Ministerie van Economische Zaken

Licht op de digitale schaduw

Verantwoord innoveren met big data

Rapport van de expertgroep Big data en privacy aan de minister van Economische Zaken

Samenstelling expertgroep:
Jeroen van den Hoven (TBM, TUDelft), *voorzitter*
Rob Dielemans (GoDataDriven)
Jitty van Doodewaerd (DDMA)
Mireille Hildebrandt (Digital Security, Radboud Universiteit/PI.lab)
Geert-Jan Houben (Delft Data Science, TUDelft)
Ronald Leenes (TILT, University of Tilburg/PI.lab)
Rachel Marbus (NS)
David de Nood, (VNO-NCW/MKB)
Bart Schermer (eLaw@Leiden, Universiteit Leiden; Considerati)
Jeroen Terstegge (VNO-NCW/MKB; Privacy Management Partners)
Eric van Tol (Fontys Hogescholen)

Secretaris:
Marc van Lieshout (TNO/PI.lab)
mmv Somayeh Djafari (TNO/PI.lab)

Licht op de digitale schaduw

Verantwoord innoveren met big data

Rapport van de expertgroep Big data en privacy
aan de minister van Economische Zaken

Inhoudsopgave

Voorwoord

Ons gebruik van smart phones, internet en slimme apparaten die met elkaar zijn verbonden is in zeer korte tijd enorm toegenomen. We genereren inmiddels met elkaar astronomische hoeveelheden data door het continue gebruik van deze digitale technologie en door de benutting van on-line diensten.
Wij bevinden ons midden in wat gerust een Big Data *Samenleving* genoemd mag worden. Een samenleving waarin steeds meer processen mogelijk worden gemaakt en worden gevoed door analyse van zeer grote hoeveelheden data. Voorafgaand aan de digitale revolutie moesten wij moeite doen om informatie te genereren, vast te leggen en te bewaren, nu is het veeleer andersom. Nu moeten wij juist moeite doen om geen informatie te genereren, vast te leggen en te bewaren. Wij spreken zelfs als reactie op deze ontwikkeling van “een recht om vergeten te worden”.

Zowel in de publieke als in de private sector zijn door de gestage toename van data zeer veel nieuwe mogelijkheden ontstaan die ieder tot voordeel zouden kunnen strekken. Zonder overdrijving kan worden gezegd dat wij de samenleving – en ook ons zelf – beter kunnen begrijpen en bedienen aan de hand van data. Wat beweegt mensen, wat kan ze in beweging brengen? We zullen de commerciële en andere kansen die big data bieden echter niet kunnen benutten als het aan vertrouwen ontbreekt. Vertrouwen in de technologie en vertrouwen in de partijen die zich van de technologie bedienen is essentieel. Om vertrouwen een kans te geven te midden van technologische turbulentie en wirwar van informatiestromen is wetgeving onontbeerlijk die personen en hun persoonsgegevens beschermt, transparantie en rekenschap vraagt en het respect voor grondrechten van burgers garandeert.

De dataprotectiewetgeving die thans van kracht is en de nieuwe Europese Algemene Verordening Gegevensbescherming die mei 2018 van kracht wordt leggen belangrijke beperkingen op aan degenen die persoonsgegevens willen gebruiken. In de afgelopen jaren is een situatie ontstaan waarin perspectieven op wat met data mag worden gedaan steeds sterker uit elkaar zijn gaan lopen. Dit houdt het risico in zich van een onproductieve en eindeloze strijd tussen voor- en tegenstanders van strenge dataprotectiewetgeving. Sommigen menen dat we weliswaar veel kunnen, maar te weinig mogen. Anderen zijn van mening dat we te veel willen omdat het kan.

Dit rapport van een groep van privacy- en big-dataexperts richt zich tot het Nederlandse bedrijfsleven en biedt een perspectief op een vreedzame co-existentie van de begrijpelijke wens om big data te gebruiken en anderzijds de gerechtvaardigde zorg over de kwetsbaarheden van burgers en consumenten in een big-datasamenleving.

De expertgroep beveelt aan de blik te richten op verantwoorde innovatie met big data. Hierin kan Nederland een leidende rol spelen. Maatschappelijk Verantwoord Innoveren met big data houdt in dat nieuwe oplossingen worden gezocht om de voordelen van big data te benutten zonder daarbij de privacynadelen te hoeven ondergaan. Maatschappelijke, economische, technologische en ethische vooruitgang moeten gelijke tred houden. Verstoring van de balans zal leiden tot begrijpelijke zorgen, afnemend vertrouwen en gemiste kansen.

Privacy Enhancing Technologies, privacy respecting technologies, vormen een voorbeeld van een geslaagde uitweg uit de patstelling tussen privacyvoorstanders en -tegenstanders. Hoe groter de belangen zijn des te groter is onze verplichting om die uitwegen aan te leggen en begaanbaar te maken. Het rapport geeft een toegankelijk overzicht van de nieuwe dataprotectiewetgeving en van concrete voorbeelden van verantwoord innoveren in *the Age of Big Data* door het Nederlandse bedrijfsleven. De voorbeelden laten zien dat er al veel mogelijk is. De aanbevelingen beogen de oplossingen die innovatie bespoedigen en consumenten beschermen te versterken en te versnellen. Dat doet een beroep op alle spelers in het innovatiesysteem. Juist daar liggen kansen voor een land als Nederland.

Prof. dr. Jeroen van den Hoven
Voorzitter Expertgroep Big data en privacy
University Professor Ethics and Technology
Delft University of Technology

Managementsamenvatting

Bedrijven maken steeds vaker gebruik van persoonsgegevens bij hun dienstverlening. Daarmee kunnen slimme, op de persoon en situatie toegesneden diensten worden aangeboden. Veel van die diensten dragen bij aan verbetering van maatschappelijke activiteiten: veiligheid in het verkeer, verduurzaming van huishoudens, verbetering van de zorg. Daarnaast maken ze het leven van consumenten op vele terreinen makkelijker, van de aanschaf van producten tot het vinden van nieuwe partners. De persoonsgegevens zijn afkomstig van uiteenlopende bronnen. Het grootste deel bestaat inmiddels uit zogenaamde geobserveerde data, zoals locatiegegevens van een telefoon, data van cookies op een computer en klikgedrag op een website. De verwerking gebeurt steeds vaker aan de hand van slimme algoritmen die patronen uit de data afleiden en getraind kunnen worden om verbanden te vinden die anders verborgen blijven. Het is vooral dit geavanceerde en geautomatiseerde gebruik van data dat de kracht van het gebruik van big data vormt.

De verwerking van persoonsgegevens raakt aan de privacy van burgers en aan hun vertrouwen in de digitale samenleving. Dat geldt in het bijzonder voor de toepassing van big data, die voor de gebruiker ondoorgrondelijk is en onbedoelde effecten kan hebben voor individuen en specifieke groepen. Zo kunnen de gebruikte data onvolledig zijn of onjuiste accenten leggen, en kunnen er verbanden worden gelegd die er niet zijn. De burger weet zijn privacy geborgd door wetgeving die regels bevat voor een verantwoorde omgang met persoonsgegevens. De Wet Bescherming Persoonsgegevens – die invulling geeft aan de Europese Data Protectie Richtlijn – wordt vanaf 25 mei 2018 opgevolgd door de Algemene Verordening Gegevensbescherming (AVG). De AVG regelt de omgang met persoonsgegevens, en definieert de rechten van individuen en de plichten voor partijen die persoonsgegevens verwerken. De werking van de AVG is breed: zij is van toepassing op alle tot een persoon herleidbare gegevens en vormt een belangrijk uitgangspunt voor de verantwoorde omgang met persoonsgegevens.

Uit gesprekken met bedrijven die data (willen) verwerken blijkt dat onbekendheid met en onzekerheid over de toepassing en implicaties van wettelijke eisen hun parten speelt. Daarnaast worden sommige eisen als lastig en zelfs als onuitvoerbaar ervaren. Een verantwoorde verwerking van gegevens biedt alle partijen echter voordelen. Consumenten zullen eerder bereid zijn om gegevens te delen in het vertrouwen dat bedrijven zorgvuldig met hun gegevens omgaan en er mogelijkheden zijn tot controle en verantwoording. Bedrijven profiteren van het vertrouwen dat consumenten in hen stellen en kunnen daardoor datagedreven producten en diensten blijven ontwikkelen. Het maakt bovendien de bedrijfsvoering rond gegevens inzichtelijk en controleerbaar en ondervangt daarmee bepaalde risico's zoals datalekken. De wetgeving, die soms wordt ervaren als een last, kan als een prikkel fungeren om op verantwoorde wijze met persoonsgegevens om te gaan en daarin nationaal en internationaal zelfs onderscheidend te zijn.

De AVG biedt instrumenten die bedrijven daarbij ondersteunen. De dataprotectie impact assessment bijvoorbeeld, kan bedrijven helpen bij het tijdig in kaart brengen van privacyrisico's en bij het treffen van gepaste maatregelen. Het rapport geeft voorbeelden van maatregelen uit de praktijk die bedrijven als inspiratie kunnen gebruiken voor een verantwoorde omgang met persoonsgegevens. Er is een groeiend maatschappelijk belang om hierin te investeren. Dat hoeven bedrijven niet alleen te doen. Ondersteuning door andere partijen is essentieel om de beweging naar een verantwoorde omgang met persoonsgegevens te (kunnen) maken. Er is een rol voor een brede coalitie van betrokken bedrijven, branche- en koepelorganisaties, toezichthouders, consumenten, kennisinstellingen en toeleverende bedrijven. De regie ligt – zoals dat past in een complexe omgeving – niet bij één partij maar wordt gedeeld door verschillende belanghebbenden.

Inzet van de aanbevelingen is om het wettelijk kader te gebruiken als springplank naar een verantwoorde omgang met persoonsgegevens: maatschappelijk verantwoord innoveren met big data. Dit is voor bedrijven een stevige opgave, zeker in een zich zo snel ontwikkelend veld met vele partijen, vele belangen en een wettelijk kader dat uitleg en toelichting vraagt voordat de positieve werking ervan begrepen kan worden. De gesprekken die gevoerd zijn met partijen uit het veld geven weer dat bij velen de wil bestaat om de uitdaging van maatschappelijk verantwoord innoveren op te pakken. Zodoende kunnen de maatschappelijke en bedrijfsmatige voordelen die besloten liggen in big-datatoepassingen worden gerealiseerd, terwijl de maatschappelijke nadelen worden ondervangen.

1 Inleiding

De minister van Economische Zaken heeft, tezamen met de minister van Binnenlandse Zaken en Koninkrijksrelaties en de staatssecretaris van Veiligheid en Justitie, de Tweede Kamer op 19 november 2014 geïnformeerd over zijn visie op big data en privacy.[1] In deze brief kondigt de minister aan een expertgroep in te stellen. Deze expertgroep krijgt als opdracht om "*de relatie tussen big data en profilering en de bescherming van grondrechten verder te verkennen en oplossingsrichtingen uit te werken voor het verenigen van twee doeleinden: het benutten van de mogelijkheden van big data enerzijds en het behoud van het vertrouwen van de samenleving in het internet anderzijds*." In een brief van 20 juli 2015 geeft de minister aan dat hij van de expertgroep verwacht met praktisch toepasbare kennis te komen over hoe om te gaan met de wettelijke kaders op het terrein van privacy.[2]

In dit rapport presenteert de expertgroep haar bevindingen. De expertgroep heeft met diverse partijen uit verschillende maatschappelijke sectoren gesprekken gevoerd over de wisselwerking van big-dataontwikkelingen met de grondrechten, in het bijzonder privacy en het recht om niet geprofileerd te worden. De resultaten van deze gesprekken zijn gebruikt om te komen tot een analyse van de huidige ontwikkelingen, de betekenis van het wettelijke kader, een inventarisatie van de knelpunten en een overzicht van maatregelen die bedrijven en derden kunnen benutten om tot maatschappelijk verantwoorde innovatie met big data te komen.


BIG
DATA

2 Big data

Big data biedt de mogelijkheid om nieuwe verbanden te ontdekken, processen slimmer in te richten en te optimaliseren. Gerichte inzet van big data kan bijdragen aan het verbeteren van de zorg, het terugdringen van het energiegebruik en het beheersen van mobiliteit. Omdat een belangrijk deel van big-datatoepassingen uit de verzameling en verdere verwerking van persoonsgegevens bestaat krijgen veel mensen er in uiteenlopende omstandigheden mee te maken. Ook commerciële partijen maken er steeds meer gebruik van om hun diensten beter op de persoon en op de situatie af te stemmen. De persoonsgegevens zijn afkomstig van verschillende bronnen. Data worden persoonlijk verschaft (bijvoorbeeld via Facebook en online formulieren), via observatie verkregen (bijvoorbeeld via cookies of sensoren) of afgeleid uit eerder verzamelde data (bijvoorbeeld in profielen). De hoeveelheid gegevens die via observatie wordt verkregen overtreft inmiddels de hoeveelheid data die direct van individuen afkomstig is. Al deze data tezamen worden 'big data' genoemd: grote volumes aan data, die gevarieerd zijn in samenstelling en herkomst en snel kunnen veranderen.

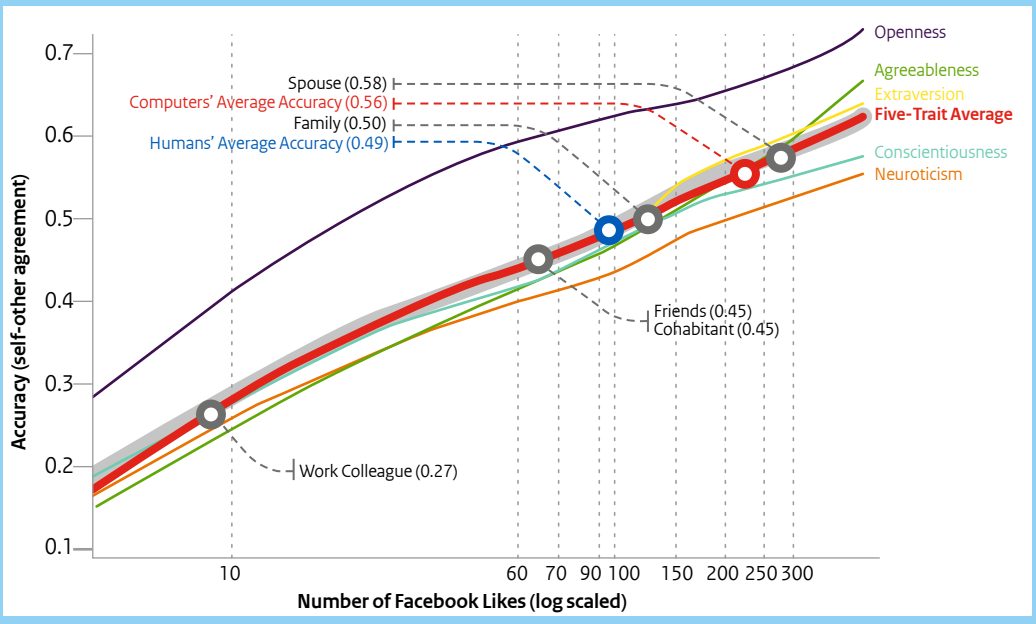
De kracht van 'big data' zit echter niet zozeer in de omvang, de variatie en de snelle doorlooptijd van data maar veeleer in de inzichten die uit deze data te halen zijn door geavanceerde (gedrags-)modellen en technieken. 'Slimme' computeralgoritmen richten zich op het clusteren van grote hoeveelheden data, waarbij het resultaat verfijnd kan worden. Ook zijn er algoritmen die 'getraind' worden door ze te voeden met grote hoeveelheden data. De inzet van kunstmatige intelligentie en systemen die patronen leren herkennen (*machine learning*) levert nieuwe inzichten over voorkeuren en gedragingen van mensen. Uit een grote hoeveelheid gegevens kunnen relevante kenmerken van groepen mensen worden gehaald en kunnen schijnbaar ongerelateerde kenmerken met elkaar in verband worden gebracht zodat nieuwe inzichten in gedragspatronen ontstaan. Zodoende kunnen mensen gericht worden benaderd met aanbevelingen en specifieke diensten waarmee ook hun keuzegedrag beïnvloed kan worden[3].

Bij de analyses van de gegevens en het ontwikkelen van toepassingen zijn bedrijven betrokken die zelf geen directe relatie met een consument hebben maar wel hun diensten aan andere bedrijven en organisaties leveren. Dit leidt binnen en tussen sectoren tot een soms ingewikkeld systeem van gegevensuitwisseling en -benutting.

Innovatieve diensten op basis van big data zijn zichtbaar in nagenoeg alle sectoren van de economie. Er is inmiddels sprake van een data-economie met een substantiële omvang.[4] Het aantal bedrijven dat zich toelegt op het verzamelen, analyseren en verder verwerken van persoonsgegevens neemt zeer snel toe.[5] Deze bedrijven kunnen zelf klein van omvang zijn maar wel enorme hoeveelheden data verzamelen, analyseren en verder verwerken.[6] Ze vormen daarmee een bouwsteen van de nieuwe data-economie. De grote spelers in deze nieuw gecreëerde economische sector zoals Google en Facebook begeven zich op vele data-intensieve gebieden. Zij kunnen vanwege de enorme hoeveelheid data die zij verzamelen, analyseren en verder verwerken snel een concurrerende positie in uiteenlopende economische sectoren verkrijgen. Zo oriënteren deze internationale datagiganten zich op nieuwe markten in de gezondheidszorg, energie en verkeer en vervoer. Daarnaast ontstaan gespecialiseerde bedrijven die zich toeleggen op aanvullende dienstverlening die gebaseerd is op persoonsgegevens. Een voorbeeld vormt de Onafhankelijke Diensten Aanbieder (ODA) die consumenten inzicht geeft in hun energieverbruik en mogelijkheden biedt tot energiebesparing. De ODA verhandelt zelf geen energie maar biedt diensten aan op basis van kennis van het energieverbruik van zijn klanten. Een ander voorbeeld vormen de zogenaamde Fintech bedrijven die consumenten nieuwe vormen van financiële dienstverlening aanbieden op basis van data en geavanceerde digitale technologie. Net als de nieuwkomers zijn de gevestigde partijen bezig met de ontwikkeling van nieuwe diensten met behulp van big data die hun portfolio verbreden en die aansluiten bij de behoeften van hun consumenten en van andere partijen in de ketens waarin zij opereren.

Kader 1: Marktimperfecties

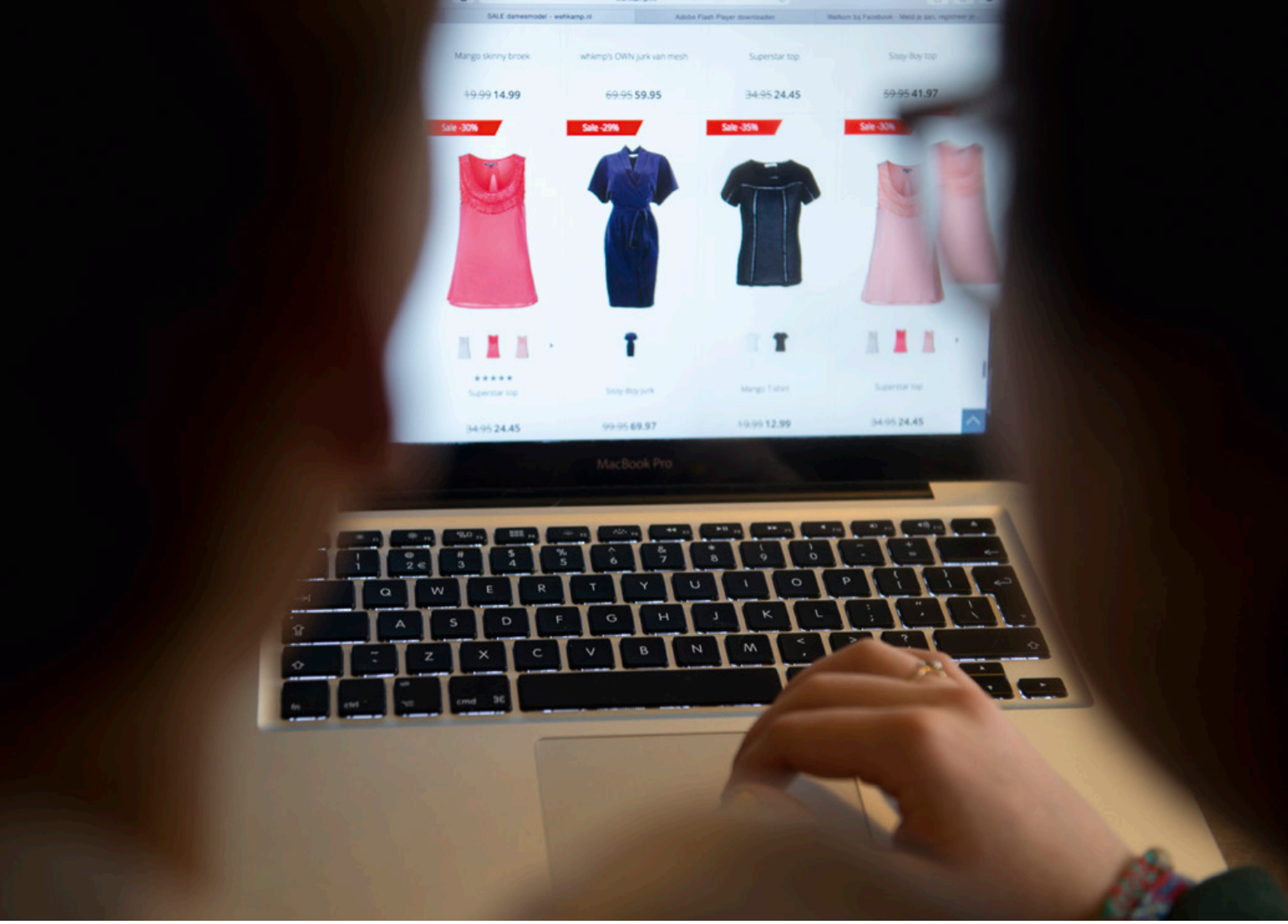
Een ontwikkeling die veelvuldig in de gesprekken naar voren kwam zijn schuivende markt-verhoudingen door toenemend datagebruik. In een recente studie analyseert de OECD de gevolgen van door data voortgebrachte innovaties (*data driven innovations*). De OECD constateert dat sprake is van een disruptieve ontwikkeling met verregaande consequenties voor marktordening en marktverhoudingen. De te verwachten productiviteitsgroei door *data driven innovations* is groot, maar vraagt om doordacht beleid om mogelijk ongewenste gevolgen het hoofd te bieden.
Die ongewenste gevolgen manifesteren zich onder meer in verschuivende verhoudingen in de markt en in het ontstaan van marktimperfecties die worden versterkt door data. Een vorm van zo'n marktimperfectie is het optreden van informatie-asymmetrie: de ene partij (in de regel de verkoper) heeft een informatievoorsprong op de andere partij (de koper) en benut dit voordeel in de diensten die ze aanbiedt. Dit effect kan optreden bij het aanbieden van diensten op basis van bewerkte en geanalyseerde data. Een andere vorm is het netwerkeffect: een eenmaal verkregen positie maakt het voor andere partijen moeilijker om op dezelfde markt actief te worden.
Een voorbeeld vormen de 'tweezijdige platformen' die kunnen leiden tot het *de facto* afsluiten van een markt. Zo is een dienst als Whatsapp interessant omdat er zoveel andere mensen mee bereikt kunnen worden. Dit netwerkeffect wordt versterkt door het gebruik van data die het platform in staat stellen zijn dienst te verbeteren. Hierdoor gaan meer mensen het gebruiken, waardoor het aantrekkelijker wordt voor weer andere mensen en voor adverteerders etc. Heeft een partij eenmaal zo'n dominante positie dan wordt het voor nieuwkomers steeds moeilijker om ook een plaats te veroveren.



Figuur 1 De voorspellende waarde van likes*: Het blijkt dat met tien `likes' al informatie over voorkeuren, houdingen en gedragingen kan worden afgeleid die in de regel de betreffende persoon beter karakteriseert dan zijn/haar collega's dat kunnen. W. Youyou, M. Kosinski and D. Stillwella 2014, p.3.*

Eenmaal verzamelde gegevens worden in andere domeinen hergebruikt, verrijkt met andere data en opnieuw onderworpen aan analyse. Daardoor ontstaat een fundamenteel andere ordening van bedrijfsmatige activiteiten. Betrekkelijk geringe hoeveelheden persoonsgegevens geven – op basis van het gebruik van gedetailleerde gedragsmodellen – inzicht in voorkeuren, houdingen en gedragingen van consumenten en kunnen gebruikt worden voor (nieuwe) consumentgerichte diensten (zie figuur 1). Anderzijds ontstaan diensten die gebruik maken van (analyse van) grote hoeveelheden persoonsgegevens zonder dat de individuele personen waarop de gegevens betrekking hebben voor de dienst van belang zijn.[7] Persoonsgegevens kunnen daarnaast verrijkt worden met gegevens die uit andere bronnen zijn verkregen. Dit kunnen ook gegevens uit openbare bronnen zijn (zoals gegevens die het CBS beschikbaar stelt). Hierdoor is het voorstelbaar dat geaggregeerde gegevens die aanvankelijk niet tot een persoon te herleiden waren via de koppeling met deze andere gegevens plotseling wel tot gegevens leiden die tot een persoon herleidbaar zijn.[8] De herleiding hoeft geen onderdeel van de dienst te vormen, maar het feit dat er een gerede kans tot herleiding is kan om aanvullende maatregelen vragen.

De verkregen inzichten zijn het resultaat van geavanceerde analyses op grote hoeveelheden data. Hier ligt zoals gezegd de vernieuwende kracht van big data. De inzichten bieden een nieuw perspectief op complexe vraagstukken. De specifieke samenstelling van de data en de precieze werking van de algoritmen zijn bepalend voor de uitkomsten van de analyse. Een dataverzameling die niet *up-to-date* is of incompleet zal tot andere resultaten leiden dan een volledige en bijgewerkte verzameling. Daarnaast heeft de keuze om bepaalde categorieën data wel te verwerken en andere niet gevolgen voor de uitkomsten. Ook kunnen de gebruikte algoritmen bepaalde aspecten uit de data benadrukken en andere aspecten onderdrukken.[9] In het gebruik van de resulterende profielen uit een data-analyse is het van belang om na te gaan hoe '*fair*' de resultaten van de analyses zijn, en in welke mate er sprake is of kan zijn van bepaalde vooraf gemaakte keuzes die van invloed kunnen zijn op de uitkomst van de analyse.[10]


Mango skinny broek
whkmp's OWN jurk van mesh
Superstar top
Sissy Boy top
19.99 14.99
69.95 59.95
34.95 24.45
59.95 41.97
Sale -30%
Sale -29%
Sale -35%
Sale -30%
34.95 24.45
99.95 69.97
19.99 12.99
34.95 24.45
MacBook Pro

3 Vertrouwen en privacy

Diensten die gebaseerd zijn op de slimme analyse van gegevens die bij consumenten zijn verzameld, richten zich op consumenten die in zekere mate aan een profiel voldoen. De gegevens waar een profiel op gebaseerd is, worden met regelmaat ververst om het profiel actueel te houden. Naar gelang een bedrijf over een langere periode gegevens kan verwerken van een consument zal de voorspellende waarde van de modellen en de gegevens navenant toenemen. Daarmee kunnen bedrijven op de persoon en situatie afgestemde diensten bieden die de consument tot voordeel strekken. Daar staat tegenover dat consumenten in toenemende mate transparant worden in hun doen en laten terwijl de verzameling en verwerking van data zelf weinig transparant zijn. De genoemde kenmerken van big data maken de consument kwetsbaarder, omdat deze voor controle en begrip van zaken meer is aangewezen op de verwerkers en experts.

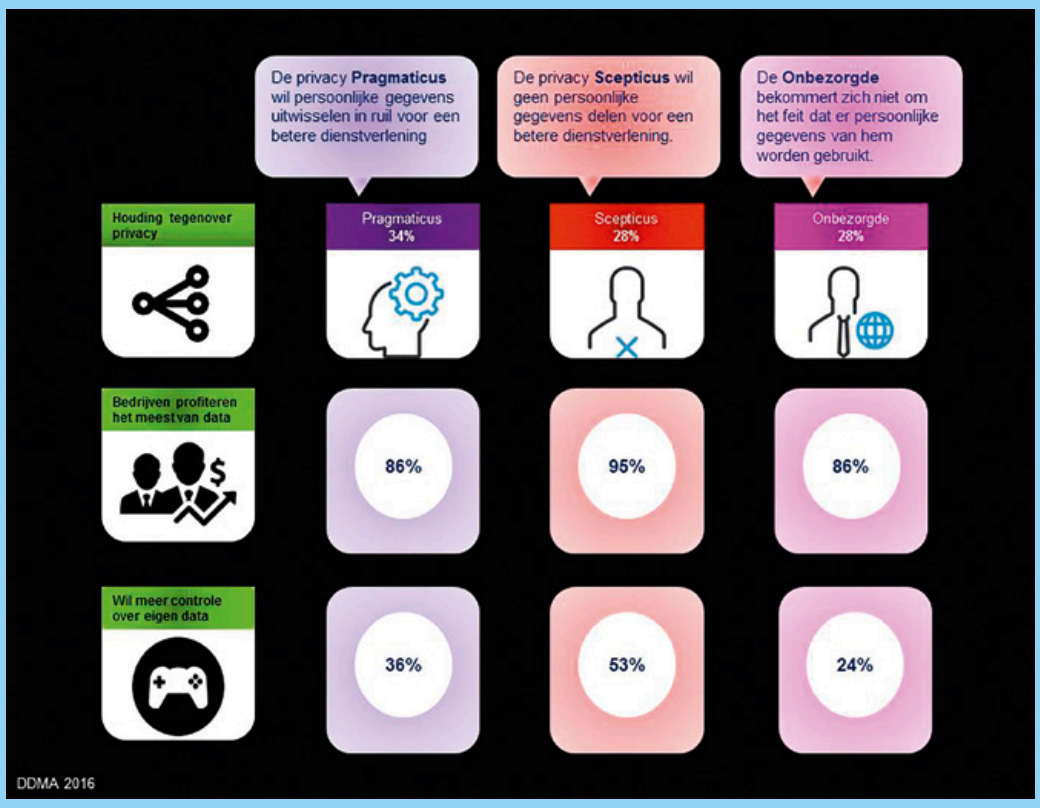
Kader 2: Vertrouwen

Onderzoek naar het vertrouwen van consumenten levert inzicht in wat zij belangrijk vinden bij een dienst en een dienstverlener (zie figuur 2). Ten eerste hechten consumenten belang aan de mogelijkheid om te controleren wie wat met hun gegevens doet. Ten tweede hebben consumenten soms een beperkt vertrouwen in een dienst (vooral bij social media) maar voelen ze zich min of meer gedwongen om deze diensten te gebruiken ('peer pressure'). Ten derde ondernemen consumenten zelf beschermende acties maar vinden ze het moeilijk de effectiviteit daarvan in te schatten. Tot slot is een deel van de consumenten onaangenaam getroffen als bedrijven geld verdienen aan gegevens die zij voor hun gevoel gratis verstrekt hebben.

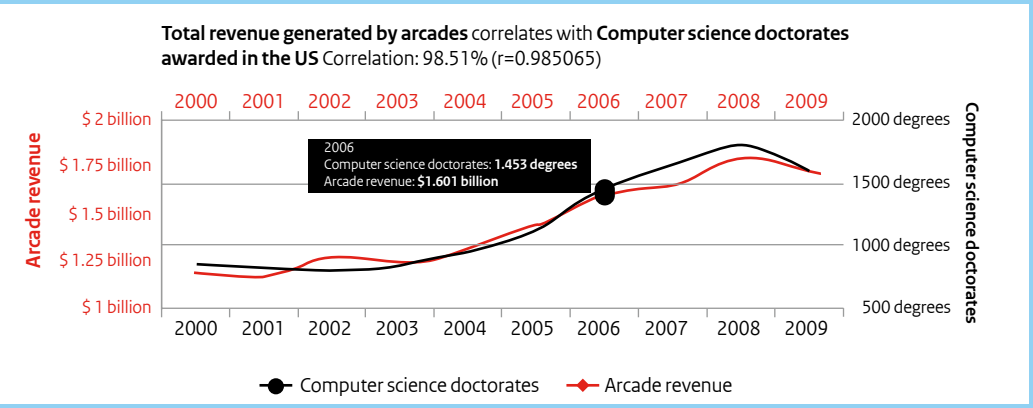
Een recente studie concludeert dat het overgrote deel van de consumenten (89%) vindt dat het bedrijfsleven het meest profiteert van de data-economie. Slechts 3% van de respondenten vindt dat het voordeel bij de consumenten ligt. Dat neemt niet weg dat twee-derde deel van de respondenten vindt dat het delen van persoonsgegevens bij de huidige tijd past, terwijl de helft begrijpt dat hun gegevens nodig zijn voor de levering van persoonsgebonden diensten. Meer dan de helft begrijpt dat hun surfgedrag wordt geanalyseerd en gebruikt voor toekomstige dienstverlening. Transparantie (over de motieven achter het gebruik van persoonsgegevens), context (welke gegevens worden in welke situatie gevraagd) en een veilige omgang met gegevens kunnen volgens het onderzoek *deal breakers* zijn voor de bereidheid om data te delen.

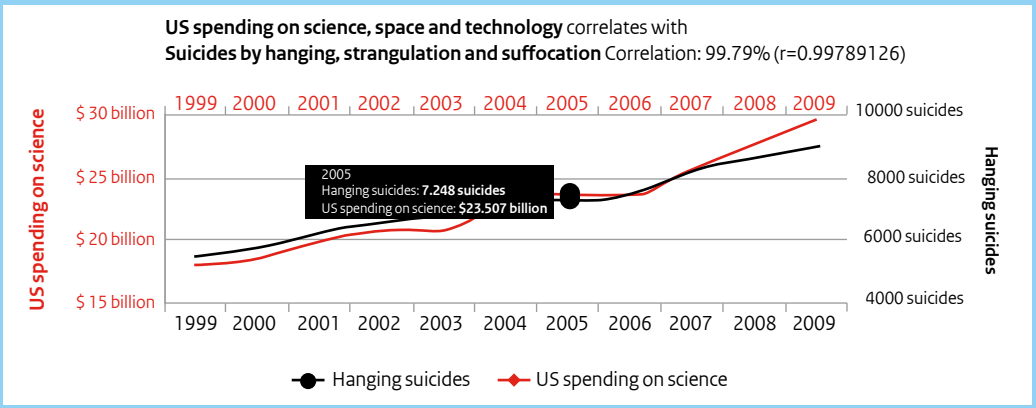
Bron: TNO 2015; DDMA 2016

Zo kan het zijn dat een consument op basis van de uitkomsten van de data-analyse bepaalde producten of diensten niet of tegen andere voorwaarden aangeboden krijgen. Ook is het mogelijk dat de uitkomst van de analyse niet klopt, omdat een statistisch verband niet noodzakelijk op een oorzakelijk verband wijst (figuur 3).[11] Voorts kunnen consumenten op basis van bepaalde kenmerken worden ingedeeld bij een groep, terwijl ze op basis van andere kenmerken weinig van doen hebben met deze groep. Consumenten kunnen in deze situaties uitgesloten worden zonder dat ze hiervan op de hoogte zijn, ze kunnen zich ergeren aan een aangeboden dienst, of erger, zich aangetast voelen in hun waardigheid omdat ze blijkbaar in een bepaald hokje zijn geplaatst. Dat kan ook het geval zijn bij een aanbod dat passend is, maar dat de consument onaangenaam verrast, bijvoorbeeld omdat het is gebaseerd op zeer persoonlijke of intieme details. De consumenten ervaren een dergelijk aanbod of handelswijze dan als een inbreuk op hun privacy.[12] Er kan ook sprake zijn van situaties waarin consumenten materieel of immaterieel geschaad, onrechtmatig behandeld (gediscrimineerd, gemanipuleerd, geëxploiteerd), of oneerlijk bejegend worden.[13] Door het groeiende gebruik van persoonsgegevens bij dienstverlening zal het in de toekomst vaker voorkomen dat mensen zich afvragen hoe een aanbieder weet heeft van bepaalde details en hoe deze gebruikt zijn om tot een bepaald dienstenaanbod te komen of beslissingen te nemen.



Figuur 2 *Vertrouwen van consumenten in bedrijven en diensten; DDMA 2016.*





Figuur 3 *Twee voorbeelden van een correlatie tussen twee variabelen die geen zinvol inzicht oplevert. http://www.tylervigen.com/spurious-correlations.*

Bedrijven kunnen investeren in het vergroten van vertrouwen van consumenten in hun diensten en in hun aanpak. Dit vertrouwen betreft twee aspecten: (i) het bedrijf handelt competent en naar de verwachtingen van de consumenten (*confidence*) en (ii) het bedrijf heeft niet alleen oog voor het eigen belang maar ook voor de belangen van consumenten, derde partijen en de samenleving (*trust*). In dit laatste geval gaat het niet alleen om wat het bedrijf doet, maar ook om de motivatie en de intentie van deze partij. Daarmee kan bepaald worden of het bedrijf morgen ook nog zal doen wat het gisteren beloofde en wat het vandaag daadwerkelijk deed. Het is belangrijk beide aspecten van vertrouwen van elkaar te onderscheiden. Een bedrijf kan investeren in het creëren van *confidence* door afspraken na te komen, aan te geven wat de consument kan verwachten, en te zorgen voor een competente uitvoering en vlekkeloze functionaliteit. Consumenten verwachten echter ook steeds meer duidelijkheid over de achterliggende intenties en basiswaarden van een bedrijf. Dit geldt ook voor de wijze waarop een bedrijf omgaat met het hem toevertrouwde 'sociale kapitaal', de persoonsgegevens van consumenten. De aantoonbaar verantwoorde omgang met persoonsgegevens kan het vertrouwen van consumenten vergroten.[14]

Met de omvangrijke nieuwe mogelijkheden voor diensten waarbij persoonsgegevens een rol spelen komt dus ook een bijzondere verantwoordelijkheid voor de zorgvuldige omgang met deze gegevens mee. Bedrijven moeten zich aan het vigerende databeschermingsrecht houden, maar kunnen zich hierbij bovendien positief onderscheiden: door de privacy van consumenten te respecteren investeren zij in een duurzame relatie met de consument. Passende waarborgen ter bescherming van de privacy dienen daarmee meerdere doelen. Ze zorgen voor een tweezijdige relatie tussen consumenten en bedrijven waarbij het delen van persoonlijke data meerwaarde voor de consumenten heeft en bedrijven meerwaarde realiseren. De verantwoorde omgang met deze gegevens wordt dan een essentiële factor om de positieve aspecten van deze relatie te waarborgen.[15] Waarborgen voor die verantwoorde omgang zijn voor een belangrijk deel vastgelegd in een wettelijk kader.


IVSTITIA IN TOTO VIR

4 Het wettelijk kader

4.1 De Algemene Verordening Gegevensbescherming

De Algemene Verordening Gegevensbescherming (AVG)[16] is in april 2016 door het Europese Parlement en de Raad aangenomen en is vanaf 25 mei 2018 van kracht. Deze verordening is de opvolger van de Dataprotectierichtlijn[17] die in Nederland is geïmplementeerd in de Wet bescherming persoonsgegevens (Wbp). Eén van de doelen van de AVG is de verdere harmonisatie van de bescherming van personen in de EU bij de verwerking van persoonsgegevens. De AVG beoogt het vrije verkeer van deze gegevens te bevorderen en daarmee innovatie en dienstverlening, tegen een adequaat beschermingsniveau. De AVG heeft het karakter van een verordening waardoor deze rechtstreekse werking in de lidstaten heeft en bestaande nationale privacywetgeving grotendeels zal vervangen. Wel is er enige ruimte voor een nationale benadering, bijvoorbeeld waar het gaat om aanvullende sectorale wetgeving. Figuur 4 geeft een uitleg van de AVG op hoofdlijnen.

Binnen de AVG heeft de verwerking van persoonsgegevens betrekking op alle handelingen die met persoonsgegevens uitgevoerd kunnen worden, zoals verzamelen, opvragen, verspreiden, combineren, opslaan, verwijderen en vernietigen. Het begrip persoonsgegeven moet breed geïnterpreteerd worden. Het gaat niet alleen om direct identificerende gegevens maar ook om indirect identificerende gegevens.[18] Ook als direct identificerende gegevens vervangen worden door een pseudoniem is volgens de AVG nog steeds sprake van persoonsgegevens indien herleiding mogelijk is.[19]

Het wettelijk kader beoogt onder meer om voorspelbaarheid en transparantie rond het verkeer van persoonsgegevens te bieden. Voorspelbaarheid is gerelateerd aan redelijke verwachtingen die consumenten mogen hebben met betrekking tot de verwerking van hun gegevens. Er moet bijvoorbeeld een doel worden vastgesteld voordat met de verwerking van gegevens wordt begonnen en een rechtmatige grondslag om de gegevens te verwerken (zie kader 3). Transparantie stelt consumenten in staat zicht te krijgen op wat er, onder welke omstandigheden, met hun gegevens gebeurt. Dit biedt mogelijkheden aan consumenten om zich te weer te stellen tegen onzorgvuldig of onrechtmatig gedrag van bedrijven. Tegelijkertijd draagt het wettelijk kader bedrijven op om te investeren in de verantwoorde omgang met gegevens door hun bepaalde verplichtingen op te leggen en daar ook sanctionering tegenover te stellen (zie kader 4 en 5 voor rechten van het individu en plichten van de verwerkingsverantwoordelijke).

Ten opzichte van de huidige Dataprotectierichtlijn ziet de AVG nog iets strenger toe op de activiteiten die bedrijven met persoonsgegevens uitvoeren in relatie tot personen binnen de EU. De toepasbaarheid van de AVG geldt nu ook indien het betrokken bedrijf zelf geen vestiging en middelen in de EU heeft maar wel gegevens verwerkt van personen binnen de EU. Dit geldt expliciet indien sprake is van het monitoren van het gedrag van betrokkenen voor zover zich dat binnen de EU afspeelt.

Figuur 4 *Europese gegevensbescherming in het digitale tijdperk. Raad van Europa, 2016.*

4.2 Spanning tussen de AVG en big data

Een verantwoorde omgang met persoonsgegevens in algemene zin is een noodzakelijke voorwaarde voor een verantwoorde benadering van big-datatoepassingen waar gebruik wordt gemaakt van persoonsgegevens. Daarbovenop heeft de AVG aandacht voor de risico's die verbonden zijn met de verwerking van persoonsgegevens in big-datatoepassingen.

Met het publiceren van de wet is nog niet alles in detail geregeld. Uit de gesprekken met partijen uit het veld blijkt dat partijen het belang van duidelijke regels voor de omgang met persoonsgegevens onderschrijven en hiernaar zullen handelen. Bedrijven ervaren echter onzekerheid in wat wel is toegestaan en wat niet, bijvoorbeeld doordat technologische ontwikkelingen nieuwe vragen over oude interpretaties oproepen. Veel bedrijven hebben behoefte aan ondersteuning en duiding op het gebied van de verantwoorde omgang met persoonsgegevens, zowel algemeen als voor big-datatoepassingen.

In sommige gevallen is er duidelijk spanning tussen de praktijk en wat de wet voorschrijft. Dat is niet te vermijden in een veld dat zo snel in ontwikkeling is als het veld rond big data.

Een probleem dat geregeld in de gesprekken met bedrijven naar voren is gekomen, is het vereiste om bij verwerking van gegevens helder te zijn over het doel waartoe de verwerking dient. Het blijkt met name moeilijk om doelen helder te omschrijven in de fase van hergebruik van al dan niet geaggregeerde en verrijkte gegevens. Het datasysteem dat achter een big-datadienst zit is complex, en omvat een veelheid van spelers die op verschillende manieren gegevens verzamelen en verwerken. Ieder van deze spelers en ieder van de verwerkingen is onderhevig aan het wettelijk kader. Maar de tot op zekere hoogte onbepaalde dynamiek, de enorme hoeveelheid van gegevens die verzameld wordt, de hoge omloopsnelheid van deze gegevens en de verzameling van gegevens uit meer bronnen leidt ertoe dat partijen de verplichting van doelbinding, en daaraan gerelateerd de rechtmatige grondslag in de praktijk als lastig of zelfs als onuitvoerbaar ervaren.

Daar staat tegenover dat een zinvolle data-analyse vooronderstelt dat is nagedacht over wat men met de analyse beoogt. Een mogelijk doel kan bijvoorbeeld zijn het verkennen van relevante patronen in de data, waarmee toegevoegde waarde kan worden gecreëerd. Het is zaak dat – steeds wanneer dat het geval is – dit doel als zodanig wordt gespecificeerd.

Gegevens kunnen steeds vaker voor meer doeleinden benut worden. Van belang is dan de vraag of de verschillende doeleinden verenigbaar zijn of niet. Indien dit het geval is dan is een nieuwe grondslag voor de gegevensverwerking niet nodig. Indien de doeleinden niet verenigbaar zijn, dan mag niet worden verwerkt op basis van de oude grondslag maar dient een nieuwe grondslag voor de verwerking te worden aangegeven. Doelbinding ondersteunt daarmee het proces van data selecteren ("Select before you collect"), beveiligen, analyseren, testen en vernietigen. Indien een nieuwe grondslag nodig is en de oorspronkelijke grondslag toestemming betrof, kan opnieuw om toestemming worden gevraagd. Het is zaak dat hiertoe goede interfaces worden gebouwd die consumenten toestaan om snel en goed geïnformeerd toestemming te geven voor het nieuwe doel.

Een andere grondslag om hergebruik van gegevens op te baseren, is het gerechtvaardigd belang. Dit vraagt een specifieke afweging ten aanzien van de rechten en vrijheden van de consument. Bij de beoordeling van de vraag of het nieuwe doel in dat geval verenigbaar is met het oorspronkelijke moet de verwerkingsverantwoordelijke in ieder geval de volgende factoren betrekken: het verband tussen het oorspronkelijke en het nieuwe doel, het kader van de oorspronkelijke verzameling (met name de verhouding tussen de verwerkingsverantwoordelijke en de betrokkene), de aard van de persoonsgegevens (bijzondere categorieën of niet), de mogelijke gevolgen van de verwerking en het bestaan van passende waarborgen (waaronder versleuteling en pseudonimisering).[30]

Kader 3: Voorwaarden voor rechtmatige verwerking

De AVG hanteert dezelfde uitgangspunten voor de verwerking van persoonsgegevens als de Dataprotectierichtlijn. Zo stelt de AVG dat er een doel moet zijn vastgesteld wanneer met de verwerking van gegevens wordt begonnen. Het doel zelf moet "welbepaald, uitdrukkelijk omschreven en gerechtvaardigd" zijn. Verzamelde gegevens mogen dan gebruikt worden voor het realiseren van dat doel, en voor doeleinden die verenigbaar zijn met dat oorspronkelijk doel.

Behalve een doel heeft de verantwoordelijke een rechtmatige grondslag nodig om de gegevens te verwerken. Die grondslag kan zijn de toestemming van de betrokkene (voor de verwerking van zijn/haar gegevens voor een of meer specifieke doeleinden). Die toestemming moet vrijelijk, specifiek, geïnformeerd en ondubbelzinnig zijn. Een individu kan toestemming altijd weer intrekken en moet dit intrekken op net zo'n eenvoudige manier kunnen doen als de manier waarop de toestemming gegeven is. De verantwoordelijke kan zich ook beroepen op een van de vijf andere grondslagen. Daarvan zijn er in de regel drie voor bedrijven van belang: verwerking van de gegevens is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, verwerking is noodzakelijk in verband met een wettelijk voorschrift, of verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verantwoordelijke of van een derde. In dit laatste geval moeten de belangen van de verantwoordelijke opwegen tegen de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zoals de AVG stelt.[20] Doel en grondslag hangen samen.[21] De grondslag is rechtmatig in het licht van het gestelde doel.

De AVG ruimt een speciale plaats in voor bijzondere categorieën van persoonsgegevens.[22]
De verwerking van deze gegevens is verboden tenzij een bepaalde uitzonderingsgrond aanwezig is. Twee daarvan zijn voor bedrijven van belang: de betrokkene heeft zelf uitdrukkelijk toestemming gegeven voor de verwerking en/of de verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt. Voor de eerste uitzonderingsgrond betekent dit dat de toestemming schriftelijk moet zijn verkregen. Voor de tweede uitzonderingsgrond zal de wetgever nader moeten aangeven wat hij onder "kennelijk" verstaat.

Belangrijke algemene voorwaarden betreffende de verwerking van gegevens zijn de eis van noodzakelijkheid, proportionaliteit en subsidiariteit. Het eerste verwijst naar de noodzaak voor de gegevensverwerking; het te realiseren doel kan slechts door het verwerken van gegevens worden gerealiseerd. De hoeveelheid gegevens die daarbij verwerkt wordt moet in overeenstemming zijn met het doel (proportionaliteit). Daarbij moet gekozen worden voor de lichtste vorm van verwerking denkbaar, dat wil zeggen die vorm die de minste impact op de betrokkenen heeft (subsidiariteit). Worden er persoonsgegevens verzameld dan moet de verwerker streven naar een minimum van te verzamelen gegevens (niet meer dan strikt noodzakelijk; dataminimalisatie).

Tot slot biedt de AVG een uitzonderingsgrond voor historisch, wetenschappelijk en statistisch onderzoek. In die gevallen (het gaat dan om hergebruik van gegevens) stelt de AVG dat verdere verwerking niet als onverenigbaar met de oorspronkelijke doeleinden wordt beschouwd. Wel moet de verantwoordelijke technische en organisatorische maatregelen treffen die garanderen dat sprake is van minimale gegevensverwerking en de verwerking zodanig inrichten dat waar dit mogelijk is geen gebruik wordt gemaakt van identificerende gegevens.[23]

Het kan ook voorkomen dat de verwerker wel een vermoeden heeft dat een bepaalde dienst interessant is maar dit nog onvoldoende onderbouwd weet om de dienst al op de markt te brengen. Dan is het mogelijk wenselijk om eerst in een besloten omgeving te kunnen testen wat de waarde van een aanpak is, welke (combinatie van) gegevens daarvoor noodzakelijk zijn, welke doelgroepen onder welke omstandigheden interessant zijn, etc. Een dergelijke vorm van testen is niet mogelijk zonder dat het gebruik van de gegevens een rechtmatige grondslag heeft, in het licht van een specifiek doel.
In hoofdstuk 7 volgt een aanbeveling voor een 'experimenteerruimte' (*regulatory sandbox*) die bedrijven de mogelijkheid biedt de zinvolheid van bepaalde diensten te verkennen in samenspraak met de toezichthouder. Het doel van de verwerking is dan het detecteren van toegevoegde waarde in de data, waarbij dit afhankelijk van de specifieke verwerkingsverantwoordelijke nader kan worden toegespitst.[31]

Een volgend onderwerp dat gerelateerd is aan big-datatoepassingen betreft de voorwaarden die de AVG aan geautomatiseerde verwerking van gegevens, inclusief profilering, stelt. Een individu heeft het recht om niet onderworpen te zijn aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waar rechtsgevolgen aan verbonden zijn of dat de betrokkene in aanmerkelijke mate treft.[32] Met deze benadering omvat de AVG de ontwikkelingen zoals die momenteel plaatsvinden rond kunstmatige intelligentie en zelflerende systemen. Een individu moet kunnen weten dat sprake is van een dergelijk besluit. Een bedrijf moet in staat zijn het besluit toe te lichten, en heeft de plicht om passende wiskundige en statistische procedures te hanteren en maatregelen te nemen die het risico op fouten en ondeugdelijke interpretaties minimaliseren.[33] De wijze waarop een individu getroffen kan worden, hebben we eerder aangegeven. De AVG stelt dat dit ieder aanzienlijk economisch of maatschappelijk nadeel voor de betrokkene betreft.[34] Bij de geautomatiseerde verwerking van gegevens kan zich het probleem voordoen dat de werking van algoritmen die bij de analyse en verdere verwerking van de gegevens gebruikt worden, niet afdoende kunnen worden doorgrond om de resultaten van de analyses eenduidig te begrijpen en te verklaren. Het is dan de vraag in hoeverre ze kunnen voldoen aan de vereiste in de Verordening om betrokkenen inzicht te geven in de 'logica van de gegevensverwerking'.[35] Voldoen aan de wettelijke kaders impliceert dat profieltransparantie[36] een serieuze rol dient te spelen in de ontwikkeling van analysemethoden en -technieken. Dit is temeer van belang omdat profielen het resultaat zijn van – impliciete en expliciete – normatieve keuzen in zowel de gebruikte dataverzameling als in de algoritmen die de profielen genereren. In hoofdstuk 7 zullen wij omtrent deze problematiek een aanbeveling doen. Deze aanbeveling is gebaseerd op de conclusie dat op dit moment onvoldoende kennis bestaat over de mate waarin de ontwikkelingen rond deze zelf-lerende systemen en andere vormen van kunstmatige intelligentie leiden tot ongewilde vormen van discriminatie, stigmatisering, uitsluiting en onheuse behandeling, naast doeltreffende en gewenste bijdragen aan het oplossen van maatschappelijke vraagstukken (zoals duurzaamheid en veiligheid).

Kader 4: Rechten van betrokkenen

Betrokkenen hebben verschillende rechten. Veel van die rechten zijn overgenomen van de Dataprotectierichtlijn. Dit geldt voor het recht van inzage, het recht op rectificatie, het recht op beperking van de verwerking, en het recht van verzet.[24] De rechten stellen betrokkenen in staat om te weten wat er met hun gegevens gebeurt, deze te corrigeren of zich tegen de verzameling te verzetten als zij die onnodig vinden (en andere belangen zich daar niet dusdanig tegen verzetten dat ze zwaarder wegen dan de geboden rechten). Nieuwe rechten die de AVG introduceert zijn het recht om een elektronische kopie van de eigen persoonsgegevens te ontvangen, het recht op vergetelheid en het recht om gegevens van de ene dienstverlener naar de andere mee te nemen (dataportabiliteit).[25] Deze rechten zijn gebonden aan een aantal voorwaarden.[26]

Kader 5: Plichten

De plichten voor de verwerkingsverantwoordelijke bestaan om de rechten van de betrokkenen mogelijk te maken en om zorg te dragen voor een goede borging van de persoonsgegevens die de verantwoordelijke verzamelt en verder verwerkt. Deze plichten zijn grotendeels gelijk aan de plichten die in de Dataprotectierichtlijn opgenomen waren. Nieuwe instrumenten zijn de plicht om aan te tonen dat passende maatregelen zijn getroffen voor de bescherming van de persoonsgegevens, de plicht om te streven naar gegevensbescherming door ontwerp en door standaardinstellingen (*Data protection by design* en *by default*).[27] Daarnaast wordt de gegevensbeschermingseffectbeoordeling (*Data protection impact assessment*) ingevoerd.[28] Deze verplicht de verwerkingsverantwoordelijke om, bij een hoog risico voor de rechten en vrijheden van het individu, voorafgaand aan de verwerking de risico's van deze verwerking in kaart te brengen en aan te geven welke maatregelen getroffen worden om de gesignaleerde risico's te ondervangen.

Andere instrumenten die de AVG benoemt zijn de functionaris voor de gegevensbescherming (*Data protection officer*), de gedragscode en certificeringsmechanismen. Deze instrumenten zijn niet nieuw maar worden in de AVG nadrukkelijker naar voren geschoven als instrumenten die door bedrijven zelf ingezet kunnen worden om aantoonbaar te werken aan een verantwoorde omgang met persoonsgegevens. De aanwijzing van een functionaris voor de gegevensbescherming wordt daarbij in sommige situaties verplicht gesteld.

Mocht een verwerkingsverantwoordelijke niet aan zijn plichten voldoen dan bestaat de mogelijkheid van sanctionering. De hoogte van de mogelijk op te leggen boetes is fors verhoogd ten opzichte van de Dataprotectierichtlijn: administratieve boetes kunnen oplopen tot 20 miljoen Euro of, voor een onderneming, tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.[29]

4.3 Overige wettelijke kaders die van belang zijn voor big data

De AVG is niet het enige wettelijke kader waar bedrijven rekening mee moeten houden. Zo is de ePrivacyrichtlijn (in Nederland uitgewerkt in de Telecommunicatiewet) een belangrijk tweede kader dat aanvullende eisen aan aanbieders van elektronische communicatienetwerken en -diensten stelt. Een relevant element voor de verzameling van persoonsgegevens betreft de geëiste transparantie indien informatie op de computer van een betrokkene wordt geplaatst of eruit wordt gelezen, en de vrijheid van een betrokkene om zich hier tegen te verzetten (de zogenaamde cookiebepaling).[37] De Wet Handhaving Consumentenbescherming stelt regels om onterechte behandeling van consumenten tegen te gaan. Sectorspecifieke wetten en regels kunnen eveneens van toepassing zijn.[38] De manier waarop bedrijven die werken met persoonsgegevens invulling geven aan de voorwaarden die de wettelijke kaders stellen, zal van bedrijf tot bedrijf verschillen en afhangen van de diensten die een bedrijf aanbiedt, de omgeving waarin het opereert, de omvang van de activiteiten waarmee persoonsgegevens gemoeid zijn, de samenhang met activiteiten van andere bedrijven, etc. Er is geen 'one size fits all' benadering. Sommige bedrijven opereren in redelijk vrije markten, andere bedrijven hebben te maken met streng gereguleerde sectoren (de energiesector, de financiële sector). Daarnaast zijn er bedrijven die zich uitsluitend richten op de verdere verwerking van (persoons-)gegevens en hieromtrent diensten aan andere bedrijven aanbieden. Zij opereren naast bedrijven voor wie persoonsgegevens een onderdeel vormen van de dienstverlening en producten die ze bieden.

De druk om nieuwe manieren van werken te ontwikkelen, tot nieuwe inzichten te komen door het maken van analyses en nieuwe diensten te ontwikkelen die profijtelijk voor de onderneming kunnen zijn, is groot. De trend tot personalisering en profilering die we beschreven hebben, is gebaseerd op het gebruik van persoonsgegevens. Daarmee hebben bedrijven met de AVG te maken, en vanwege de cookiebepaling vaak ook met de ePrivacyrichtlijn, ongeacht de grootte en het soort dienstverlening van de bedrijven.

5 Maatschappelijk verantwoord innoveren

De big-datarevolutie betekent een groeiende hoeveelheid toepassingen van geavanceerde statistische technieken en modellen in combinatie met zelflerende en andere op kunstmatige intelligentie gebaseerde systemen. De verwerking van grote hoeveelheden zeer gedetailleerde informatie en gedragsmodellen over de consumenten leidt tot nieuwe vormen van dienstverlening die een zeer persoonlijk karakter kan krijgen. Gerechtvaardigd vertrouwen van consumenten in de goede bedoelingen en motieven van bedrijven (*trust*) is door die ervaren nabijheid van de dienstverlening een essentiële factor om deze diensten breed ingang te laten vinden. Daarbij zijn goede bedoelingen alleen niet voldoende, en gaat het uiteindelijk niet alleen om vertrouwen maar ook om betrouwbaarheid. Een goede organisatie van de bescherming van persoonsgegevens, zowel in technische als in organisatorische zin, biedt een goed uitgangspunt om de complexere vragen rond de zorgvuldigheid van gegevensverwerking in big-datatoepassingen te adresseren en een basis voor vertrouwen te leggen.

Dezelfde big-datarevolutie maakt dat dit geen gemakkelijke opgave is. Bedrijven ervaren soms spanning met de opgelegde eisen rond de omgang met persoonsgegevens, zoals die in hoofdstuk 4 zijn aangegeven. Die spanning komt voort uit snelle ontwikkelingen in de informatietechnologie en de *data science* waardoor het een grote opgave is het overzicht te bewaren en inzicht te houden in de bewerking en het gebruik van (big) data. Dit geldt evenzeer voor de verhouding met het wettelijke kader. Het is dus een constante uitdaging voor bedrijven om te overzien aan welke wettelijke bepalingen moet worden voldaan en hoe dat moet worden gedaan, terwijl men tegelijkertijd kansrijke nieuwe initiatieven probeert te ontplooien.

De bedrijvigheid rond data en persoonsgegevens bevindt zich in een ander stadium van ontwikkeling dan andere domeinen en sectoren in de samenleving. In de burgerluchtvaart, de farmacie, voedselindustrie wordt verwacht dat bedrijven transparant zijn in hun handelswijze. Het idee van lange ketens en *supply chains* en de bijbehorende ketenaansprakelijkheden wordt gemeengoed. Hierdoor kan een consument bijvoorbeeld achterhalen welke materialen zijn gebruikt voor de fabricage van een product en nagaan of een product onder verantwoorde omstandigheden is geproduceerd. Is de dienst of het product veilig, duurzaam, *fair-trade*, verantwoord en worden wat dat betreft geen compromissen gesloten uit puur winstbejag?

Achter het vanzelfsprekende vertrouwen dat consumenten in de regel hebben in het economisch verkeer gaat een uitgebreid netwerk van regels, wetten, normen, standaarden, keurmerken, reputatiemechanismen, toezicht, *service level agreements*, afspraken en instituties schuil dat er voor zorgt dat burgers en consumenten op goede gronden vertrouwen kunnen hebben in wat hun wordt aangeboden. Voor de data-economie is een zodanig uitgewerkt institutioneel systeem van *checks and balances* nog niet uitgekristalliseerd.
De aanwezigheid van hoogwaardige instituties die door middel van controles het gecreëerde vertrouwen waarborgen is een kwaliteitskenmerk van succesvolle samenlevingen. Het is dus ook een belangrijke dimensie van moderne hoogwaardige *digitale* samenlevingen. Het vertrouwen van de klant wordt in een samenleving die om data draait verkregen op basis van verantwoorde innovaties met big data.

Deze verantwoorde innovaties bestaan juist precies in het benutten van de nieuwe mogelijkheden van big data met in achtneming van belangrijke ethische overwegingen en juridische eisen, gevormd door het wettelijk kader.

Domein Mobiliteit

De hoeveelheid data die in en om de auto te vinden is, is gigantisch gegroeid. De auto zelf genereert steeds meer data die iets zeggen over conditie van het voertuig en de manier waarop het wordt gebruikt. Deze data kunnen vervolgens gebruikt worden voor onderhoud, veiligheid en rijprestaties. Daarnaast zijn er vele registratiesystemen rondom de auto zoals de Nationale Kenteken Registratie NKR (voorheen: Nationale AutoPas; NAP) en de APK. Het RDC Datacentrum en enkele andere soortgelijke communicatieproviders stroomlijnen de gegevensuitwisseling tussen (de leden van) RAI en BOVAG en leveren inmiddels vele honderden diensten voor de aangesloten leden. Deze datadiensten kunnen worden aangevuld met data die gegenereerd worden door andere systemen, zoals navigatiesystemen en ritregistratiesystemen. De gegenereerde informatie kan leiden tot diensten voor verkeer en vervoer zoals meldingen over files, drukte op de weg, waargenomen ongevallen, slecht wegdek en parkeervoorzieningen. Daarnaast wordt vanaf april 2018 eCall verplicht in auto's ingebouwd.
Dit systeem stuurt specifieke informatie naar de meldkamers van de hulpcentrales in geval van een ongeluk met de auto. Hoewel het eCall-systeem in beginsel een gesloten systeem is, kan de techniek worden gebruikt voor andere (commerciële) online diensten.

Maatschappelijk verantwoord innoveren met big data betekent steeds op zoek gaan naar nieuwe mogelijkheden om nieuwe diensten en producten te ontwikkelen waarin deze combinatie van *business opportunities*, technische mogelijkheden en juridische, maatschappelijke en morele eisen gestalte krijgt. Wie verantwoord innoveert met big data vindt in de geschetste moeilijkheden een uitdaging om slimme oplossingen te bedenken, waardoor 'of-of', verandert in 'en-en' en een competitief voordeel wordt gevonden.

Er komen steeds meer instrumenten beschikbaar om bedrijven hierbij te ondersteunen. In een internationaal speelveld dat kenmerkend is voor de big-datatoepassingen is de verleiding echter groot om voor korte-termijngewin te gaan en de wettelijke eisen als een norm te zien waaraan voldaan moet worden. De expertgroep meent echter dat bedrijven die maatschappelijk verantwoord innoveren en ondernemen met big-datatoepassingen de beste kaarten hebben om een blijvende vertrouwensrelatie met consumenten te ontwikkelen en te behouden.

6 Oplossingsrichtingen

6.1 Naar een professionele omgang met big data

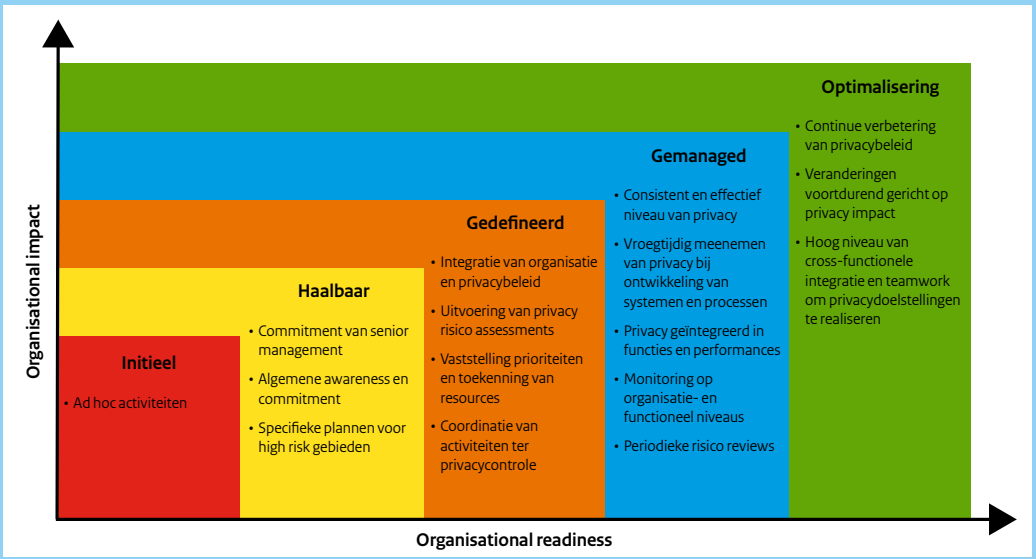
In dit hoofdstuk presenteren we een aantal praktische maatregelen voor de verantwoorde omgang met persoonsgegevens. In deze verantwoorde omgang ligt ook vaak de sleutel voor verantwoorde big-datatoepassingen besloten. Een groot deel van de maatregelen wordt genoemd in de AVG en heeft een verplichtend karakter. Bij verschillende van deze maatregelen zit enige speelruimte in de toepassing van de maatregel. Door deze speelruimte op een privacyrespecterende manier in te vullen kunnen bedrijven op een onderscheidende manier werken aan vergroting en borging van het consumentenvertrouwen. Met deze maatregelen werken bedrijven aan de verdere professionalisering van de zorg voor de privacy van klanten en een goede omgang met hun persoonsgegevens.
Een instrument dat bedrijven de mogelijkheid biedt om zichzelf 'langs een maatlat' van professionalisering te leggen is het *Privacy Maturity Model* (zie figuur 5). Een bedrijf kan daarmee zelf inschatten hoe ver het is in de professionalisering van de zorg voor privacy en zien wat nodig is om een hoger niveau te bereiken. Voldoen aan de vereisten van de AVG impliceert een volwassenheid die past bij niveau 'Gemanaged'.

De te treffen maatregelen kunnen in drie groepen worden onderverdeeld. De eerste groep betreft maatregelen die bedrijven zelf kunnen nemen in hun bedrijfsprocessen en hun dienstverlening. Dit zijn technische en organisatorische maatregelen die zich richten op een betere omgang met persoonsgegevens en op het vergroten van het bewustzijn voor de extra risico's die big-datatoepassingen met zich meebrengen. In de tweede groep bevinden zich maatregelen die bedrijfstakken, branche- en koepelorganisaties kunnen nemen om met name het bewustzijn voor de extra risico's die big-datatoepassingen met zich meebrengen te vergroten. Die maatregelen zijn gericht op het bij elkaar brengen van bedrijven om van elkaar te leren en gezamenlijk te werken aan betere oplossingen voor big data en privacy. De derde groep betreft de maatregelen die derde partijen kunnen treffen om bepaalde belemmeringen voor bedrijven weg te nemen of om het voor bedrijven makkelijker te maken om zelf de juiste maatregelen te treffen.

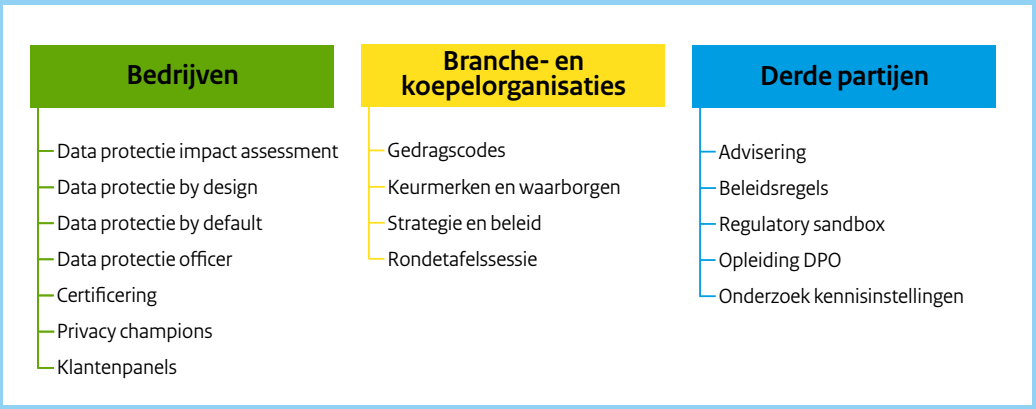
6.2 Maatregelen die bedrijven zelf kunnen treffen

De Dataprotectie Impact Assessment

Een bewuste benadering van het privacyvraagstuk begint bij een oriëntatie op de privacyrisico's van bedrijfsprocessen en geleverde diensten. Een Dataprotectie Impact Assessment (DPIA) is een instrument om risico's met betrekking tot de schending van de rechten van de betrokkenen rond de verwerking van persoonsgegevens in kaart te brengen en om gepaste maatregelen tegen die risico's te nemen (waaronder risico's van big-datatoepassingen). Een DPIA is in bepaalde omstandigheden verplicht.[39]
De ervaring leert dat een DPIA niet een eenmalig instrument is dat als een afvinklijstje 'gescoord' kan worden. Een organisatie die zich op een professionele manier rekenschap wil geven van de omgang met persoonsgegevens en de hiermee gepaard gaande risico's benut de DPIA als een instrument om dit in de organisatie te borgen (zie ook het *Privacy Maturity Model*). Tegelijkertijd constateren we dat er nog geen vaststaande en eenvoudig te gebruiken methodiek voor de DPIA beschikbaar is die in kan spelen op de verschillende situaties waarin ondernemers zich kunnen bevinden. In de aanbevelingen komen we hier op terug.



Figuur 5 *Privacy Maturity Model. http//www.theia.org – Global Technology Auditing Guide 5*



Figuur 6 *Overzicht van oplossingsrichtingen.*

Voorbeeld: Een smart grid DPIA

Inmiddels is er op Europees niveau enige ervaring met de ontwikkeling van de DPIA. De Europese energiesector is gezamenlijk aan de slag gegaan om een DPIA op te stellen voor het smart grid en de slimme meter. De Smart Grid DPIA bestaat uit een aantal templates die bedrijven kunnen gebruiken om zelf te evalueren met welke privacyrisico's ze geconfronteerd kunnen worden. Behalve een inventarisatie van de risico's geeft de aanpak ook aan hoe de DPIA organisatorisch moet worden ingericht, en welke stappen gezet moeten worden om de risico's tegemoet te treden. Wat betreft de ervaringen tot nu toe constateren de betrokken organisaties dat het geen eenvoudige zaak is om op detailniveau tot overeenstemming te komen over de aanpak van de DPIA. Er is sprake van een 'steile leercurve', maar wel één die noodzakelijk is, gegeven het belang van een goede regeling van de privacy van hun klanten.

Voorbeeld: NOREA PIA handreiking

Bedrijven hoeven niet zelf het wiel uit te vinden. Er zijn vele organisaties die hen ondersteunen bij het uitvoeren van een Data Protectie Impact Assessment. De Nederlandse Orde voor Register EDP/IT Auditors (NOREA) heeft een handreiking uitgebracht waarin beschreven wordt waar een Privacy Impact Assessment aan moet voldoen, compleet met vragenlijst aan de hand waarvan een concrete PIA kan worden uitgevoerd. De handreiking wordt van tijd tot tijd aangepast. De laatste aanpassing (november 2015) betrof de opname van de gevolgen van de Wet Meldplicht datalekken. De huidige instrumenten richten zich op de eisen van de Wbp. De verwachting is dat deze instrumenten in de komende jaren zullen evolueren tot instrumenten die de AVG als uitgangspunt hebben en beter zijn afgestemd op de analyse van risico's rond big data en privacy.

Voorbeeld: VNO-NCW/MKB quick scan voor een DPIA

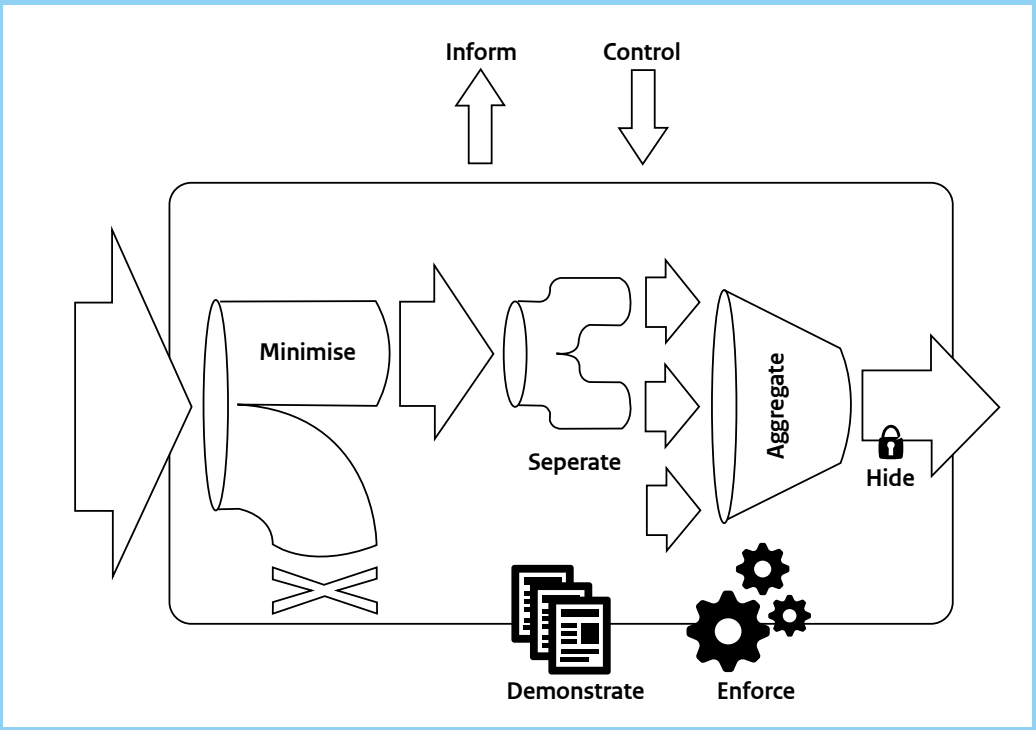
Een belangrijk en behulpzaam instrument dat in de regel onderdeel uitmaakt van een DPIA is de quick scan. Deze quick scan biedt bedrijven de mogelijkheid om snel in te schatten of een uitvoeriger assessment noodzakelijk is. De quick scan achterhaalt óf er sprake is van de verwerking van persoonsgegevens, en of er in dat geval sprake is van de verwerking van bijzondere categorieën gegevens.[40] Is dit laatste het geval dan moet het bedrijf rekening houden met strengere procedures rond de verwerking van deze gegevens. Na het uitvoeren van een quick scan heeft een bedrijf een globaal beeld van de risico's die het loopt met betrekking tot de mogelijke schending van de rechten van de betrokkenen en wat dit impliceert (bijvoorbeeld: het uitvoeren van een diepgaandere dataprotectie impact assessment). VNO-NCW/MKB is één van de partijen die een dergelijke quick scan op zijn website beschikbaar stelt.

Dataprotectie *by design* en *by default*

Ongeacht of sprake is van big-datatoepassingen hebben bedrijven de plicht om gepaste technische en organisatorische maatregelen te nemen die bijdragen aan de bescherming van de data.
Deze maatregelen worden aangeduid met de term dataprotectie *by design* en *by default*. Ook zij zijn omschreven in de AVG.[41] Data moeten adequaat beveiligd worden, bijvoorbeeld door ze versleuteld op te slaan en organisatorische maatregelen te treffen rond toegangsbeheer. Daarnaast moeten deze maatregelen bijdragen aan het beperken van de verzameling en het gebruik van gegevens tot hetgeen noodzakelijk is voor het betreffende doel (het in hoofdstuk 4 genoemde principe van dataminimalisatie).

Voorbeeld: ENISA uitwerking DP by design en by default

De uitwerking van dataprotectie by design en by default wordt door wetenschappers en privacy-experts binnen organisaties ter hand genomen. De Europese Network and Information Security Agency (ENISA) draagt in twee recente rapporten bij aan een systematisering van deze concepten. Zo wordt gewerkt aan de uitwerking van deze concepten via privacy design strategies en patterns (zie figuur 7).[42] Deze strategieën zijn behulpzaam om de door de AVG genoemde principes te ondersteunen. Ze richten zich op de technische omgang met data, zoals het minimaliseren, scheiden, aggregeren en verbergen van data. Daarnaast richten de strategieën zich op het informeren van en bieden van controlemogelijkheden aan betrokkenen en op het aantonen van naleving door verantwoordelijken/bewerkers. Voor ieder van de strategieën zijn tools beschikbaar, zonder dat op dit moment evenwel sprake is van een gestandaardiseerde aanpak.



Figuur 7 Privacy design strategieën. J-H Hoepman 2014.

Voorbeeld: ZorgTTP en pseudonimisering
De AVG noemt pseudonimisering als voorbeeld om het principe van dataminimalisatie te ondersteunen. Deze strategie om directe herleidbaarheid te voorkomen wordt inmiddels door Trusted Third Parties als dienst aangeboden. Een voorbeeld is ZorgTTP, een organisatie die zorgorganisaties ondersteunt met de afhandeling van gepseudonimiseerde (en ook geaggregeerde) zorgdata. Ook andere bedrijven bieden deze diensten aan.

Voorbeeld: Nieuwe vormen van gegevensbeveiliging
De beveiliging van data is een standaard onderdeel van dataprotectie by design en by default. Inmiddels zijn er versleutelingstechnieken voorhanden die het mogelijk maken om op de versleutelde data bewerkingen uit te voeren. Deze technieken, waaronder Homomorfe encryptie, zijn voldoende ontwikkeld om in pilots beproefd te worden maar zijn nog niet zover dat ze 'industrieel' kunnen worden ingezet.[43] Dat geldt ook voor een andere klasse van technieken, de zogenaamde Attribute Based Credentials.[44] Een derde techniek die met name voor big-datatoepassingen interessant is, is Polymorfe encryptie en pseudonimisering (PEP). Deze techniek is speciaal voor big-datatoepassingen ontwikkeld om ongewenst hergebruik zo veel mogelijk tegen te gaan.[45] Deze technieken gaan a priori uit van dataminimalisatie en leveren in specifieke omstandigheden alleen de strikt noodzakelijke gegevens.

Voorbeeld: Nieuwe dienstenontwikkeling voor big data
Bedrijven ontwikkelen ook nieuwe diensten om big-datatoepassingen te verbinden met een verantwoorde omgang van persoonsgegevens. Het Tippiq-platform en het MPARE-platform, initiatieven opgezet vanuit Alliander, zijn hier voorbeelden van. Beide initiatieven richten zich op de ontwikkeling van een tweezijdig platform dat tot doel heeft om op een verantwoorde en transparante manier nieuwe diensten in en rond het huis mogelijk te maken. Het MPARE platform geeft huishoudens controle over hun energiegegevens. Het Tippiq-platform, een R&D-initiatief van Alliander, biedt digitaal inzicht in en controle over datadeling. Diensten vragen via het platform aan bewoners toestemming voor toegang tot hun data. Bewoners bepalen vervolgens onder welke condities data gedeeld mogen worden, met wie en om welke reden.[46] Daarnaast zijn in Nederland verschillende innovatieve, in de regel kleine, bedrijven en organisaties te vinden die privacyvriendelijke aanpakken ontwikkelen en op de markt brengen. Dat gaat zowel om platforms met datakluizen als om geavanceerde vormen van versleutelde uitwisseling van minimale datasets als om geavanceerde vormen van toegangsbeheer. Hier vormt zich een potentiële markt van privacyvriendelijke oplossingen.

Aanvullende organisatorische maatregelen

Een bewuste benadering van privacy vraagt om borging van de aandacht voor privacy in een organisatie. Verschillende organisaties hebben voor dit doel Functionarissen voor de gegevensbescherming in dienst. De AVG zorgt ook op dit vlak voor een stroomlijning. De AVG spreekt van *Data Protection Officers* (DPO).[47] In bepaalde gevallen is een DPO verplicht, zoals bij grootschalige regelmatige en systematische monitoring van personen en bij de grootschalige verwerking van bijzondere gegevens. Voor andere situaties is een DPO niet verplicht maar kan aanstelling van een DPO wel bijdragen aan systematische en structurele aandacht voor privacy binnen een bedrijf. Het is niet strikt noodzakelijk om zelf een DPO aan te stellen. Het is ook mogelijk om een externe DPO in te schakelen en daarmee gebruik te maken van de opgebouwde expertise van deze DPO. De AVG benadrukt het belang van de onafhankelijke status van een DPO.[48] Daarnaast is betrokkenheid van directie/bestuur gewenst bij onderwerpen die de privacy betreffen, zeker als sprake is van grootschalige, systematische verwerking van (bijzondere) persoonsgegevens. Dat betekent dat een DPO direct rapporteert aan de directie/het bestuur.[49]
De AVG stelt dat DPO's gekwalificeerd moeten zijn voor de uitoefening van hun taak.[50] Die kwalificaties zijn in algemene zin goed te herleiden uit de AVG maar hebben nog niet tot een uniform systeem van gecertificeerde DPO's geleid. Wel zijn er verschillende opleidingsmogelijkheden tot DPO, en wordt er gewerkt aan het realisering van een schema van certificeringen dat bijdraagt aan de kwaliteitsbewaking van de kwalificaties van een DPO (zie ook 6.4).

Domein Dataconsultancy

De dataconsultancy vormt een relatief nieuwe sector van internationale economische bedrijvigheid die zich richt op het creëren van meerwaarde uit verzamelde en verwerkte data.
Deze meerwaarde wordt zichtbaar in toenemende relevantie van communicatie tussen de adverteerder en consument. Dataconsultants richten zich op de verzameling, verrijking, analyse en opslag van data en op de ondersteuning van adverteerders in hun datastrategie. Een belangrijk deel van hun werk is gericht op *real time advertising* en op mogelijkheden tot *branding* van een derde partij. Op basis van gedetailleerde profielinformatie van bezoekers van een website vindt in milliseconden een veiling plaats tussen partijen die content willen plaatsen en partijen die ruimte in de aanbieding hebben. Deze nieuwe communicatiestrategie wordt voor deze partijen uitgevoerd door gespecialiseerde bedrijven met de benodigde technische, compliancy of marketingkennis. Daarnaast spelen dataspecialisten een rol bij de ondersteuning van derde bedrijven in de data-analyse. Hoewel het effect van hun activiteiten direct op een consument kan zijn gericht (gepersonaliseerde aanbiedingen) staan ze zelf relatief ver van de consument af en handelen ze in de regel in opdracht van een klant die wel een directe relatie met een consument heeft (dan wel deze probeert op te bouwen).

Voorbeeld: Privacy champions en privacy awareness panels
De aandacht voor privacy kan bevorderd worden door de DPO te ondersteunen met personen die een speciale verantwoordelijkheid hebben voor de verantwoorde omgang met data. Ziggo heeft zogenaamde privacy champions aangesteld. Deze champions hebben geen formele accreditatie (dat zou wel kunnen). Ze zijn de aanspreekpunten van de DPO binnen de verschillende afdelingen die met klantgegevens werken. Op deze wijze vindt een verspreiding van het denken en het handelen met klantgegevens plaats. Iets soortgelijks heeft ING met de instelling van interne awareness panels, panels met personeelsleden die geraadpleegd worden over op handen zijnde dienstenontwikkelingen.

6.3 Ondersteunende maatregelen door branche- en koepelorganisaties

Gedragscodes

De AVG stelt dat gedragscodes bij kunnen dragen aan een verantwoorde omgang met data binnen organisaties.[51] De AVG biedt ruimte voor zelfregulering, bijvoorbeeld doordat competente organisaties worden opgericht die toezien op de naleving van de gedragscodes. De gedragscodes zelf dienen bij de toezichthouder ingebracht te worden die checkt of de codes voldoen aan de eisen die de AVG hieraan stelt. Vervolgens is het zaak erop toe te zien dat de gedragscode in de praktijk wordt nageleefd.

Voorbeeld: VEDEK en VMNED
Verschillende branches zijn zelf aan de slag met het opstellen van gedragscodes. Gegeven de recente aanvaarding van de AVG zijn deze codes nog niet getoetst aan de eisen van de AVG, maar in sommige gevallen wel aan de Wbp. Zo heeft de VEDEK, de brancheorganisatie voor de ODA's in de energiebranche, samen met VMNED, de Vereniging van Meetbedrijven in Nederland, een gedragscode opgesteld voor de omgang met de data uit de slimme meter. Deze gedragscode is voorgelegd aan de Autoriteit Persoonsgegevens. Deze heeft de conceptversie met enkele vragen teruggelegd. Een belangrijke voorwaarde voor de AP is dat de gedragscode door een representatief deel van de ODA's ondertekend wordt. De AP heeft in juli 2016 verklaard van plan te zijn de bijgestelde gedragscode te accepteren. Na acceptatie zullen VMNED en VEDEK werken aan de (verdere) verspreiding van de gedragscode onder hun leden, en zal eveneens gewerkt worden aan het opstellen van een gezamenlijke gedragscode met andere partijen uit de energiesector (netbeheerders en energieleveranciers).[52]

Keurmerken en waarborgen

Een gedragscode heeft een intern disciplinerende en sturende werking. Een ander instrument dat meer op consumenten is gericht is het keurmerk of de waarborg. Deze borgt kwaliteit, ondervangt bepaalde zorgen bij de consumenten, creëert mogelijkheden voor beroep en draagt op deze wijze bij aan de 'accountability' van een bedrijf.

Voorbeeld: DDMA
Zo biedt DDMA, de brancheorganisatie voor marketingactiviteiten, een Privacy Waarborg aan. Bedrijven die deze waarborg onderschrijven, verplichten zich tot een verantwoorde omgang met persoonsgegevens. De door DDMA ingestelde Privacy Autoriteit controleert of de bedrijven zich houden aan de wettelijke vereisten rond het recht op informatie, op inzage, op gericht gebruik en waar van toepassing het toestemmingsvereiste. Ook controleert de Privacy Autoriteit of het bedrijf voldoende is toegerust op een verantwoorde verwerking van gegevens, zoals de aanwezigheid van een toegangsregeling voor toegang tot en verwerking van de data, beveiliging (ISO gecertificeerd), het inschakelen van bewerkers en de aanwezigheid van bewerkersovereenkomsten. Het bij herhaling niet voldoen aan de vereisten van de waarborg kan tot uitsluiting van het betreffende bedrijf leiden. De waarborg is nu gebaseerd op de Wbp, maar zal met de introductie van de AVG daarop worden aangepast.

Domein Banken

De bancaire sector heeft van oudsher een gedetailleerd inzicht in de financiële situatie van zijn klanten. Steeds meer transacties verlopen langs elektronische weg waardoor gedetailleerde profielen van klanten kunnen worden opgesteld die steeds meer contextuele informatie bevatten. Dit leidt tot op de persoon afgestemde producten en diensten. In principe zijn banken ook in staat om klanten te helpen bij het tijdig signaleren van risicovolle situaties en hun te ondersteunen bij het betalingsgedrag dat bij een betreffende situatie passend is. Vanuit privacy-oogpunt zijn banken hier terughoudend in. Daarnaast kan een bank vanuit zijn kennis over de financiële situatie van een klant en zijn of haar bestedingspatroon ondersteuning bieden bij het organiseren van het financiële huishouden van een klant. Daarbij kan gebruik worden gemaakt van kennis van de bestedingspatronen van vergelijkbare huishoudens om bepaalde doelen te stellen en te realiseren. Dit soort diensten wordt wel verkend maar nog niet in de praktijk toegepast. Nieuwe betaaldiensten bieden klanten tegelijkertijd mogelijkheden om onderlinge betalingen te verrekenen zonder tussenkomst van een bank.

Strategie en beleid

Branche- en koepelorganisaties oriënteren zich met behulp van beleidsdocumenten op de vraag hoe om te gaan met big data en privacy. Behalve een uiting van de zorg om de privacy zijn *white papers* en *green papers* ook een manier om de veranderende markten in kaart te brengen en na te gaan wat de ontwikkelingen voor de verschillende partijen betekenen. De aandacht voor privacy in deze plaatsbepaling geeft aan dat branches een verantwoorde omgang met big data als essentieel voor hun bedrijfstak zien.

Voorbeeld: Mobiliteitsbranche

In de mobiliteitsbranche hebben verschillende partijen beleidsdocumenten uitgebracht waarin ze aangeven hoe ze tegenover de omgang met persoonsgegevens staan. De Europese Associatie van Automobielfabrikanten ACEA hanteert vijf uitgangspunten (transparantie, keuzevrijheid, dataprotectie, data security en proportionele bewerking) voor de verantwoorde omgang met persoonsgegevens door de aangesloten automobielfabrikanten. De BOVAG stelt de consument centraal, en wil deze in een regierol. Die regierol betreft zowel de data die van randapparatuur (zoals navigatiesystemen en ritregistratiesystemen) als van de auto zelf afkomstig zijn. De ANWB zet de gebruiker centraal en vindt dat de gebruiker keuzevrijheid moet hebben welke data wordt verzameld, met welk doel en wie toegang krijgt tot deze data.

Voorbeeld: Verbond van verzekeraars

Het Verbond van Verzekeraars heeft een green paper gepubliceerd waarin het ingaat op de rol van big data voor verzekeraars en de consequenties voor de privacy.[53] Verzekeraars zijn al via de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen (GVPFI) gebonden aan bepaalde handelingen om de privacy van verzekerden te borgen. Het green paper gaat een stap verder door expliciet in te gaan op de thematiek van big data en privacy voor de verzekeraars. Het green paper besteedt uitgebreid aandacht aan de risico's op onterechte vormen van uitsluiting en discriminatie door de gedetailleerde benutting van data. Deze data kunnen van allerlei bronnen afkomstig zijn. Profielen kunnen worden opgesteld op basis van uiteenlopende bronnen en vervolgens worden toegepast op verzekerden.[54] Het Verbond onderkent deze risico's. Het Verbond stelt dat het nog te vroeg is om nu al verdergaande maatregelen af te kondigen. Eerst is het zaak om beter grip te krijgen op wat de werkelijke risico's zijn en hoe die zich in de praktijk manifesteren.
Wel stelt het Verbond dat het nu al aan de slag gaat, bijvoorbeeld door de gedragscode te actualiseren met daarin aandacht voor hoe klanten geïnformeerd kunnen worden over hun gegevens en de verwerkingen met deze gegevens. Het Verbond richt zich op de inzetbaarheid van technische maatregelen. Daarnaast meldt het Verbond de start van een Solidariteitsmonitor waarmee het zicht wil blijven houden op de uitwerking van het gebruik van big data op de praktijk van verzekeraars (wel of niet onbedoelde en indirecte vormen van discriminatie).

Ronde-tafelsessies

Branche- en koepelorganisaties lanceren initiatieven om met elkaar te verkennen welke uitdagingen het hoofd geboden moeten worden. Een voorbeeld van een dergelijk initiatief waarin big data en privacy een rol spelen zijn de ronde-tafelsessies die in de mobiliteitsbranche worden georganiseerd.

Voorbeeld: Mobiliteitsbranche

De verschillende partijen die met datageneratie en -verwerking rond auto, verkeer en vervoer te maken hebben, komen sinds enige tijd bij elkaar om helder te krijgen wat er precies gaande is in de verkeers- en vervoerswereld, welke rol de verschillende partijen in deze ontwikkelingen spelen, welke ontwikkelingen zich manifesteren rond big data en nieuwe diensten, en welke consequenties dit heeft voor de positie van de automobilist (waaronder consequenties voor zijn/haar privacy). Vanuit de programma's 'Beter Benutten' en 'Connecting Mobility' van het ministerie van Infrastructuur en Milieu is een aantal Overlegtafels in het leven geroepen waarbij marktpartijen, kennisinstellingen en overheidspartijen elkaar met regelmaat treffen over specifieke deelonderwerpen rondom connectiviteit en data met betrekking tot mobiliteit. Privacy is onderdeel van twee overlegtafels: Juridische aspecten en Security. Deze aanpak biedt goede mogelijkheden om op nieuwe ontwikkelingen in te spelen, knelpunten en risico's te benoemen en oplossingen voor te stellen en uit te werken.

Domein Energie – Netbeheerders

De netbeheerders hebben de opgave om de energietransitie die is aangegeven in het Energieakkoord te faciliteren. Een betere voorspelbaarheid van de energievraag en een vlakkere vraag naar energie (met minder pieken en dalen) helpt om met minder capaciteit de benodigde energie te transporteren. Stimuleren van energiebesparing bij de klant door inzicht in energieverbruik helpt daarbij om de pieken te verlagen. De investeringen van de netbeheerders in de energie-infrastructuur zijn aanzienlijk; iedere besparing in die investering is welkom.
Voor netbeheerders is inzicht in vraag en aanbod van energie van groot belang om de elektriciteitsvoorziening adequaat in te kunnen richten en te kunnen beheren. Ontwikkelingen die hierin een rol spelen zijn de toenemende aanleg van decentrale energieopwekkingssystemen (zonnepanelen, windenergie, warmtenetten, warmtekrachtinstallaties, biomassa) die een bijdrage leveren aan de energieproductie, de opkomst van coöperaties die een belangrijk deel van hun energievraag en –aanbod zelf afhandelen (maar in kritieke situaties wel terug moeten kunnen vallen op energielevering via het net), nieuwe energievragers zoals de elektrische auto en energieopslag zoals een thuisbatterij. Het slimme net en de slimme meter zijn voor de netbeheerders twee cruciale innovaties die in de komende jaren over heel Nederland uitgerold worden. De werkzaamheden van de netbeheerders worden in toenemende mate datagedreven. Zij hebben er groot belang bij dat de data die via de slimme meter beschikbaar komt gebruikt kan worden voor het faciliteren van de energietransitie op een voor de klant transparante en acceptabele wijze.

6.4 Ondersteunende maatregelen door derde partijen

De waarborging van de privacy van consumenten vraagt niet alleen om inspanningen van bedrijven en brancheorganisaties maar ook van andere partijen. Het op peil houden van de kennis over privacy en mogelijkheden om deze te beschermen vraagt om een afgestemd aanbod van advisering en opleiding. Nieuwe inzichten kunnen tot voordeel strekken, bijvoorbeeld omdat daardoor nieuwe diensten op een inherent privacyrespecterende manier kunnen worden ingericht. En ook de toezichthouder kan bijdragen aan het creëren van goede randvoorwaarden voor bedrijven om op een verantwoorde manier met persoonsgegevens om te gaan.

Voorbeeld: Advisering door derde partijen
Verschillende consultancybedrijven hebben zich toegelegd op advisering over de borging van privacy in organisaties en hun dienstverlening. Dit betreft ook onderwerpen rond big data en privacy. De consultancyorganisaties bieden tools om privacykwesties die aan dataprocessen en dienstverlening vast zitten in kaart te brengen, en deze kwesties op de juiste manier aan te pakken. Deze organisaties spelen als één van de eerste in op de nieuwe vragen die de AVG met zich meebrengt. Daarnaast richten steeds meer consultancyorganisaties zich niet alleen op juridische en organisatorische kwesties maar ook op onderliggende systeemarchitecturen en de technische infrastructuur van diensten. Dat betekent dat er ook meer kennis en ervaring beschikbaar komt om dataprotectie by design en by default te regelen. Naarmate het afdekken van risico's rond big data en privacy voor bedrijven belangrijker gaat worden (bijvoorbeeld vanwege de toegenomen boetes die de AP op mag leggen) zullen consultancybedrijven ook hier op inspringen en hun methodieken hierop aan gaan passen.

Voorbeeld: Beleidsregels van de Autoriteit Persoonsgegevens
De Autoriteit Persoonsgegevens biedt op zijn website informatie over hoe ze wettelijke bepalingen toepast (de beleidsregels). Het betreft informatie over datalekken, de beveiliging van persoonsgegevens, cameratoezicht, persoonsgegevens op internet. Voor bedrijven bieden deze regels duidelijkheid over toegestane praktijken. Het aantal beleidsregels is nu nog beperkt. Uitbreiding van deze regels met voor bedrijven relevante informatie over toegestane big-datapraktijken biedt bedrijven aanvullende duidelijkheid.

Voorbeeld: Regulatory sandbox
De Engelse toezichthouder op de financiële sector gebruikt een regulatory sandbox die bedrijven speelruimte biedt om nieuwe activiteiten te onderzoeken waarvan de wettelijke implicaties nog niet duidelijk zijn.[55] Ook voor de Nederlandse bedrijven die zich richten op big-datatoepassingen zou zo'n sandbox behulpzaam kunnen zijn. Deze regulatory sandbox bestaat uit drie onderdelen: een uitleg van de toezichthouder over de toepassing van regels op het betreffende product/dienst; de speelruimte die de toezichthouder kan bieden (uitzonderingsgronden) om een product/dienst te kunnen testen zonder geconfronteerd te worden met beperkende eisen vanuit de Wbp/Avg; een formele toezegging van de toezichthouder dat hij niet zal ingrijpen zolang het bedrijf zich aan de afspraken houdt. Bedrijven geven aan dat ze in aanmerking willen komen voor een dergelijke behandeling en dat ze met de toezichthouder tot formele en afdwingbare afspraken willen komen. Zo'n regulatory sandbox biedt onder meer mogelijkheden om te oefenen met het formuleren van legitieme, voldoende afgebakende doelen in het kader van data-analyse die toegevoegde waarde in de data hoopt te ontsluiten.

Voorbeeld: Privacy policy generator
Andere ondersteunende instrumenten zijn de privacy policy generator en de beschikbaarstelling van modelbewerkersovereenkomsten. Op basis van informatie die een bedrijf aanlevert wordt een privacy policy gegenereerd die op de betreffende situatie van toepassing is. Deze dienst wordt door verschillende consultancyorganisaties aangeboden. Bij verschillende organisaties is deze dienstverlening geautomatiseerd waarbij een bedrijf via internet een privacy policy kan laten genereren. Voor beide geldt dat een aanvullende toets nodig is om zeker te zijn dat deze instrumenten voldoen aan de eisen die de AVG stelt. In de praktijk is dit nog niet geregeld.

Domein Verzekeringen

De verzekeraars zijn van oudsher organisaties die gebruik maken van statistische modellerings-technieken om risicoinschattingen te kunnen maken en hierop verzekeringspakketten en -premies te baseren. Deze modelleringstechnieken maken gebruik van historische dataverzamelingen waaruit trends en specifieke kenmerken van situaties te herleiden zijn. Via een stelsel van wettelijke bepalingen is aangegeven op welke gebieden het verzekeraars is toegestaan om te differentiëren in hun aanbod aan verzekerden. Ook is vastgelegd welke schotten verzekeraars moeten hanteren om te voorkomen dat verschillende soorten informatie over een verzekerde met elkaar gecombineerd worden. Verzekeraars zoeken naar manieren om de actuariële gegevens verder te verrijken met informatie uit andere bronnen. De kwaliteit van de data van die bronnen is van groot belang om tot zinvolle afleidingen te kunnen komen. Tegelijkertijd verkennen verzekeraars de mogelijkheden om verzekerden op het juiste moment met het juiste aanbod te benaderen (bijv. een reisverzekering). Daarbij spelen ze in op de trend dat verzekerden sneller geneigd zijn te switchen tussen verzekeraars en actiever reageren op aangeboden verzekeringsproducten.
De verzamelde gegevens bieden verzekeraars ook mogelijkheden om fraude en misbruik van verzekeringsproducten sneller op te sporen.

Voorbeeld: Opleiding tot Functionaris voor de gegevensbescherming

Verschillende instellingen bieden een opleiding tot Functionaris voor de gegevensbescherming/dataprotectie officer aan. Deze opleidingen – die relatief kort van duur zijn (één tot enkele dagen) – behandelen alle relevante aspecten voor het functioneren van een DPO. Daarbij is ook aandacht voor privacyrisicomanagement en big data. Er is aandacht voor organisatorische aspecten van dataprotectie maar minder voor de technische aspecten. De International Association of Privacy Professionals (IAPP) biedt verschillende gecertificeerde opleidingen, onder meer tot Information Privacy Professional, tot Information Privacy Manager en tot Information Privacy Technologist. Ook hier is sprake van een in de tijd beperkt opleidingstraject (in de regel slechts twee dagen). De opleidingen zijn geaccrediteerd door het American National Standards Institute (ANSI), waarmee ook strikte richtlijnen voor het toezicht op de accreditatie zijn vastgelegd.

Voorbeeld: Onderzoek door kennisinstellingen

Onderzoeksinstellingen werken via onderzoeksprogramma's aan oplossingen die bedrijven moeten ondersteunen in de verantwoorde omgang met persoonsgegevens. Deze onderzoeksprogramma's zijn nationaal van aard (bijvoorbeeld het in ontwikkeling zijnde Commit2Data programma en het voorstel voor een Zwaartekrachtprogramma Responsible Data Science, het NWO-programma voor alle topsectoren "Maatschappelijk Verantwoord Innoveren") en Europees en internationaal (Horizon2020 met aparte onderzoekslijnen voor big data en privacy, ERC grants, Wereldbank, OECD). In de regel duurt het even voor de onderzoeksresultaten tot rijpe marktproducten hebben geleid, maar tegelijkertijd geven deze programma's een behoorlijke boost aan het denken over verantwoord innoveren en kunnen zij Nederland gunstig positioneren. Daarnaast zijn kennisinstellingen betrokken bij advisering van bedrijven over technische, juridische en organisatorische vraagstukken rond big data en privacy.

7 Aanbevelingen

Zoals in hoofdstuk 6 naar voren komt staan bedrijven dus vele mogelijkheden ter beschikking om op een verantwoorde manier met persoonsgegevens om te gaan en zich rekenschap te geven van de risico's die aan big-datatoepassingen verbonden zijn. In dit laatste hoofdstuk presenteert de expertgroep enkele aanbevelingen die ertoe bij moeten dragen dat wat in theorie mogelijk is in de praktijk ook gestalte krijgt. De aanbevelingen worden op dezelfde driedeling gebaseerd als waar de oplossingen in hoofdstuk 6 in zijn geplaatst: aanbevelingen aan bedrijven, aanbevelingen aan branche- en koepelorganisaties en aanbevelingen aan derde partijen.

7.1 Aanbevelingen aan bedrijven

Bedrijven kunnen zelf investeren in een verantwoorde omgang met persoonsgegevens. Dit leidt intern tot een zorgvuldiger benadering van het gebruik van persoonsgegevens, en extern tot een vertrouwenwekkend profiel. Privacy staat nu als een '*dissatisfier*' bekend, als een factor waarop alleen maar negatief gescoord kan worden. Door meer (gerichte) investeringen in de verantwoorde omgang met persoonsgegevens en verantwoord innoveren met big data, en door dit gericht en bewust uit te dragen creëert een bedrijf een vertrouwensband met zijn consumenten en bewijst het ook zichzelf een dienst.

Benut het onderscheidend vermogen van een verantwoorde omgang met persoonsgegevens

Het wettelijk kader dwingt bedrijven bepaalde voorzorgsmaatregelen in acht te nemen en te investeren in een aantal voorzieningen om consumenten tegemoet te komen en te tonen dat zaken goed geregeld zijn. Dat is mooi, maar het levert weinig onderscheidend gedrag op. De expertgroep adviseert om de noodzakelijke investeringen in de verantwoorde omgang met persoonsgegevens te zien als een manier om het bedrijf onderscheidend te laten zijn op de markt, en dit actief uit te dragen.

Investeer in de professionalisering van de verantwoorde omgang met persoonsgegevens

Er zijn vele mogelijkheden om invulling te geven aan de eisen die het wettelijk kader stelt.
De expertgroep adviseert om deze eisen te benaderen vanuit een raamwerk dat professionalisering in de omgang met persoonsgegevens nastreeft. Daar zijn verschillende instrumenten voor op de markt. Naast het *Privacy Maturity Model* als kader waarin een bedrijf zijn eigen niveau van professionalisering kan 'scoren' beveelt de expertgroep aan:

1. Benut de Dataprotectie Impact Assessment als risico-instrument om privacyrisico's voortijdig in kaart te brengen en te minimaliseren. Ga ervan uit dat de DPIA steeds van toepassing is wanneer individuen getarget worden op basis van big-datatoepassingen en dat de assessment regelmatig herhaald moet worden. Maak binnen de bedrijfsvoering een helder onderscheid tussen het risico voor de consumenten en de aansprakelijkheidsrisico's voor het bedrijf.
2. Ga ruimhartig na op welke plekken in de gegevensstromen gebruik kan worden gemaakt van pseudonimisering en gegevensversleuteling als standaardinstelling. Investeer in de aanpak van dataprotectie *by default* en *by design*. Onderzoek de mogelijkheden tot implementatie van dataprotectie *design patterns* in het gehele dataverwerkingsproces. Dit soort maatregelen verkleint de kans dat in geval van datalekken het lekken van onrechtmatig verwerkte gegevens tot grotere privaatrechtelijke aansprakelijkheid leidt.
3. Ga na hoe de zorg voor een verantwoorde omgang met persoonsgegevens in de gehele organisatie kan worden ingebouwd. Pas de DPO en de daarin meekomende organisatorische elementen breed en ruimhartig toe als onderdeel van een professionaliseringsstrategie. Betrek de directie/de Raad van Bestuur bij de algehele in de organisatie in te voeren privacystrategie en inventariseer op welke cruciale onderdelen in de ontwikkeling en exploitatie van nieuwe diensten de directie/Raad van Bestuur betrokken dient te worden om de privacyrisico's te beoordelen.
4. Ga na in hoeverre derde partijen kunnen worden ingezet om toe te zien op de verantwoorde omgang met persoonsgegevens. Deze derde partijen kunnen bijdragen aan het voorkomen van risico's voor consumenten.

Domein Retail

De retailsector verzamelt informatie over het koopgedrag van consumenten via de ‘kassabon’, via de ‘klantenkaarten’, door de consument rechtstreeks te bevragen in surveys en enquêtes maar ook via analyse van looproutes in winkels en zoekgedrag op websites. De data bieden retailers de mogelijkheid om producten en diensten af te stemmen op (individuele) voorkeuren van consumenten waarbij ook rekening kan worden gehouden met bijzondere omstandigheden of gebeurtenissen. In principe ontstaan hierdoor ook mogelijkheden tot prijsdifferentiatie en een verregaande personalisering van het aanbod. De gedetailleerde inzichten die verkregen worden in het koopgedrag bieden retailers ook de mogelijkheid tot efficiënt voorraadbeheer en een efficiënte inrichting van hun logistieke processen, waardoor verspilling in producten en overbodige kilometers in vervoersstromen kunnen worden teruggedrongen.

Investeer in transparantie voor de consument

Het wettelijk kader legt bepaalde verplichtingen op in de wijze waarop onder meer consumenten hun rechten kunnen laten gelden. De expertgroep adviseert om ruimhartig met deze verplichtingen om te gaan en deze te benutten om het vertrouwen van consumenten in de intenties en de handelswijze van het bedrijf te vergroten. Door te investeren in transparantiemaatregelen geeft het bedrijf aan zich zijn verantwoordelijkheid jegens de consument te realiseren. Deze transparantiemaatregelen moeten wel worden aangepast aan het type consument en dienst. Niet alle consumenten willen alles in detail weten, en voor niet elke dienst is dit nodig.

7.2 Aanbevelingen voor branche- en koepelorganisaties

Branche- en koepelorganisaties kunnen bedrijven bereiken die door andere partijen moeilijker te benaderen zijn. Ze zijn gericht op wat bedrijven bindt, en kunnen min of meer verplichtende eisen aan bedrijven opleggen die lid willen zijn van een branche- of koepelorganisatie. Ze kunnen bijdragen aan het vergroten van het bewustzijn bij bedrijven voor de uitdagingen die er rond de benutting van persoonsgegevens voor big-datatoepassingen spelen. Ze kunnen concreet bijdragen door de branche te organiseren en middelen aan te bieden die bedrijven helpen.

Stimuleer de ontwikkeling van gedragscodes

De expertgroep beveelt aan om te werken aan de ontwikkeling van gedragscodes rond de verantwoorde omgang met persoonsgegevens in het licht van big-datatoepassingen. Gedragscodes dragen bij aan het creëren van een gelijk speelveld. Bedrijven kunnen aangesproken worden op hun gedrag. Daarnaast is het opstellen van een gedragscode een beproefde manier om het veld te verenigen, na te gaan waar problemen zitten en te onderzoeken hoe deze problemen door de branche opgepakt moeten worden.

Stimuleer het exploreren van nieuwe ontwikkelingen in dialogen

De expertgroep beveelt aan om de problemen die bedrijven ervaren rond de ontwikkeling van nieuwe big-datatoepassingen te adresseren in dialoogsessies waar alle relevante partijen bij zijn aangehaakt. Op deze manier kunnen blokkades die door partijen worden ervaren, geïnventariseerd worden en kunnen ontwikkelingen die zich voordoen snel betrokken worden in de dialoog. In de regel zal sprake moeten zijn van privaat-publieke organisatie van de dialoog. Veel innovatieve ontwikkelingen vinden plaats in sectoren waar traditionele rollen en patronen onder druk staan door nieuwe toetreders, nieuwe business modellen en nieuwe marktverhoudingen. De verantwoorde omgang van persoonsgegevens hoeft in deze ontwikkelingen niet altijd de centrale kwestie te zijn maar de ervaring leert dat dit vaak wel een belangrijk onderdeel van de ontwikkelingen is.

Creëer awareness bij de bedrijven in de branche

De expertgroep beveelt aan dat branche- en koepelorganisaties het voortouw nemen bij het informeren van bedrijven over het belang van een verantwoorde omgang met persoonsgegevens, de mogelijkheden die er zijn om dit te organiseren en de rol die bedrijven hier zelf in kunnen spelen. Daarmee geven branche- en koepelorganisaties aan dat de verantwoorde omgang met persoonsgegevens een kwestie is die vanuit bedrijfs- en maatschappelijk perspectief hoog op de agenda staat. Branche- en koepelorganisaties kunnen de uitwisseling van ervaringen stimuleren in hoe bedrijven hiermee omgaan en welke instrumenten gepast zijn.

Domein Energie - leveranciers en dienstenaanbieders

Energieleveranciers en onafhankelijke dienstenaanbieders bieden huishoudens inzicht in hun energieverbruik. De data uit de slimme meter geven – met een vertraging van een dag – een beeld van het elektriciteits- (per kwartier) en gasverbruik (per uur). Daaruit is veel af te leiden over de energieconsumptie van een huishouden. Deze informatie kan gebruikt worden om consumenten te ondersteunen in het nemen van energiebesparende maatregelen (zonnepanelen, energiezuinige apparatuur). Behalve de reguliere data uit de P4-poort van de slimme meter biedt de P1-poort nog fijnmaziger informatie over het energieverbruik (in de toekomst eens per minuut). Met de komst van sensoren in het huishouden (internet der dingen) wordt fijnmazige regeling van het energieverbruik mogelijk. Daarnaast biedt het mogelijkheden tot het verzorgen van andere diensten (brandveiligheid, alarmering, aan- en aanwezigheidsmeldingen, etc.).

7.3 Aanbevelingen voor derde partijen

Toezichthouders en ministeries spelen een speciale rol in de organisatie van een goed lopend innovatiesysteem rond big-datatoepassingen. Toezichthouders hebben een wettelijke taak tot toezicht, en agenderen wettelijke kwesties in de daartoe bestemde organen. Ministeries houden oog op mogelijk optredende marktimperfecties en kunnen stimulerende maatregelen uitvaardigen om blokkades weg te nemen.

Verbeter de organisatie van het toezicht

De expertgroep beveelt aan om te investeren in de organisatie van het toezicht op de markt van big-datatoepassingen. Door de invoering van de AVG worden de taakstelling en het functioneren van de AP beïnvloed. Tijdens de dialoogsessies brachten vele partijen naar voren behoefte te hebben aan een toezichthouder die geconsulteerd kan worden voorafgaand aan de introductie van een nieuwe dienst. Daarnaast werd gewezen op de spreiding van toezichttaken over meerdere toezichthouders.
De uitvoering van de e-Privacy richtlijn is verdeeld over Autoriteit Consument en Markt, de Autoriteit Persoonsgegevens en het Agentschap Telecom. Ook in andere lidstaten speelt deze spreiding.
De Europese Unie buigt zich over een herziening van de ePrivacy richtlijn, waarbij ook de positie van de toezichthouder aan bod kan komen.
De expertgroep ziet de volgende mogelijkheden om het toezicht te verbeteren:

1. Investeer in capaciteit bij de toezichthouder(s) om met (organisaties van) bedrijven al tijdens het innovatieproces (niet bindend) mee te kunnen denken en richting te kunnen geven aan de invulling van de kaders bij big-datatoepassingen. Het karakter van de toezichthouder *as such* dient hierbij te worden bewaakt.
2. De investering in capaciteit moet ook leiden tot een intensivering van het overleg met branche- en koepelorganisaties om ook het MKB te bereiken met algemene kennis over de wet.
3. Onderzoek de mogelijkheden tot het creëren van een *regulatory sandbox* zoals deze in het Verenigd Koninkrijk is ontwikkeld en waar de toezichthouder in overleg met bedrijven speelruimte creëert om nieuwe big-datatoepassingen te onderzoeken.
4. Onderzoek nauwkeurig de verdeling van verantwoordelijkheden rond het toezicht op de opvolger van de ePrivacyrichtlijn. Communiceer de verdeling breed via branche- en koepelorganisaties.

Maak consumenten bewust van de veranderingen die gaande zijn en hun rol daarbij

De expertgroep beveelt aan om een apart programma op te zetten dat gericht is op bewustwording van en dialoog met consumenten over de huidige ontwikkelingen. Consumenten zijn startpunt en sluitpunt van vaak ingewikkelde processen waar zij via hun persoonsgegevens deelgenoot van zijn. Tegelijk zijn deze processen zo complex of spelen zich zo ver af van de leefwereld van de consument dat deze zich daar geen beeld van kan vormen. Daarnaast hebben consumenten weinig of geen weet van de rechten die ze kunnen uitoefenen rond de verzameling en verdere verwerking van hun gegevens.
Door consumenten bewuster te maken van de veranderingen en de rol die persoonsgegevens daar bij spelen kan wantrouwen worden weggenomen en vertrouwen worden bevorderd. Een dergelijke campagne kan het initiatief zijn van het ministerie van Economische Zaken en voortbouwen op de website veiliginternetten.nl.

Investeer in kennisopbouw over de impact van big data op burgerrechten

De veranderingen die zich in de samenleving manifesteren rond de toepassing van big data zijn fundamenteel en diepgravend van aard. Ze worden gevoed door de resultaten van onderzoek naar nieuwe algoritmen, nieuwe modelleringstechnieken (waaronder gedragsmodellering), machine leren en kunstmatige intelligentie. Al deze terreinen kunnen een enorme impact kunnen hebben op grondrechten van consumenten (en burgers). Dit roept de vraag op hoe ervoor te zorgen dat maatschappelijke normen en waarden leidend blijven bij deze ontwikkelingen. De expertgroep beveelt aan om apart te investeren in een onderzoeksprogramma zoals dat ook in het Verenigd Koninkrijk is opgezet rond deze thematiek.

Eindnoten

[1] Kamerstuk 32761, nr. 78.
[2] Kamerstuk 33009, nr. 10.
[3] Een voorbeeld is het geautomatiseerd plaatsen van advertenties (*real time bidding*) via een wisselwerking tussen een *Data Selling Platform* en een *Data Management Platform*. Het biedproces verloopt in milliseconden en gebeurt op basis van gecreëerde *audiences*. De *clickthrough rate* geeft inzicht in welke advertentiestrategieën de hoogste impact hebben. Die gegevens worden *real time* verwerkt en kunnen tot aanpassing van het biedproces leiden.
[4] Een studie van BGC schat dat in 2020 de 'personal data market' een omvang heeft van 8% van het BNP. Zie BGC, 2012, p.3-4.
[5] Een voorbeeld vormen de dataconsultants, partijen die data verzamelen en verder verwerken en die andere partijen ondersteunen in het valoriseren van data (onder meer via advertenties en *branding*). In Europa kenden deze over de jaren 2012 - 2015 een vertienvoudiging, van 200 in 2012 naar 2000 in 2015. Zie http://idlewords.com/talks/website_obesity.htm#top.
[6] Voorbeelden zijn de ontwikkelaars en aanbieders van nieuwe apps. Dit kunnen zeer kleine ondernemingen zijn (vijf tot tien personen) met toegang tot een grote hoeveelheid data van personen. Andere voorbeelden zijn online game aanbieders en bekende bedrijven als booking.com en vliegtickets.nl.
[7] Een voorbeeld is het meten van bezoekersstromen op festivals, stations, drukke winkelcentra en dergelijke. Het herleiden van vervoerspatronen geeft inzicht in mogelijk optredende knelpunten dat voor de inrichting van een winkelcentrum van belang kan zijn, of dat de politie ondersteunt bij het in goede banen leiden van een menigte mensen bij een evenement.
[8] Dit is het probleem van de re-identificatie van personen. Zie Artikel 29 Werkgroep, Opinie 05/2014 over Anonimiseringstechnieken.
[9] Zo kunnen in een dataverzameling bepaalde categorieën respondenten oververtegenwoordigd zijn en andere ondervertegenwoordigd. In bepaalde gevallen wordt hiervoor gecorrigeerd. Soms is evenwel niet bekend hoe het *sample* gecorrigeerd moet worden. Bij de analyse zullen keuzes worden gemaakt van onderlinge afhankelijkheden tussen variabelen. Dat kan er toe leiden dat bepaalde afhankelijkheden buiten beeld blijven terwijl die mogelijk wel van belang zijn.
Zie Solon Barocas & Andrew D. Selbst, 2016, Mireille Hildebrandt, 2015 en Kate Crawford, 2013.
[10] Executive Office of the President, 2016, p. 9. In dit rapport wordt voor een vijftal toepassingen de invloed van de samenstelling van de data en de gebruikte algoritmen onderzocht (kredietverlening, werkgelegenheid, opleidingskansen, opsporing). De resultaten van de verkenning leiden tot de conclusie dat het van belang is alert te zijn op de samenstelling van de data en de werking van de algoritmen omdat deze tot onbedoelde en ongewenste uitkomsten in de beoordeling van situaties kunnen leiden.
[11] Een interessant overzicht van toevallige verbanden biedt Tyler Vigen in zijn boek *Spurious correlations*. Een voorbeeld van zo'n toevallige correlatie is het verband dat aangegeven kan worden tussen de het aantal doctoraten in de computerwetenschappen en de verkoop van stripboeken. Zie Vigen, 2015, p. 42.
[12] Een bekend voorbeeld is het aanbod dat een Amerikaans bedrijf deed aan een tienerdochter voor artikelen die bedoeld waren voor zwangere vrouwen. De vader van de dochter voelde zich gebruuskeerd, met name omdat hij ervan uitging dat het bedrijf een vervelende fout had gemaakt. Dit bleek niet het geval, alleen had het meisje haar vader nog niet ingelicht. Zie New York Times, 19 februari 2012.
[13] Zie Van den Hoven, 2008, 310 ev.. Het accent ligt hier op de schade die individuen kunnen oplopen wanneer gegevens over hen gebruikt worden. Zie ook overweging 75 van de Algemene Verordening Gegevensbescherming.
[14] We gaan vooral in op de bescherming van personen inzake hun gegevens. Er is een direct verband tussen de bescherming van persoonsgegevens en de privacy van personen. Door gegevens over een persoon te beschermen wordt ook de privacy van deze persoon beschermd. Het begrip privacy betreft echter meer dan alleen de bescherming van gegevens betreffende een persoon. Er zijn vele omschrijvingen te vinden van dit begrip. Een veel gebruikte beschrijving stelt dat privacy betrekking heeft op de vrijwaring van onredelijke beperkingen in de constructie van je eigen identiteit (Agre en Rotenberg 1997; zie ook Hildebrandt 2015, 80). In deze rapportage spreken wij vooral over de bescherming van persoonsgegevens.
[15] Partijen die verder van de consument afstaan en zich richten op het leveren van diensten aan derde partijen hebben ook met deze tweezijdige relatie te maken. Naarmate een bedrijf verder afstaat van de consument groeit echter het risico dat het betreffende bedrijf ook minder de directe noodzaak van verantwoord handelen ervaart, bijvoorbeeld omdat een directe confrontatie met consumenten ontbreekt.

[16] Verordening 2016/279, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.
[17] Richtlijn 95/46/EG.
[18] Direct identificerende gegevens zijn bijvoorbeeld de naam van een persoon, een foto van een persoon en de geboortedatum. Indirect identificerende gegevens zijn gegevens die in combinatie met een of meer andere gegevens de identiteit van een persoon onthullen. Voorbeelden hiervan zijn het IP-adres en het kenteken van een auto. Bij identificatie gaat het onder meer om de mogelijkheid om een unieke persoon af te zonderen uit een groep ('singling out', aan te wijzen of te herkennen). Als dat kan dan is sprake van identificerende gegevens (direct dan wel indirect).
[19] Een pseudoniem ontstaat door identificerende gegevens te vervangen door een willekeurige verzameling van tekens. Identificatie is dan in de praktijk nog steeds mogelijk, bijvoorbeeld door een koppelingstabel te gebruiken die het pseudoniem koppelt aan identificerende gegevens. Door organisatorische en technische maatregelen kan deze koppeling feitelijk onmogelijk worden gemaakt. Dergelijke handelswijzen worden door de AVG gepropageerd. Ze dragen bij aan een daadwerkelijke bescherming van personen in verband met de verwerking van hun gegevens.
[20] AVG, art 6, lid 1, sub f.
[21] Een contract impliceert dat het doel het nakomen van het contract moet zijn, vitale belangen van de betrokkene impliceert dat het doel niet verder mag gaan dan het behartigen van die belangen, een juridische verplichting is altijd doelgebonden, en een publiek belang geeft een duidelijke indicatie over het soort doel. Toestemming moet vrijelijke, specifiek, geïnformeerd en ondubbelzinnig gegeven zijn voor de verwerking van gegevens voor een expliciet, afgebakend en legitiem doel.
[22] Dit betreft persoonsgegevens over ras of etnische afkomst, politieke overtuigingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens gericht op identificatie, gezondheidsgegevens, gegevens over seksueel gedrag of seksuele gerichtheid (AVG, art 9, lid 1).
[23] AVG, art. 5, lid 1 en art. 89, lid 1. Dit laat onverlet dat niet in alle gevallen evident is of onderzoek gezien kan worden als historisch, wetenschappelijk of statistisch.
[24] AVG, art. 15, 16, 18, en 21.
[25] AVG, art. 15, lid 3, art. 17 en 20.
[26] Zie art 17 lid 3 en art 20 lid 3. Deze verwijzen naar het recht op vrijheid van meningsuiting en informatie, wettelijke verwerkingsplichten, redenen van algemeen belang, archivering in het algemeen belang, en het instellen, uitoefenen of onderbouwen van een rechtsvordering.
[27] AVG, art 24 en 25.
[28] AVG, art 35.
[29] AVG, art 83.
[30] AVG, art 6, lid 4. Daarnaast is het de vraag of er altijd een vrije keuze is voor een van de grondslagen. Indien een bedrijf ook te maken heeft met de ePrivacyrichtlijn (zoals in het geval van aanbieders van elektronische communicatienetwerken en/of -diensten) en gegevens over personen opslaat op of verzamelt van de computer van de betrokkenen dan is toestemming de enige grondslag die is toegestaan (Art 5.3 van de Telecommunicatiewet).
[31] Zie https://www.the-fca.org.uk/firms/project-innovate-innovation-hub/regulatory-sandbox voor een toelichting op de wijze waarop de Financial Conduct Authority van het Verenigd Koninkrijk deze *regulatory sandbox* invult.
[32] AVG, art 22, lid 1.
[33] AVG, overweging 71.
[34] AVG, overweging 75.
[35] Waarbij we opmerken dat dit afhankelijk is van de mate waarin de logica uitgelegd moet kunnen worden. Het gaat dan met name om de vraag in hoeverre besluiten die een persoon treffen in detail kunnen worden toegelicht (bijvoorbeeld waarom een persoon in een specifieke situatie wel of niet in aanmerking komt voor een bepaalde dienst).
[36] Transparantie in de herkomst van het profiel en in de motivering van de koppeling van een betrokkene aan een specifiek profiel.
[37] Deze eis (die bekend staat als de 'cookiebepaling') is in Nederland aanvankelijk zeer strikt geïnterpreteerd. Inmiddels is er meer speelruimte gekomen voor de plaatsing en verzameling van noodzakelijke informatie (om de geboden dienst ook goed te laten functioneren en om informatie over het gebruik van de dienst te kunnen verzamelen). De Europese Commissie is in mei 2016 gestart met een procedure voor de herziening van de ePrivacyrichtlijn, dit mede als consequentie van de aanvaarding van de AVG.
[38] Bijvoorbeeld de Elektriciteitswet1998 en de Gaswet, de Wet ter voorkoming van witwassen en financieren van terrorisme.

[39] Dit is het geval (1) als sprake is van een systematische en uitgebreide beoordeling van persoonlijke aspecten van individuen op basis van geautomatiseerde besluitvorming (waaronder profilering) met rechtsgevolgen voor of een wezenlijke impact op het individu; (2) bij grootschalige verwerking van bijzondere categorieën gegevens; (3) bij stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten. Zie AVG, art. 35, lid 3.
[40] Zie voetnoot 25.
[41] AVG, artikel 25.
[42] Zie onder meer het werk aan de Radboud Universiteit, vakgroep Digital Securities.
[43] Zie onder andere de toepassing van homomorfe encryptie in de TrustTester. https://www.tno.nl/nl/aandachtsgebieden/industrie/networked-information/information-creation-van-data-naar-informatietrusttester-veilig-valideren-van-persoonlijke-gegevens/.
[44] Zie onder andere de toepassing van ABC in IRMA technologie. http://www.cs.ru.nl/~jhh/publications/irma-bits-n-chips.pdf.
[45] Zie https://eprint.iacr.org/2016/411.
[46] Zie https://www.tippiq.nl/. Tippiq heeft een discussiepaper uitgebracht 'Democracy for design – food for thought'. Hiermee vraagt Alliander aandacht voor het feit dat onze wereld digitaliseert en daarmee nieuwe systemen worden geïntroduceerd die een steeds belangrijkere rol gaan spelen in cruciale voorzieningen in onze samenleving.
[47] AVG, art. 37-39.
[48] AVG, art. 38, lid 3.
[49] AVG, art. 38, lid 3. De AVG stelt dat de Functionaris gegevensbescherming "rechtstreeks verslag uit[brengt] aan de hoogste leidinggevende van de verwerkingsverantwoordelijke of de verwerker."
[50] AVG, art. 37, lid 5.
[51] AVG, art. 40.
[52] http://www.vmned.nl/Nieuwsbrief2-2016-2/.
[53] Verbond van verzekeraars, *Grip op data – green paper big data*, 2016.
[54] Waarbij voor alle bronnen geldt dat voldaan moet zijn aan de bepalingen uit de AVG. Dit geldt ook indien data worden verrijkt met data uit openbare bronnen.
[55] https://innovate.fca.org.uk/innovation-hub/regulatory-sandbox.

Geraadpleegde deskundigen

Kelly Aartsen, NLE
Jilles van den Beukel, Vice-president Regulatory Affairs, Eneco
Boas Bierings, Privacy officer, Enexis
Leo Bingen, Directeur, SIMS
Yannick Debye, Product manager, Cadreon
Martin Heijnsbroek, Managing partner, MICompany
Marcel van Hest, Strategy, Alliander
Alex van Hoen, Senior statisticus, Verbond van Verzekeraars
Maarten Jonker, Senior manager, Achmea
Ronald de Jong, Senior adviseur Public Affairs, ANWB
Hanne Esther Kruyt, DPO ING Bank Nederland BV, Nederlandse Vereniging van Banken/ ING
Ronald Langendoen, Dataconsultant en CEO, EDM
Alexander van Loon, Adjunct directeur Marketing Particulier, ASR
Mark Noet, CEO, Dataprovider
Diederik Mohr, Adviseur Consumer Affairs, Nederlandse Vereniging van Banken
Léon Mölenberg, Senior beleidsmedewerker/Jurist, Thuiswinkel.org
Carlos Montes Portela, DSO security officer, Enexis
Gerard Moussault, Managing director, Cadreon
Mike Pinckaers, Senior advisor Public Affairs, ANWB
Jan Pino, Compliance officer privacy, Achmea
Johan Rambie, Privacy & Security adviseur, Alliander
Jos Schaffers, Beleidsadviseur algemene zaken, Verbond van Verzekeraars
Harald Swinkels, CEO, NLE
Maarten Vellema, RDW
Bart Voorn, Lead HR analytics, Ahold Delhaize
Joost Zonneveld, CEO/voorzitter, Ealyze/VEDEK

Geraadpleegde literatuur

P.E. Agre & M. Rotenberg, Eds., *Technology and Privacy: The New Landscape,* The MIT Press: California, CA, USA, 1997.

Solon Barocas & Andrew D. Selbst, 'Big Data's Disparate Impact', *104 California Law Review 671*, 2016 (DOI: http://dx.doi.org/10.15779/Z38BG31).

BGC, *The value of our digital* identity, Liberty Global Policy Series, 2012.

Colin Bennett & Charles Raab, *The Governance of Privacy – Policy instruments in global perspective*, Cambridge: The MIT Press, 2006.

Kate Crawford, *The hidden biases in big data*, 2013.
https://hbr.org/2013/04/the-hidden-biases-in-big-data/#

DDMA, *Hoe Nederlanders denken over data en privacy,* DDMA Privacy onderzoek 2016.
http://www.ddma.nl/

ENISA, *Privacy and Data Protection by Design – from policy to engineering*, December 2014.

ENISA, *Privacy by Design in big data – an overview of privacy enhancing technologies in the era of big data analytics*, December 2015.

Executive Office of the President, *Big Data: A report on Algorithmic Systems, Opportunity, and Civil Rights*, Washington, 2016.

Mireille Hildebrandt, *Smart Technologies and the End(s) of Law*, New York: Elgar Publications, 2015.

Jaap-Henk Hoepman, *Privacy Design Strategies*. In: IFIP TC11 29th Int. Conf. on Information Security (IFIP SEC 2014), 446-459, 2014.

Jeroen van den Hoven, 'Information Technology, Privacy and the Protection of Personal Data', in: Jeroen van den Hoven & John Weckert, *Information Technology and Moral Philosophy*, 301-21, Cambridge: Cambridge University Press, 2008.

Viktor Mayer-Schönberger & Kenneth Cukier, *Big data – A revolution that will transform how we live, work and think*, 2013.

OECD, *Data Driven Innovation – Big data for growth and well-being*, OECD: Paris, 2015.

TNO, *Privacybeleving op het internet in Nederland*, Delft: TNO, 2015.

Tyler Vigen, *Spurious correlations*, New York, Hachette Books, 2015.

Alan Westin, *Privacy On and Off the Internet: What Consumers Want* 2002.
http://www.ijsselsteijn.nl/slides/Harris.pdf.

World Economic Forum, *Rethinking personal data: A new lens for strengthening trust*, 2014.

W. Youyou, M. Kosinski & D. Stillwella, 'Computer-based personality judgments are more accurate than those made by humans', *PNAS*, 2014.

Deze brochure is een uitgave van:

Ministerie van Economische Zaken

Postbus 20401 | 2500 EK Den Haag

Augustus 2016
Xerox/OBT, Den Haag | 95075