Kabinetsreactie initiatiefnota Nijboer en Oosenbrug over gegevensgebruik in de financiële sector

1. Inleiding

De initiatiefnota van de leden Nijboer en Oosenbrug (PvdA)[1] gaat in op privacy en gebruik van big data in de financiële sector. De technologische ontwikkelingen gaan snel en brengen een maatschappelijk debat op gang over de voordelen en risico's van deze ontwikkelingen. In de initiatiefnota worden voorstellen gedaan om specifiek voor de financiële sector aanvullende maatregelen te treffen.

Onder invloed van technologische ontwikkelingen wordt het verwerken en analyseren van grote hoeveelheden persoonsgegevens – big data analyse - steeds belangrijker en eenvoudiger. Big data analyse wordt grootschaliger en intelligenter, met toenemende aanwendingsmogelijkheden – variërend van onderzoek naar het gedrag van consumenten t.b.v. advertenties tot allerlei vormen van (financiële) dienstverlening. Het verzamelen van data wordt een zelfstandige activiteit. Gegevens zijn niet langer een bijproduct van de hoofddienst, maar het doel van gegevensverzameling wordt het benutten van de gegevens zelf. Dit wordt veroorzaakt door de toename van de beschikbare rekencapaciteit en doordat telkens meer informatie over mensen beschikbaar is. Technologische ontwikkeling is hier een drijvende factor, zoals bij het *Internet of Things* en het gebruik van algoritmische gegevensverwerking. Deze ontwikkeling biedt weliswaar meer mogelijkheden om op basis van persoonsgegevens nieuwe diensten te ontwikkelen, tegelijkertijd brengt zij risico's met zich mee, bijvoorbeeld ten aanzien van privacy van mensen.

In deze kabinetsreactie worden op basis van eerdere kabinetsreacties en bestaand beleid en regelgeving, de verschillende voorstellen van de initiatiefnemers Nijboer en Oosenbrug besproken. Beleid en regelgeving op dit gebied is volop in ontwikkeling, zowel nationaal als Europees. Derhalve kunnen effecten of consequenties ervan nog niet allemaal volledig worden geschetst.

2. De initiatiefnota

De initiatiefnemers vragen aandacht voor zorgen over privacy in relatie tot big data in de financiële sector. Zij stellen dat de financiële sector vanwege zijn essentiële functie over privacygevoelige gegevens beschikt: iedereen heeft een bankrekening en verzekeringen en daarbij is het onvermijdelijk dat bepaalde persoonsgegevens worden gedeeld. Het is van essentieel belang dat deze gegevens ordentelijk worden verwerkt, veilig worden bewaard en niet (zomaar) met anderen worden gedeeld. De initiatiefnemers hebben de verwachting dat big data zich binnen de financiële sector op een vijftal manieren zal ontwikkelen:

1. analyse van klantpatronen;
2. intensiever monitoren van klanten;
3. koppelen van verschillende bronbestanden;
4. binnen het raamwerk van de herziene richtlijn betaaldiensten (Payment Services Directive II of 'PSD2') meer data delen tussen verschillende partijen; en

[1] Kamerstukken II, 2016/17, 34 616, nr. 2.

5. nieuwe spelers treden toe tot de betaalmarkt.

Deze ontwikkelingen zetten - volgens de initiatiefnemers - privacy in toenemende mate onder druk. De zorgen van initiatiefnemers zijn dat profilering – dat is het indelen van klanten op basis van aangeleverde data in een bepaalde groep - kan leiden tot discriminatie en uitsluiting. Verder zijn zij bezorgd dat datalekken de privacy en autonomie van burgers kunnen aantasten en dat privacy iets voor uitsluitend welgestelden kan worden, omdat er een prijskaartje komt te hangen aan diensten waarin de persoonsgegevens adequaat worden beschermd.

Huidige regelgeving en zelfregulering (zoals gedragscodes) zijn volgens initiatiefnemers niet toereikend om deze problemen op te lossen. De primaire verantwoordelijkheid voor bescherming van privacy ligt op dit moment te veel bij de burger zelf, zo stellen zij. Burgers hebben namelijk weinig tot geen inzicht in de mate waarin hun persoonsgegevens door bedrijven worden verwerkt. Burgers geven vaak gemakkelijk toestemming aan privacyvoorwaarden zonder deze - grondig - te lezen. En zelfs bij grondige bestudering is veelal niet duidelijk waarvoor uiteindelijk toestemming is verleend en wat bedrijven materieel mogen met de data. Daarnaast zijn burgers zich misschien wel bewust van de rechten die zij hebben, maar is het voor elk individu te tijdrovend om voor deze rechten op te komen. Ook is de handhaving van de privacywetgeving door de toezichthouder op dit moment niet afdoende volgens de initiatiefnota.

De initiatiefnemers stellen het volgende voor:

1. *Data mogen niet voor andere doeleinden gedeeld worden dan binnen het kader van PSD2, en dan alleen met ondubbelzinnige toestemming van de klant. Buiten de kaders van PSD2 gaat een verbod gelden op het delen van persoonsgegevens voor zowel banken als verzekeraars. Deze data hebben financiële instellingen verkregen op basis van hun nutsfunctie.*

2. *Ook data die gedeeld worden in het kader van PSD2 met derde partijen (de zogenaamde payment initiation services of account information services) mogen door deze partijen niet verder gedeeld worden. Dit willen wij Europees regelen.*

3. *Bij het gebruik van data in de financiële sector moet het principe van 'surprise minimization' als uitgangspunt gelden. Klanten mogen niet worden verrast. Data mogen niet voor andere doeleinden worden gebruikt dan de klant redelijkerwijs kan en mag verwachten. Hier moet streng op worden toegezien.*

4. *Privacy statements moeten helder en overzichtelijk zijn. Hiervoor dient de sector in overleg met de Autoriteit Persoonsgegevens (AP) een standaard op te zetten.*

5. *Klanten moeten kunnen kiezen in welke gradatie ze data willen delen. Het moet voor klanten mogelijk worden om op basis van opt-outs bepaalde type data wel of niet te delen met financiële instellingen.*

6. *Klanten moeten gemakkelijk inzicht kunnen verkrijgen in de data die door financiële instellingen over hen zijn verzameld.*

7. *De zorgplicht voor financiële instellingen moet worden uitgebreid. Automatische besluitvorming mag niet alleen voor eigen gewin worden ingezet. Klanten moeten geïnformeerd worden wanneer op basis van automatische besluitvorming een beslissing is genomen. Financiële instellingen moeten er zorg voor dragen dat automatische besluitvorming plaats vindt op basis van redelijke gronden.*

8. *De AP moet beter worden toegerust op de verantwoordelijkheden die volgen uit de ontwikkelingen met betrekking tot big data, privacy, en aankomende Europese wetgeving zoals PSD2 en de Algemene verordening gegevensbescherming (AVG)*.[2]

9. *De minister moet bewerkstelligen dat de verschillende toezichthouders (Autoriteit Consument en Markt (ACM), de Autoriteit Financiële Markten (AFM), de AP en De Nederlandsche Bank (DNB) meer gaan samenwerken en informatie delen.*

10. *De minister moet op Europees niveau de problemen met het Europees paspoort voor financiële instellingen aan de kaak stellen om te voorkomen dat er in Nederland via de achterdeur partijen privacywetgeving omzeilen.*

3. Regelgeving

Voor een reactie op de voorstellen van de initiatiefnemers is relevant te bezien wat al geregeld is in wetgeving. Belangrijk in dit kader is de op 27 april 2016 in EU-verband aangenomen Algemene Verordening Gegevensbescherming (AVG). De AVG vervangt vanaf 25 mei 2018 de nu nog geldende EU-privacyrichtlijn,[3] die in Nederland onder meer is geïmplementeerd in de Wet bescherming persoonsgegevens (Wbp).

De Wbp regelt de verwerking van persoonsgegevens in verticale (overheids-(rechts)personen) en horizontale (tussen (rechts)personen onderling) verhoudingen en dus ook voor de financiële sector.[4] Verwerking is een ruim begrip. Met verwerking wordt onder meer bedoeld *het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens*. Kort gezegd: alles wat je met gegevens 'doet'.

[2] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119).
[3] Richtlijn nr. 95/46/EG van het Europees Parlement en de Raad van de Europese Unie van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEG L 281).
[4] Leidraad afstemmen van wetgeving op de Wbp, 26: Artikel 8 EVRM en artikel 10 Grondwet werken door in de rechtsverhoudingen tussen burgers onderling.

Rechtmatige verwerking kan alleen plaatsvinden indien de verwerking steunt op één van de zes wettelijk bepaalde verwerkingsgronden. In de financiële sector zijn de drie belangrijkste verwerkingsgronden: ondubbelzinnige toestemming, noodzakelijk voor de uitvoering van een overeenkomst en noodzakelijk voor het nakomen van een wettelijke plicht. Met ondubbelzinnige toestemming wordt bedoeld dat bij de verantwoordelijke elke twijfel dient te zijn uitgesloten over de vraag of de betrokkene zijn toestemming heeft gegeven. Als er twijfel is of de betrokkene zijn toestemming heeft verleend, dient de verantwoordelijke te verifiëren of hij er terecht vanuit gaat dat de betrokkene heeft ingestemd. Indien in algemene voorwaarden wordt bepaald welke gegevens er voor welk doel en door wie worden verwerkt, wil dat nog niet automatisch zeggen dat betrokkene daartoe ondubbelzinnig zijn toestemming heeft gegeven, enkel omdat hij de betreffende overeenkomst heeft ondertekend. In zo'n geval is meer vereist. De verantwoordelijke zal de betrokkene duidelijk moeten wijzen op de betreffende bepalingen in de algemene voorwaarden. Verder mogen persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. Verdere verwerking die niet verenigbaar is met dit doel is niet toegestaan. Ook mogen gegevens niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor ze zijn verzameld. De betrokkene heeft onder meer het recht op inzage in de van hem verwerkte persoonsgegevens, het recht op verbetering van zijn gegevens indien deze feitelijk onjuist zijn en een recht van verzet.

Op 27 april 2016 is de AVG vastgesteld.[5] Deze is vanaf 25 mei 2018 van toepassing in de lidstaten en treedt in de plaats van de Privacyrichtlijn die wordt ingetrokken.[6] Aangezien de AVG rechtstreekse werking heeft in de Nederlandse rechtsorde, mogen nationaal geen regels gesteld worden die overlappen dan wel in strijd zijn met bepalingen uit de AVG. De AVG komt voor een groot deel overeen met hetgeen in de Privacyrichtlijn is geregeld en verduidelijkt en verscherpt een aantal bestaande normen. Zo is sprake van een wijziging in het territoriale toepassingsbereik, zijn de rechten van de betrokkene uitgebreid en zijn ook de verplichtingen en het toepassingsbereik daarvan uitgebreid, bijvoorbeeld de rechtstreeks werkende verplichting betreffende *privacy by design and by default*.

Met de AVG is een wettelijk kader voor de gehele EU in het leven geroepen. Dat is een goede basis voor gegevensbescherming. Relevant voor de effectiviteit is dat de normen daadwerkelijk worden nageleefd door burgers en bedrijven. De naleving van de veelal open normen uit de Wbp en AVG kan op verschillende manieren worden bevorderd. De initiatiefnemers bepleiten specifieke maatregelen voor de financiële sector vanwege het specifieke karakter van de sector en specifieke problemen die zich voordoen in de financiële sector en dan in het bijzonder bij verzekeringen en in het betalingsverkeer. Het wettelijk kader, in het bijzonder de AVG, biedt evenwel al adequate waarborgen. Dat wordt hieronder toegelicht.

[5] De Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) 4.5.2016 PbEU L119/1

[6] De AVG is gebaseerd op artikel de in artikel 16, tweede lid, VWEU nieuw gecreëerde rechtsgrondslag voor het stellen van voorschriften betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens (en dus niet meer op een rechtsgrondslag betreffende de werking van de interne markt).

4. Kabinetsvisie op big data in de private sector

Het kabinet baseert zich voor deze visie, in aanvulling op het regelgevend kader, op twee bronnen. Ten eerste het kabinetsstandpunt over het rapport van de WRR 'Big data in een vrije en veilige samenleving'[7] waarin het kabinet een aantal beleidsuitgangspunten heeft geformuleerd over big data in het veiligheidsdomein.[8] Daarbij kunnen onderdelen van de reactie behalve voor de overheid ook voor de private sector betekenis hebben. Bedrijven/sectoren die als verantwoordelijken voor gegevensverwerking kunnen worden aangemerkt, dienen actief invulling te geven aan deze beleidsuitgangspunten. Daarbij kan gedacht worden aan het ontwikkelen van begrijpelijke en effectieve privacy statements en het ontwikkelen en toepassen van *privacy by design and by default*. Het ontwikkelen van gedragscodes op sectorniveau kan daarbij behulpzaam zijn.

De tweede bron betreft het rapport van de *High Level Expert Group Big Data en Privacy* dat in 2016 gereed is gekomen. Daarin wordt specifiek ingegaan op de betekenis voor de private sector.[9] De rol van de overheid met betrekking tot de ontwikkeling van big data en privacy in de private sector is erop gericht evenwicht te bewaren tussen het benutten van de kansen van innovatie en het bewaken van de publieke belangen voor zover daaromtrent risico's en zorgen bestaan. De nadruk wordt daarbij gelegd op de noodzaak van verantwoord innoveren. Anders zal de effectiviteit en legitimiteit van innovatie ter discussie komen te staan.

Genoemd rapport schetst de technologische ontwikkeling. Exponentiële groei van gegevens, toename van de rekencapaciteit en ontwikkeling van intelligente adaptieve systemen bieden enorme kansen maar brengen ook risico's met zich mee. De *High Level Expert Group Big Data en Privacy* had als opdracht 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 met het behoud van vertrouwen van de samenleving in innovatieve ontwikkelingen. Het rapport geeft een overzicht van de belangrijkste bepalingen van de Algemene Verordening Gegevensbescherming (AVG). De expertgroep beveelt aan om dialogen binnen sectoren te organiseren waarin uitdagingen worden besproken. De overheid kan participeren in dit soort dialogen. Het rapport constateert ook dat de verwerking van gegevens zo complex kan zijn dat het moeilijk is om aan betrokkenen inzicht te geven in de werking ervan. De expertgroep beveelt daarom aan meer kennis te ontwikkelen van de effecten van kunstmatige intelligentie en zelflerende systemen op de bejegening van individuen.

Het zorgvuldig omgaan met big data door bedrijven draagt bij aan het vertrouwen dat nodig is om de kansen van big data op lange termijn te kunnen blijven benutten. In een omgeving die zich bewuster wordt van privacyrisico's ziet het kabinet ook concurrentievoordelen voor bedrijven die zorgvuldig omgaan met persoonsgegevens. Belangrijke randvoorwaarden voor het vertrouwen in het gebruik van big data door overheid en bedrijven zijn controle van de burger over zijn

[7] Wetenschappelijke Raad voor het Regeringsbeleid, *Big Data, privacy en veiligheid*, (Den Haag, 2016).
[8] Kamerstukken II, 2016/17, 26 643, nr. 426, p. 7-10.
[9] High level expert Group (2016), Licht op de digitale schaduw , Verantwoord innoveren met big data.

gegevens, transparantie over gegevensverwerking en het nemen van verantwoordelijkheid door bedrijven. Tot de verantwoordelijkheid van bedrijven en overheid hoort ook het bewuster maken van consumenten.

Al met al acht het kabinet het voor de financiële sector van groot belang dat verschillende sectoren, banken, verzekeraars en overige financiëledienstverleners werk maken van het effectief maken van de normen zoals die in de regelgeving zijn (en worden) neergelegd. Dit kan door middel van zelfregulering, zoals gedragscodes. Ook biedt de AVG de mogelijkheid van het aanstellen van een functionaris gegevensbescherming bij verwerkingsverantwoordelijke instellingen. In bepaalde gevallen, zoals wanneer de verwerkingsverantwoordelijke of de verwerker hoofdzakelijk is belast met verwerkingen op grote schaal, is het instellen van een functionaris gegevensbescherming op grond van de AVG zelfs verplicht. Het kabinet verwacht dat financiële instellingen aan beide invulling geven.

Er is een gedragscode op basis van het huidige wettelijk kader.[10] Ter implementatie van de verordening zullen aanpassingen nodig zijn. Verzekeraars en banken zijn al geruime tijd bezig met de voorbereiding van de implementatie van de AVG. Het Verbond van Verzekeraars geeft aan dat het een gedragscode ontwikkelt voor de verzekeringssector. Daarnaast heeft het Verbond van Verzekeraars ook een Solidariteitsmonitor ontwikkeld. Deze is erop gericht te voorkomen dat verdergaand gegevensgebruik tot onverzekerbaarheid leidt. De banken geven aan te wachten op meer duidelijkheid over invulling van normen in de AVG door de wetgever, voordat zij besluiten tot het al dan niet ontwikkelen van een nieuwe gedragscode. Het kabinet juicht zelfregulering toe, zoals de ontwikkeling van genoemde gedragscodes, zal dit waar mogelijk faciliteren en zal hierover met banken het gesprek aangaan.

5. Reactie op de voorstellen in de initatiefnota

Voorstel 1: *Data mogen niet voor andere doeleinden gedeeld worden dan binnen het kader van Payment Service Directive 2 (PSD2), en dan alleen met ondubbelzinnige toestemming van de klant.*

Voorstel 2: *Ook data die gedeeld wordt in het kader van PSD2 met derde partijen (de zogenaamde payment initiation services of account information services) mogen door deze derde partijen niet verder gedeeld worden.*

In het kader van PSD2 mogen betaaldienstverleners alleen met uitdrukkelijke toestemming van de betaaldienstgebruiker toegang krijgen tot persoonsgegevens die noodzakelijk zijn voor het verrichten van hun betaaldiensten. Daarnaast is de AVG onverkort van toepassing. Dit betekent dat de AVG ook van toepassing is op het verder delen van persoonsgegevens waartoe een (nieuwe) betaaldienstverlener - met uitdrukkelijke toestemming van de klant – toegang heeft gekregen. Als een betaaldienstgebruiker toestemming verleent voor het verder delen, dan is dat pas toegestaan indien aan de daarvoor geldende voorwaarden van de AVG is voldaan. Dat betekent ook dat een betaaldienstgebruiker zijn toestemming voor het verlenen van toegang of verder delen van zijn

[10] https://www.nvb.nl/publicaties/gedragscodes/1934/gedragscode-verwerking-persoonsgegevens-financiele-instellingen.html

gegevens te allen tijde kan intrekken. Deze intrekking moet volgens de AVG even gemakkelijk zijn als het verlenen van toestemming. Het is aan betaaldienstverleners om te zorgen dat dit ook daadwerkelijk mogelijk is.

Voorstel 1: *Buiten de kaders van PSD2 gaat een verbod gelden op het delen van persoonsgegevens voor zowel banken als verzekeraars.*

Het algemene kader wordt gegeven door de AVG en bijzondere bepalingen zijn opgenomen in PSD2. Hiermee worden eisen gesteld aan banken en verzekeraars. Een verbod bovenop de Europees geharmoniseerde eisen van de AVG en PSD2 is niet nodig en niet mogelijk gelet op het beoogde gelijk speelveld voor dataverwerkers (waaronder banken). Een absoluut verbod op verwerking van persoonsgegevens door een specifieke groep verantwoordelijken is een verregaande maatregel die geen recht doet aan de belangenafweging die steeds moet worden gemaakt. Voor die belangenafweging biedt de AVG, ook buiten de kaders van de PSD2, een adequaat kader. In dit kader is het ook verplicht dat financiële instellingen een functionaris gegevensbescherming instellen, indien er sprake is van een verwerkingsverantwoordelijke of de verwerker die hoofdzakelijk is belast met verwerkingen op grote schaal.

Voorstel 3: *Bij het gebruik van data in de financiële sector moet het principe van 'surprise minimization' als uitgangspunt gelden. Klanten mogen niet worden verrast. Data mogen niet voor andere doeleinden worden gebruikt dan de klant redelijkerwijs kan en mag verwachten. Hier moet streng op worden toegezien.*

Voorstel 4: *Privacy statements moeten helder en overzichtelijk zijn. Hiervoor dient de sector in overleg met de Autoriteit Persoonsgegevens een standaard op te zetten.*

Het uitgangspunt van 'surprise minimization' vloeit reeds voort uit het ook al in de huidige privacyrichtlijn en in de AVG gehanteerde beginsel dat persoonsgegevens niet voor een ander doel mogen worden verwerkt dan waarvoor ze zijn verzameld, tenzij hiervoor een rechtsgrondslag aanwezig is, zoals toestemming van de betrokkene (artikel 5, eerste lid, onderdeel b, AVG). Als die er niet is en ook geen sprake is van een wettelijke bepaling die dit rechtvaardigt, is verwerking van persoonsgegevens voor een ander doel dan waarvoor deze zijn verzameld mogelijk, mits het andere doel verenigbaar is met het doel waarvoor de gegevens zijn verzameld (artikel 6, vierde lid, AVG). Voor de beantwoording van de vraag of dat het geval is, bevat de AVG, evenals thans de Wbp, een aantal criteria. Volgens rechtsoverweging 50 bij de AVG spelen hierbij ook de verwachtingen van betrokkenen inzake de verwerking voor het andere doel een rol. Gelet hierop is het belangrijk dat verwerkingsverantwoordelijken transparant zijn over de doelen waarvoor persoonsgegevens van klanten worden verwerkt, zodat klanten ook precies weten waarvoor zij toestemming geven (geïnformeerde toestemming) en zo nodig ook hun rechten kunnen uitoefenen. Primair ligt hier een rol voor de verwerkingsverantwoordelijke. Overigens is dit een voorbeeld van een onderwerp waar op Europees niveau nog bindende richtsnoeren verwacht worden. Het kabinet wil bezien of dit in Nederland binnen de bestaande wettelijke kaders nader vormgegeven kan worden in dialoog tussen toezichthouders en sector.

Verder kunnen persoonsgegevens onder meer verwerkt worden op grond van een wettelijke verplichting. De verwerking moet in dat geval noodzakelijk zijn om te voldoen aan de wettelijke verplichting van de verwerkingsverantwoordelijke. Bij zo'n wettelijke verplichting kan gedacht worden aan een expliciete verplichting om bepaalde persoonsgegevens te verwerken, maar kan ook een ruimer geformuleerde zorgplicht zijn. Een verwerkingsverantwoordelijke heeft in dat geval een grotere eigen verantwoordelijkheid bij het beoordelen van de noodzaak van de verwerking in het licht van het voldoen aan de wettelijke verplichting. De vraag welke verwerkingsdoelen precies onder deze zorgplicht vallen en welke verwerkingen van persoonsgegevens precies noodzakelijk zijn voor deze doelen laat zich niet in zijn algemeenheid te beantwoorden. Door de financiële sector op te stellen gedragscodes zijn de meest aangewezen manier om daarover duidelijkheid te geven. De AVG draagt lidstaten op om te bevorderen dat gedragscodes worden opgesteld die moeten bijdragen tot de juiste toepassing van deze verordening, onder andere op het punt van een behoorlijke en transparante gegevensverwerking.[11] Het kabinet moedigt de financiële sector dan ook aan om op korte termijn werk te maken van het opstellen van gedragscodes, waarin op dit punt duidelijkheid wordt geboden dan wel om reeds bestaande gedragscodes hierop aan te passen. Gelet op het belang hiervan is de minister van Financiën bereid om daarbij een actief ondersteunende rol te vervullen als daar behoefte aan bestaat. De Autoriteit Persoonsgegevens heeft met de AVG de opdracht gekregen om zelfregulering op dit vlak te bevorderen.

Voorstel 5: *Klanten moeten kunnen kiezen in welke gradatie ze data willen delen. Het moet voor klanten mogelijk worden om op basis van opt-outs bepaalde type data wel of niet te delen met financiële instellingen.*

Voorstel 6: *Klanten moeten gemakkelijk inzicht kunnen verkrijgen in de data die door financiële instellingen over hen zijn verzameld.*

Het kabinet kan zich vinden in de strekking van deze voorstellen. Er is evenwel misschien meer mogelijk dan opt-outs. De verantwoordelijke financiële onderneming zou dit in de sfeer van *privacy by design* kunnen regelen. Een *privacy dashboard* lijkt daarbij een interessante optie. De klant heeft daarmee overzicht en kan ook keuzes maken welke data wel en welke niet gedeeld worden. In bepaalde gevallen zou een expliciete instemming van de klant mogelijk beter passen (een opt-in). Dergelijke opties kunnen het vertrouwen in gegevensverwerking in belangrijke mate ondersteunen. In het huidige kader is deze verplichting met een open norm geregeld, die uitnodigt tot invulling na sectorale dialogen en op basis van zelfregulering. Als dat niet tot goede uitkomsten leidt, kan worden overgegaan tot invulling van de open norm door de toezichthouder. Dit is niet de voorkeursoptie van het kabinet. Immers, niet alle financiële ondernemingen willen of kunnen dit op dezelfde manier regelen. Overigens wordt ook in Europees verband aan richtsnoeren gewerkt. Dat maakt het ontwikkelen van nationale oplossingen nu niet opportuun.

Voorstel 7: *De zorgplicht voor financiële instellingen moet worden uitgebreid. Automatische besluitvorming mag niet alleen voor eigen gewin worden ingezet. Klanten moeten geïnformeerd worden wanneer op basis van automatische besluitvorming een*

[11] Artikel 40 AVG en overwegingen 98-99.

beslissing is genomen. Financiële instellingen moeten er zorg voor dragen dat automatische besluitvorming plaats vindt op basis van redelijke gronden.

De AVG omarmt dit voorstel (zie artikel 22 en overwegingen 71-72 AVG). Uit de AVG volgt – kort gezegd - dat geautomatiseerde besluitvorming op basis van persoonlijke gegevens is toegestaan, mits sprake is van menselijke tussenkomst. Geautomatiseerde besluitvorming waaraan voor de betrokkene rechtsgevolgen zijn verbonden of die hem anderszins in aanmerkelijke mate treft, is in beginsel verboden (artikel 22, eerste lid, AVG). Uitzonderingen op dit verbod zijn 1) indien het noodzakelijk is voor de totstandkoming of uitvoering van een overeenkomst, 2) in geval van uitdrukkelijke toestemming van de betrokkene en 3) als dit uitdrukkelijk is toegestaan in een wettelijke bepaling (artikel 22, tweede lid, AVG). Onder laatstgenoemde wettelijke bepaling kan ook een wettelijk bepaalde zorgplicht vallen doch deze dient wel voldoende specifiek te zijn. Bij de onder 1) en 2) genoemde uitzonderingen moet de verwerkingsverantwoordelijke bovendien passende maatregelen treffen ter bescherming van de rechten, vrijheden en gerechtvaardigde belangen van de betrokkene (artikel 22, derde lid, AVG), waaronder specifieke informatie aan de betrokkene.

Voorstel 8: De Autoriteit Persoonsgegevens moet beter worden toegerust op de verantwoordelijkheden die volgen uit de ontwikkelingen met betrekking tot big data, privacy, en aankomende Europese wetgeving zoals PSD2 en de Europese privacy verordening.

De Autoriteit Persoonsgegevens wordt beter toegerust met het oog op de verantwoordelijkheden die uit de AVG voortvloeien. Daartoe wordt het huidige budget van de Autoriteit Persoonsgegevens voor 2018 verhoogd met vijf miljoen euro en met ingang van 2019 met nog eens twee miljoen euro, zodat de totale verhoging neerkomt op zeven miljoen euro en daarmee op bijna een verdubbeling van het huidige budget.

Voorstel 9: De minister moet bewerkstelligen dat de verschillende toezichthouders (ACM, AFM, AP, DNB) meer gaan samenwerken en informatie delen.

De Autoriteit Financiële Markten, De Nederlandsche Bank, de Autoriteit Persoonsgegevens en de Autoriteit Consument en Markt krijgen bij het toezicht op financiële instellingen taken die aan elkaar raken. Een voorbeeld is het toezicht op de herziene richtlijn betaaldiensten (PSD2). Andere voorbeelden zijn het toezicht op een integere bedrijfsvoering door de AFM en DNB, dat raakt aan toezicht op de verwerking van persoonsgegevens en toezicht op het gebied van concurrentie en marktwerking. De minister van Financiën is verantwoordelijk voor goed functionerende financiële markten. Hiervoor is goed toezicht een voorwaarde. Als taken elkaar raken moet voor alle betrokkenen duidelijk zijn wie welke bevoegdheden en verantwoordelijkheden heeft en hoe deze zijn 'verdeeld' om zowel overlap als lacunes te voorkomen. In het verlengde hiervan ligt samenwerking en het hebben van mogelijkheden om informatie uit te wisselen. Afspraken hierover zijn nuttig en noodzakelijk ter beperking van administratieve lasten en ter voorkoming van 'dubbele' handhaving of het uitblijven van handhaving. Een actueel dossier dat vraagt om samenwerking tussen de AFM, DNB, de ACM en de Autoriteit Persoonsgegevens (AP), is het toezicht op PSD2. Deze richtlijn wordt geïmplementeerd onder verantwoordelijkheid van de minister van Financiën en de minister van Veiligheid en Justitie. De minister van Financiën

faciliteert momenteel overleg met genoemde toezichthouders over samenwerking voor het toezicht op PSD2. Het kabinet wil de samenwerking van de toezichthouders in de financiële sector over uiterlijk vier jaar evalueren.

Voorstel 10: De minister moet op Europees niveau de problemen met het Europees paspoort voor financiële instellingen aan de kaak stellen om te voorkomen dat partijen in Nederland via de achterdeur privacywetgeving omzeilen.

Dit raakt het principe van de interne markt waar ook de AVG aan beoogt bij te dragen. De AVG is er op gericht een Europees speelveld te regelen. Het voorstel behelst een fundamenteel andere koers dan tot nu toe gevolgd door Nederland met betrekking tot de ontwikkeling van de Europese interne markt. De minister van Financiën heeft er in zijn reactie op de consultaties van zowel de mid-term review kapitaalmarktunie als de review van de Europese Toezichthoudende Autoriteiten op aangedrongen dat Europees toezicht op financiële instellingen effectief wordt georganiseerd, bijvoorbeeld waar het gaat om instellingen die met paspoorten grensoverschrijdend diensten verlenen.

6. Conclusie

Het Europese kader dat is geschapen met de AVG geldt onverkort voor de financiële sector. Het kabinet acht specifieke maatregelen in Nederland door verdere regulering van de verwerking van persoonsgegevens in de financiële sector niet nodig en onwenselijk. Het kabinet ondersteunt daarbij wel de ratio van de voorstellen van de initiatiefnemers en ziet in de uitwerking daarvan een rol voor zich van regisseur. Die regie kan zich richten op twee taken: a) samen met de toezichthouders (ACM, AFM, AP, DNB) bezien of er wat betreft het toezicht op de naleving van regels over gegevensgebruik sprake is van overlap, lacunes en te overbruggen interpretatieverschillen inzake bevoegdheden en verantwoordelijkheden – een en ander gericht op effectieve samenwerking, en b) samen met de financiële sector de regels te effectueren in de vorm van gedragscodes en de sector daarbij faciliteren.