focusgebied Artificiële intelligentie & algoritmes

De beschikbaarheid van grote hoeveelheden data die steeds dieper inzicht geven in het online en offline leven van mensen, maakt het mogelijk om steeds meer processen te analyseren en te automatiseren. Het

geautomatiseerd analyseren van data om inzicht te krijgen in personen, beslissingen te modelleren en op basis daarvan bepaalde diensten of producten wel of niet te leveren, resulteert in geautomatiseerde besluitvorming.

Het focusgebied wordt programmatisch aangepakt. Het belangrijkste aandachtsgebied binnen Artificiële intelligentie & algoritmes is:

- Stelsel van toezicht

De inzet van algoritmes is niet nieuw. Het wetenschapsgebied artificiële intelligentie (AI) heeft de laatste tien jaar een enorme ontwikkeling doorgemaakt, met name op de mogelijkheden van *machine learning, neural networks* en *deep learning*. Door deze ontwikkelingen worden algoritmische beslismodellen en kunstmatig intelligente systemen krachtiger en complexer.

Deze 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. Dat heeft duidelijke voordelen. Bedrijven en organisaties kunnen snel en efficiënt besluiten nemen door grote hoeveelheden data te analyseren. Denk aan het snel toekennen van een verzekering of hypotheek aan een klant. Maar denk ook aan de mogelijkheden die deze technologie biedt in bijvoorbeeld de gezondheidszorg.

Maar de inzet van AI en algoritmes kent ook risico's. Bedrijven en organisaties gebruiken dit ook om mensen gericht te sturen (*nudging*) en te profileren. Er zijn belangrijke vragen over de kwaliteit van de gebruikte data, de uitkomsten op basis waarvan beslissingen worden genomen en de inzichtelijkheid van het proces. Data zijn niet altijd juist of rechtmatig verkregen, de uitkomsten geven niet altijd een passend beeld van de werkelijkheid en zowel betrokkenen als autoriteiten (zoals de AP als toezichthouder) kunnen niet altijd inzicht krijgen in de processen. Bovendien kunnen betrokkenen niet altijd hun rechten uitoefenen. Daarnaast zijn er ethische vraagstukken over de ontwikkeling en inzet van complexe AI-systemen en algoritmes. Hierover zal een maatschappelijk debat gevoerd moeten worden, waarin deskundigen en betrokkenen een balans bereiken tussen enerzijds een maatschappelijk positieve inzet van AI en algoritmes en anderzijds bescherming van de fundamentele rechten.

Omdat zowel private als publieke partijen AI en algoritmes gebruiken en er veel maatschappelijke vragen rondom deze onderwerpen spelen, kiest de AP ervoor om er speciale aandacht aan te besteden – het vormt daarom een eigen focusgebied.

Aandachtsgebied Stelsel van toezicht

De politiek en de samenleving roepen steeds sterker om toezicht op AI en algoritmes. En niet zonder reden. De AP vindt dat mensen erop moeten kunnen vertrouwen dat bedrijven en organisaties zorgvuldig met hun persoonsgegevens omgaan. De AVG-beginselen van rechtmatigheid, behoorlijkheid en transparantie bieden een goede basis om de ontwikkeling en inzet van AI en algoritmes positief te laten bijdragen aan de samenleving. Daarnaast moet de inzet van AI en algoritmes behoorlijk zijn. Dat wil zeggen dat systemen robuust en accuraat zijn, ingezet worden voor de juiste doelen en dat zij groepen mensen niet zonder meer uitsluiten. Ook is het van belang voor het toezicht en voor betrokkenen om inzicht te kunnen krijgen in hoe gegevens worden verwerkt en hoe besluiten tot stand komen.

Als AP zijn wij verantwoordelijk voor het toezicht op persoonsgegevens en daarmee ook op de toepassing van AI en algoritmes waarin persoonsgegevens worden gebruikt. De AVG biedt ook een belangrijke wettelijke basis voor het toezicht op AI en algoritmes. Zo zijn er naast de beginselen van de AVG ook artikelen gewijd aan bijvoorbeeld profilering en geautomatiseerde besluitvorming.

In de komende periode zal de AP zich richten op het vormgeven van een stelsel van toezicht op AI en algoritmes waarin persoonsgegevens worden gebruikt. Hierin werken wij samen met relevante partijen binnen en buiten Nederland. Wij zullen ons onder meer richten op de inzichtelijkheid en uitlegbaarheid van geautomatiseerde besluiten. Een betrokkene mag verwachten dat bij de toepassing van AI en algoritmes uitleg mogelijk is over het proces, de belangrijke elementen en hoe dit resulteert in uitkomsten. Dit laat nog vaak te wensen over. Het is van belang dat bedrijven en organisaties die geautomatiseerd besluiten nemen aan de eisen uit de AVG voldoen, zoals de informatieplicht, transparantie, uitlegbaarheid en menselijke tussenkomst.

Belangrijke onderdelen van het verantwoord gebruik van geautomatiseerde besluitvorming zijn ook ervoor zorgen dat betrokkenen hun rechten kunnen uitoefenen en dat verwerkers aan hun informatieplicht voldoen. Het risico is dat betrokkenen op basis van slechte, onjuiste of onvolledige informatie worden uitgesloten van diensten, producten of maatschappelijke mogelijkheden. De AP wil waken over de groepen mensen die minder zicht hebben op deze ontwikkelingen, maar hier wel disproportioneel mee geconfronteerd kunnen worden.

4. Strategie

In dit hoofdstuk staat hoe wij onze toezichtstaak- en missie invullen en welke instrumenten en middelen wij kunnen inzetten. Kortom: hoe is ons toezicht de komende jaren georganiseerd?

4.1 De AP als toezichthouder

Missie

De Autoriteit Persoonsgegevens is de onafhankelijke toezichthouder in Nederland die de bescherming van persoonsgegevens bevordert en bewaakt.

Meer uitgewerkt betekent dit het volgende:

Bevorderen

Wij bevorderen dat bedrijven en organisaties hun verantwoordelijkheid nemen om rechtmatig persoonsgegevens te verwerken en deze gegevens te beschermen. Daarnaast stimuleren we, bijvoorbeeld met voorlichtingscampagnes, dat ook mensen zelf hun verantwoordelijkheid nemen. Wij gaan steeds na of bedrijven en organisaties gebruikmaken van AVG-instrumenten en of ze hun functionaris gegevensbescherming (FG) op de juiste manier in positie brengen. De FG geeft de organisatie niet alleen

advies, maar houdt ook intern toezicht op de naleving van de AVG. De FG is hiermee een belangrijke speler die bedrijven en organisaties in staat stelt verantwoordelijkheid te nemen voor hun eigen privacy- en gegevensveiligheidsbeleid. We monitoren de mate van compliancebereidheid en gedegen risicomanagement. Ook onderhouden wij contact met verwerkingsverantwoordelijken over de knelpunten die zij daarbij ervaren. Waar nodig bieden wij *guidance*, met name aan FG's, en stimuleren wij het gebruik van instrumenten voor zelfregulering op sectoraal of brancheniveau. Hierbij houden wij rekening met het specifieke van kleinere ondernemingen. Daarnaast geven we voorlichting en zetten we slimme communicatiemiddelen in om compliance te bevorderen. Op Europees niveau werken wij aan duidelijke *guidance* en gezamenlijke normuitleg. Zo worden de rechten van burgers en de plichten van verantwoordelijken in de gehele EU op dezelfde manier geïnterpreteerd en ontstaat er een Europees *level playing field*, met een hoog beschermingsniveau van persoonsgegevens.

Bewaken

Wij bewaken de naleving van privacyregels door onafhankelijk onderzoek te doen naar (mogelijke) overtredingen door de overheid en het bedrijfsleven. Dat doen wij op eigen initiatief of naar aanleiding van een klacht. Als dat nodig is, treden wij handhavend op. Hierbij hebben we verschillende handhavingsinstrumenten tot onze beschikking. Wij kiezen een instrument door te kijken naar wat het meest gewenst is vanuit het oogpunt van bestraffing of speciale en generale preventie. Daar kunnen wij ook het wederrechtelijk voordeel bij betrekken dat is verkregen door de onrechtmatige verwerking.

Als lid van de European Data Protection Board (EDPB) werken wij nauw samen met collega-toezichthouders. Zo nemen we als leidende toezichthouder het voortouw in grensoverschrijdende zaken en treden we waar nodig actief op als betrokken toezichthouder. Ook zetten wij in op gezamenlijke Europese onderzoeken (*joint investigations*), om bij te dragen aan een eenduidige toepassing van de AVG in de gehele EU.

De bevorderende en bewakende kant van het AP-brede toezicht zijn communicerende vaten.

Visie

Waar de missie ons bestaansrecht weergeeft, vertelt onze visie het verhaal waar wij als toezichthouder naartoe willen. Het geeft ons ook richting in de keuzes die wij maken.

Wij streven naar een digitale samenleving waarin de bescherming en rechtmatige verwerking van onze persoonsgegevens vanzelfsprekend is. Overheden en bedrijven organiseren hun eigen dataprotectie op een hoog niveau. De FG speelt hierin een essentiële rol als adviseur en interne toezichthouder.

In het nastreven van deze visie stellen we ons op als een toezichthouder die ontwikkelingen beïnvloedt, issues op de kaart zet, problemen bij de wortel aanpakt en handhavend optreedt bij overtredingen. Hierbij zetten wij ook in op Europese samenwerking, om zo duidelijkheid te bieden aan bedrijven en om burgers zo goed mogelijk te beschermen.

De ambitie is om in 2023 een invloedrijke privacytoezichthouder te zijn in Europa. Wij kunnen immers alleen effectief zijn als wij internationaal kansen pakken en kaders stellen.

Risicogestuurd toezicht

Het realiseren van onze visie vraagt om een slimme aanpak. Een aanpak waarbij het even belangrijk is om aan te geven wat we wel doen als wat we niet doen en waarom niet. Waarbij preventief optreden minstens zo belangrijk als repressief. En waarbij soms niet de AP, maar een sector zelf of de wetgever in actie komt. En waarbij we accepteren dat een toezichthouder niet alles kan aanpakken of alle risico's kan uitbannen.

Om de juiste problemen aan te kunnen pakken houdt de AP risicogestuurd toezicht, zoals ook kort aangestipt in hoofdstuk 3. Risicogestuurd toezicht betekent dat de AP toezicht houdt door altijd op een methodische, kennisrijke en beheerste wijze een beeld, oordeel en besluit te vormen. Het uitgangspunt hierbij is dat de AP gespitst is op onderwerpen met een groot risico voor burgers. Daarbij wegen we onder andere af om hoeveel data het gaat en of het om gevoelige of bijzondere persoonsgegevens gaat.

Wij beoordelen risico's binnen uiteenlopende sectoren en onderwerpen op de kans dat ze zich voordoen en op de impact ervan op het dagelijks leven van mensen. Op basis daarvan gebruiken we een of meerdere instrumenten uit onze instrumentenmix. We streven ernaar dát instrument, of een mix van instrumenten, in te zetten waarmee we als toezichthouder zo effectief mogelijk kunnen zijn. Dat wil zeggen: we pakken het probleem aan en voorkomen recidive.

Onderdeel van ons risicogestuurd toezicht is dat we ook actief nadenken over de verdere ontwikkeling van effectmeting. Ook vanwege de toenemende roep om verantwoording naar de buitenwereld. Daarbij kijken we naar vragen als: wat is goed toezicht? Wat is de maatschappelijke opbrengst? Neemt de kwaliteit van de processen van bedrijven en organisaties toe? Wanneer zijn we tevreden over de inzet van onze instrumenten? Welke instrumenten ontbreken nog in onze gereedschapskist?

4.2 Onze instrumenten

De komende periode zijn wij bezig om ons toezicht en onze organisatie verder te professionaliseren. Goed toezicht vergt dat wij de juiste balans hanteren tussen bevorderen en bewaken hanteren. Of anders gezegd: tussen het stimuleren van 'goed' gedrag en handhavend optreden waar nodig.

Bevorderen

Verantwoordelijkheid stimuleren

De AVG is een *accountability based* wet. Dit wil zeggen dat het aan bedrijven en organisaties zelf is om aan te tonen dat zij aan de privacywetgeving voldoen. Dit noemen we de verantwoordingsplicht. Die plicht houdt in dat zij zelf de verantwoordelijkheid hebben om goed na te denken over hoe zij als bedrijf of organisatie persoonsgegevens verwerken en beschermen en zij dit moeten kunnen uitleggen. Dat de verantwoordelijkheid bij bedrijven en organisaties is belegd, heeft ook gevolgen voor de stijl van toezicht door de AP. Dit betekent namelijk dat wij veel verwachten van de eigen invulling door bedrijven en organisaties.

Wij trachten het zelfregulerende vermogen van Nederland zo goed mogelijk op gang te brengen. Dit doen wij onder meer door voorlichting te geven, een van onze wettelijke taken. Dit betekent dat we enerzijds brede voorlichtingscampagnes opzetten, in vervolg op de effectieve campagne 'Wat betekent privacy voor jou', en wij via onze website en sociale media communiceren. Anderzijds zetten wij handhavingscommunicatie in. Door proactief en reactief te communiceren over individuele casussen en fenomenen vergroten we de reikwijdte en uitstraling van ons toezichtwerk. Kordate handhaving is immers een voorwaarde voor effectieve speciale en algemene preventie.

We willen dat bedrijven en organisaties zelf nadenken over de bescherming van persoonsgegevens in hun bedrijfsprocessen. Dat vergt dat wij nauw in de gaten moeten houden of het hen lukt om hun eigen privacymanagement op orde te brengen, waar zij tegen aanlopen en om welke redenen zij vast kunnen lopen.

Vanwege de vaak technische complexiteit van veel verwerkingen, kan de AP niet kennis hebben over elke verwerking in elk bedrijf of elke organisatie. De AP maakt daarom gebruik van de kennis die aanwezig is in de bedrijven en organisaties en ontsluit deze bijvoorbeeld door gebruik te maken van interne toezichthouders (FG's). Interne experts weten immers het beste waar de risico's aanwezig zijn. Daarom

geeft de AP, waar nodig en gewenst, actief normuitleg om de FG's te ondersteunen in hun taak. Dat doen we zowel op nationaal niveau als in Europees verband. De AP stimuleert de verdere professionalisering van de beroepsorganisatie voor FG's en zal investeren in goed contact met privacyfunctionarissen in brede zin.

Kennisopbouw

Om goed gedrag te kunnen bevorderen is het essentieel om zicht hebben op de relevante ontwikkelingen. Dit houdt in dat wij de komende jaren onze kennis uitbouwen van de gevolgen van de digitalisering in verschillende sectoren op de privacybescherming. Dat betekent ook dat we trends en ontwikkelingen vroegtijdig onderkennen en bijsturen, afremmen of versnellen, kortom: beïnvloeden. Het betekent ook dat wij kennis hebben over de bedrijven en organisaties, over mogelijkheden van beïnvloeding en over de inzet en ontwikkeling van slimme (toezicht)instrumenten die zijn ontwikkeld voor deze nieuwe tijd. Dat vergt ook in het instrumentarium en de processen een nieuwe aanpak. Het betekent dat wij de eigen verantwoordelijkheid van bedrijven en organisaties en vormen van zelfregulering stimuleren, maar dat wij ook duidelijke kaders stellen.

Wetgevingsadvies

Door de hoge mate waarin Nederland gedigitaliseerd is, heeft wetgeving steeds vaker betrekking op grootschalige verwerkingen van persoonsgegevens. Een bijzonder instrument in handen van de AP is de adviseringsverplichting. Het gaat daarbij niet om toezicht op de naleving van bestaande regels in de praktijk, maar juist om voornemens voor nieuwe regels. De AVG eist ruimer dan voorheen dat de wetgever de AP actief raadpleegt over voorstellen voor wetgeving.

Daarnaast heeft de AP ook de ruimte om bij de totstandkoming van regelgeving en bestuursmaatregelen de betrokken instanties gevraagd of ongevraagd advies te geven over algemenere privacykwesties. Het voordeel van dit instrument is dat via een relatief eenvoudige procedure en al in een vroege fase bedreigingen voor de privacy voorkomen kunnen worden.

Dit geldt ook op Europees niveau. Als lid van de EDPB draagt de AP bij aan de wetgevingsadviezen die de EDPB opstelt over Europese wetsvoorstellen die gevolgen hebben voor de bescherming van onze privacy.

Bewaken

Onderzoek

Controlerend onderzoek is gericht op overtredingen vaststellen. Dit legt de basis om handhavingsmaatregelen te kunnen opleggen, zoals een boete. Controlerende onderzoeken vloeien direct voort uit klachten, tips of datalekmeldingen die de AP krijgt. Daarnaast kan de AP onderzoeken oppakken die niet direct zichtbaar zijn voor de burger, door mediaberichten, tips en klachten te verrijken of door eigen risico- en trendanalyses uit te voeren. Zo kunnen wij ook voor nieuwe ontwikkelingen de privacyrisico's in kaart brengen.

Handhaven

Handhaving op nationaal en internationaal niveau draagt op een niet te onderschatten wijze bij aan het creëren en bestendigen van een *level playing field* en ook aan een hoog niveau van privacybescherming. Door te handhaven laten we zien wat wij wel en niet acceptabel vinden en treden we op tegen bedrijven en organisaties die zich niet aan de wet houden. Ook handhavingscommunicatie is hierin een belangrijk instrument.

Sinds de inwerkingtreding van de AVG hebben wij nadrukkelijk ruimte gegeven aan bedrijven en organisaties om de nieuwe regels goed te implementeren. De komende jaren zullen wij partijen die hun verantwoordelijkheid niet nemen vaker bestraffen. Klachten van burgers zullen voor ons vaker aanleiding zijn om een onderzoek te starten en uiteindelijk – zo nodig – een waarschuwing te geven of een dwangsom

of boete op te leggen. Dergelijke maatregelen zijn effectief voor de betreffende organisatie, maar hebben daarnaast een breder uitstralingseffect op de samenleving als geheel.

Ook verwachten wij van bedrijven en organisaties dat zij *privacy by design* toepassen. Zo zorgen zij ervoor dat ze de AVG naleven en daarmee voorkomen ze dat de AP handhavend optreedt.

Europees en internationaal

Onderzoek

Wij houden niet alleen toezicht op nationale partijen, maar juist ook op het internationale bedrijfsleven en internationale organisaties. Gezien het grote aantal hoofdkantoren dat in Nederland gevestigd is, is de AP in veel gevallen de leidende toezichthouder. Dat betekent dat de AP als eerste verantwoordelijk is voor het toezicht op deze bedrijven en organisaties en dat de AP dus de onderzoeken hiernaar leidt.

Ook is de AP, mede vanwege de hoge mate van digitalisering van de Nederlandse samenleving, vaak een betrokken toezichthouder. Dat betekent dat de AP betrokken is bij onderzoeken van de leidende toezichthouder van een ander land, omdat de gegevensverwerking ook in Nederland impact heeft.

Het is voor de AP én de Nederlandse economie van groot belang om juist de komende periode – waarin de eerste resultaten van grote internationale onderzoeken worden verwacht – een actieve bijdrage te kunnen leveren aan de interpretatie, toepassing en handhaving van de nieuwe AVG-normen.

Europese wetgeving

De guidelines, (verplichte) adviezen en bindende besluiten die op internationaal en Europees niveau worden vastgesteld, bepalen hoe de AP de AVG en andere Europese privacywetgeving moet uitleggen en toepassen. Deze instrumenten hebben hierdoor directe gevolgen voor Nederlandse burgers, bedrijven en organisaties en de AP. Daarom stellen wij ons op internationaal niveau actief op, zoals bij de European Data Protection Board (EDPB).

4.3 Rollen

De AP houdt toezicht op een internationaal, veelomvattend en complex toezichtveld. De bedrijven en organisaties die onder ons toezicht staan, zijn diverser en met meer dan bij menig ander toezichthouder. Om effectief toezicht te houden moeten we investeren in slimme oplossingen en in de verbinding met anderen, inclusief de FG's en onze internationale collega's. Wij zien op een abstracter niveau drie rollen voor onszelf, die elkaar aanvullen en die we inzetten als de situatie daarom vraagt. Deze rollen sluiten elkaar niet uit, maar dienen vooral als middel om onze zeer verschillende doelgroepen het meest effectief te kunnen beïnvloeden. De primaire taak hierbij is onze rechtstatelijke opdracht.

Rechtstatelijke opdracht: beschermen van de grondrechten
In een vrije en democratische samenleving moeten mensen erop kunnen vertrouwen dat bedrijven en organisaties zorgvuldig omgaan met hun gegevens, nu en in de toekomst. Privacy is een grondrecht en voorwaarde voor onze rechtsorde. Het is een voorwaarde om vrij te zijn in wie je bent en wat je doet. Privacy gaat over zelfbeschikking, over dat mensen regie houden over hun gegevens. Wij zien erop toe dat mensen vrij in een stemhokje kunnen staan en vrij kunnen beslissen hoe zij hun toekomst willen vormgeven. De AP ziet zichzelf in die hoedanigheid als hoeder van de fundamenten van onze democratische rechtsorde. Ook omdat privacy een voorwaarde is om andere grondrechten te kunnen uitoefenen.

Ombudsfunctie-opdracht: opkomen voor burgers in de knel
Het uitgangspunt van een ombudsfunctie is dat deze opkomt voor burgers die niet (genoeg) voor zichzelf kunnen opkomen en die ook bij de overheid of bij bedrijven geen of onvoldoende gehoor vinden.
De AP staat voor de AVG-rechten van burgers. Zo behandelen wij de klachten van mensen die vermoeden dat hun persoonsgegevens zijn verwerkt in strijd met de wet. Denk bijvoorbeeld aan een persoon die ten onrechte wordt uitgesloten van bepaalde dienstverlening door een foutieve creditscore. Ook zullen wij de komende periode inzetten op het transparant maken van de ondoorzichtige processen achter geautomatiseerde besluitvorming. In toenemende mate zien wij namelijk dat burgers daar de dupe van worden, maar bijvoorbeeld niet weten hoe hun rechten uit te oefenen. Kortom, de AP stelt in haar ombudsrol grenzen aan kwalijke ontwikkelingen, geeft voorlichting aan burgers, bedrijven en organisaties en zorgt dat rechten bekend zijn en uitgeoefend worden.

Toezichthouder in de datamarkt
Om effectief te kunnen zijn, is het voor de AP essentieel om zicht te hebben op de dynamiek van de internationale datamarkt en dataeconomie. Wij zijn de hoeder van eerlijke bescherming op de vrije markt voor data in de EU. Enerzijds zien we hierbij toe op vrij verkeer van data en de dataeconomie. Anderzijds moeten we zorgen voor gelijke spelregels in heel Europa en waar nodig optreden tegen misbruik, zoals uitwassen van datahandel. We houden toezicht op de vraag of bedrijven die handelen in data zich wel aan de AVG houden. We kijken daarom naar de prikkels (*incentives*) binnen bedrijven en welke verdienmodellen de verschillende bedrijven hanteren. We brengen in kaart hoe bedrijven georganiseerd zijn: het gedrag, de cultuur en hoe de top van een bedrijf sturing geeft (*intelligence*). Ons doel is om zo tot de meest effectieve manier van beïnvloeding te komen. Anders gezegd: onze interventies zijn gericht op duurzame (gedrags)verandering. Bij de keuze voor een bepaald type beïnvloeding maken we gebruik van kennis uit de gedragswetenschappen. We werken nauw samen met de Autoriteit Consument & Markt (ACM), die vanuit haar toezichtperspectief op marktconcentraties naar de datamarkt kijkt. Ook werken we nauw samen met onze Europese collega's.

5. Interne organisatie

Good governance

De AP houdt toezicht op het gedrag en handelen van heel veel bedrijven en organisaties. Deze taak en verantwoordelijkheid vragen ook onberispelijk en onbesproken gedrag van onszelf. We passen daarom in de hele organisatie de *good governance*-principes toe in onze manier van werken.

Wij zien onze kernwaarden – open, onafhankelijk, deskundig en effectief – als kompas in ons handelen en spreken elkaar daar ook actief op aan.

Onafhankelijk
De Autoriteit Persoonsgegevens is een onafhankelijke toezichthouder zonder invloed van bedrijven en de overheid. We houden rekening met de belangen van anderen, maar behouden tegelijkertijd onze onafhankelijke positie. Altijd met een onbevooroordeelde en scherpe blik.

Open
De Autoriteit Persoonsgegevens staat in verbinding met haar omgeving. Mensen, bedrijven en organisaties weten ons te vinden met meldingen over mogelijke privacyschendingen en voor informatie over de regels en risico's. We zijn transparant waar het kan. We communiceren actief over ons werkproces en onze besluiten, stimuleren het publieke debat en geven duiding aan de regels. Toegankelijk taalgebruik en transparantie over ons handelen dragen bij aan onze effectiviteit en vergroten de legitimiteit ervan.

Deskundig
Medewerkers van de Autoriteit Persoonsgegevens weten waarover zij het hebben en ontwikkelen voortdurend mee met hun omgeving. De Autoriteit Persoonsgegevens stimuleert de ontwikkeling van individuele medewerkers en werkt eraan om een moderne toezichthouder te zijn.

Effectief
Omdat we moeten reageren op nationale én internationale ontwikkelingen, maken we weldoordachte keuzes. Per situatie kiezen we voor de meest effectieve aanpak. Met daadkracht en altijd met focus op het grondrecht van mensen.

Kritische blik van buiten

Ook als onafhankelijke toezichthouder heeft de AP baat bij een kritische blik van buiten. We borgen via externe toezichtmechanismen dat onze bedrijfshygiëne op orde blijft. Dit betekent bijvoorbeeld dat we actief participeren in externe evaluaties, zoals de vijfjaarlijkse zbo-evaluatie en internationale visitaties. Daarnaast hebben we een externe FG aangesteld die toezicht houdt op hoe de AP de AVG naleeft in de interne werkprocessen. Over vier jaar willen wij terugkijken op een gezond gefinancierde, robuust georganiseerde organisatie, die effectief, doelmatig en doeltreffend is.

Goede werkgever

De AP is als kennisorganisatie afhankelijk van de inzet van haar medewerkers. De AP wil zich de komende jaren verder ontwikkelen tot een slagvaardige toezichthouder en een werkgever waar talent graag wil komen werken, medewerkers zich kunnen ontwikkelen en veel werkgeluk ervaren binnen een cultuur van openheid en vertrouwen. Bevlogenheid en professionaliteit staan bij de AP voorop. We streven een diverse populatie na: van net van school of afgestudeerd tot meer ervaren, van jurist tot systeembeheerder, van administratief medewerker tot technoloog, van politicoloog tot psycholoog. Vanuit de gedachte dat wij geloven dat diversiteit op alle vlakken tot de beste resultaten leidt.

Samenwerking met anderen

De AP ziet het als essentieel om een goed netwerk van bondgenoten en stakeholders te onderhouden. Gegeven onze beperkte omvang is het des te belangrijker om ons netwerk te onderhouden en verder uit te bouwen. Vanuit het idee om samen slimme toezichtinterventies te realiseren en gebruik te maken van de kaders, ervaringen en kennis die er al zijn. We zetten daarom bijvoorbeeld in op het versterken van onze relaties met andere nationale, Europese en internationale toezichthouders. Belangrijke aspecten daarvan zijn het uitwisselen van informatie en expertise en het gezamenlijk oppakken van grensoverschrijdende klachten en onderzoeken naar bijvoorbeeld de grote technologiebedrijven binnen Nederland en Europa.

Ook zoeken we allianties met (maatschappelijke) organisaties en stakeholders die onze missie steunen en gezamenlijk willen optrekken. Een belangrijke plek wordt hierin ingenomen door kennisinstituten, zoals TNO, het Rathenau Instituut en universiteiten, maar ook instituten als het College van de Rechten van de Mens en de Nationale ombudsman. Door samen te werken met technologen, maatschappelijke organisaties en consumenten benutten wij bestaande kennis, expertise en perspectieven.

Onze beperkingen

Tegenover een groot toezichtveld en veelal omvangrijke financiële belangen van de bedrijven en organisaties waarop wij toezicht houden, staat een toezichthouder met een beperkte capaciteit, die zich in een ontwikkelingsfase bevindt. We werken een visie op de bedrijfsvoering uit waarin we voor alle aspecten van de bedrijfsvoering aangeven welke stappen we zetten. De uitdaging is om zodanig te opereren dat we de bescherming van persoonsgegevens zo effectief mogelijk kunnen uitvoeren.

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.