Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

34 616 Initiatiefnota van de leden Oosenbrug en Nijboer over de financiële sector en big data

Nr. 2 **INITIATIEFNOTA**

Inhoudsopgave

1. Voorstellen

1.1. Beslispunten

I. *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. 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.*

II. *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 derde partijen niet verder gedeeld worden. Dit willen wij Europees regelen.*

III. *Bij het gebruik van data in de financiële sector moet het principe van «surprise minimization» als uitgangspunt gelden. Klanten mogen niet*

kst-34616-2
ISSN 0921 - 7371
's-Gravenhage 2016

worden verrast. Data mogen niet voor andere doeleinden worden gebruikt dan de klant redelijkerwijs kan en mag verwachten. Hier moet streng op worden toegezien.

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

V. *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.*

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

VII. *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.*

VIII. *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.*

IX. *De Minister moet bewerkstelligen dat de verschillende toezichthouders (ACM, AFM, AP, DNB) meer gaan samenwerken en informatie delen.*

X. *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.*

De Kamer wordt gevraagd in te stemmen met deze aanbevelingen.

1.2. Financiële consequenties

Er zijn geen budgettaire effecten.

Inleiding

1.1. Aanleiding van deze initiatiefnota

Recentelijk liet onderzoek door het Maatschappelijk Overleg Betalingsverkeer (MOB) zien dat een groot deel van de Nederlanders de verkoop van betaalgegevens door banken en verzekeraars niet acceptabel vindt.[1] Ophef omtrent een dergelijk initiatief door ING weerhield deze bank al van verdere stappen in die richting. Eerder deed betalingsverwerker Equens het voorstel om betaalgegevens te analyseren en voor commerciële partijen beschikbaar te maken. Dat plan was na massieve publieke kritiek snel weer van de baan. Ook de recentelijk aangekondigde verzekering van de ANWB die klanten die veilig rijden kortingen aanbiedt leidde tot discussie.[2]

Deze ontwikkelingen vallen onder wat ook wel *big data* analyse genoemd wordt: het verwerken en analyseren van grote hoeveelheden persoonsgegevens om op basis daarvan assumpties te maken over klanten. Big data analyse onderscheidt zich van traditionele analyses in termen van snelheid van verwerking en hoeveelheid en verscheidenheid van verzamelde data.

---

[1] MOB Rapportage 2015.

[2] https://www.nrc.nl/nieuws/2016/06/18/verzekeren-met-grote-precisie-2768326-a1505902

Deze ontwikkelingen bieden grote kansen aan bedrijven en overheden en daarom is er in een groot aantal sectoren een toename te zien van het gebruik van big data. Ook in de financiële sector is er een enorme toename te zien van big data analyse. Dit biedt grote mogelijkheden om de dienstverlening van financiële instellingen aan klanten te verbeteren, bijvoorbeeld omdat betere risicoanalyses gemaakt kunnen worden. Tegelijkertijd hebben de initiatiefnemers zorgen over de manier waarop data gebruikt worden. Door bovengenoemde ophef is de financiële sector vooralsnog voorzichtig met de verkoop van betaaldata. Toch is er reden tot zorg en is een actieve houding als wetgever gewenst.

De initiatiefnemers zijn van mening dat voorkomen moet worden dat de samenleving over enkele jaren voor voldongen feiten staat. Zo zorgt de komst van de Payments Services Directive 2 (PSD2) ervoor dat de betaalgegevens van consumenten gedeeld kunnen worden met derden, overal in Europa. De banklicenties die Facebook en Google hebben aangevraagd in Ierland tonen aan dat dit soort bedrijven meer en meer interesse hebben in betaalgegevens. Tot slot blijkt uit voorbeelden in Verenigde Staten dat banken al op grote schaal persoonsgegevens voor klant-specifieke marketing gebruiken.

1.2. Doel en strekking van de initiatiefnota

De initiatiefnemers vinden dat iedereen moet kunnen beschikken over een zeker niveau van privacy, ongeacht afkomst, interesse in de materie of inkomensniveau. Het is aan de overheid om die privacy te beschermen. Daarnaast vinden de initiatiefnemers dat niet elk type persoonsgegeven zomaar gedeeld mag worden. In die context zijn de initiatiefnemers van mening dat er in het bijzonder meer aandacht moet zijn voor de datavergaring en -gebruik in de financiële sector. Deze sector vervult een essentiële functie in onze economie en beschikt mede daardoor over bijzonder grote hoeveelheden privacygevoelige gegevens: om mee te kunnen doen in de samenleving heeft iedereen immers een bankrekening en verzekeringen nodig. Bij het hebben van een bankrekening en verzekering hoort dat bepaalde persoonsgegevens overgedragen worden. Het is dus van groot belang dat deze gegevens ordentelijk worden verwerkt, veilig worden bewaard en niet met anderen worden gedeeld. De initiatiefnemers zijn zich ervan bewust dat deze ontwikkelingen zich niet alleen in de financiële sector voordoen, maar dat ook in andere sectoren vergelijkbare vraagstukken opdoemen. Dit stelt de samenleving en politiek voor fundamentele vragen over de omgang met big data door bedrijven en overheden. Tegelijkertijd zijn er tussen verschillende sectoren dusdanige verschillen dat een discussie op sectoraal niveau nodig blijft. Daarom strekt deze initiatiefnota ertoe om het debat over het gebruik van big data door de financiële sector preciezer te voeren.

In deze nota zal positie worden genomen in de discussie aangaande big data in de financiële sector. De nota zal verschillende bedreigingen bespreken alsmede beperkingen in de huidige wet- en toezichtkaders. De initiatiefnemers zijn zich er ten zeerste van bewust dat big data voordelen voor mensen kunnen opleveren, maar trachten met deze nota te bewerkstelligen dat de privacy beschermd blijft. Hiertoe doen zij een aantal voorstellen.

2. Probleemstelling

2.1. Persoonsgegevens als product

In de nabije toekomst zou het zo maar kunnen dat wanneer een klant boodschappen doet bij de Albert Heijn, deze direct bij thuiskomst een whatsapp-bericht van een andere supermarkt ontvangt met een aanbieding om de volgende keer tegen korting de boodschappen daar te doen. Tegelijkertijd stuurt de zorgverzekeraar een e-mail dat deze klant op basis van recente aankopen is aangemerkt als «gezonde eter», en daarom in aanmerking komt voor een korting op de premie. Wel pech dat de autoverzekeraar via een mobiele applicatie heeft geconstateerd dat de klant in kwestie te hard gereden heeft op de terugweg van de supermarkt: de premiekorting op de autoverzekering van deze maand komt te vervallen.

Op dit moment lopen er in Nederland en buitenland al verschillende initiatieven die aansluiten op bovenstaand verhaal. Zo biedt Bank of America klanten in de VS kortingen aan op basis van hun betaalgegevens via zogenaamd *transaction-based marketing*.[3] Op basis van eerdere aankopen, biedt deze bank klanten specifieke aanbiedingen. Eenzelfde voorstel door ING in Nederland leidde eerder tot grote ophef.[4] Verder biedt de ANWB premiekortingen aan voor veilige rijders, via een datakastje die op basis van locatiegegevens de rijstijl analyseert. Op dit moment worden nog niet op grote schaal data gedeeld tussen verschillende partijen, maar het valt te verwachten dat dit in de zeer nabije toekomst meer gaat gebeuren.

Bedrijven zullen beargumenteren dat zij klanten specifieke aanbiedingen kunnen doen. Consumenten zullen de kortingen die hen geboden worden wellicht aantrekkelijk vinden. Als klanten zelf kunnen kiezen voor het delen van betaalgegevens, wat is het probleem dan? De vraag is echter in hoeverre klanten in deze daadwerkelijk een keuze hebben. De verleidingen van hoge kortingen maken dat klanten er soms eigenlijk niet omheen kunnen om hun privacy op te geven voor gunstige aanbiedingen. Vanuit consumenten heerst er op dit moment een dubbelzinnig sentiment wat betreft big data en privacy. Enerzijds blijkt uit onderzoeken van het MOB dat een groot deel van de Nederlandse bevolking zich zorgen maakt over de commerciële exploitatie van betaalgegevens door verkoop aan derden. Ook laat publieke ophef omtrent de proef van ING om data te delen met derden zien hoe gevoelig dit onderwerp ligt. Anderzijds stemmen consumenten gemakkelijk in met allerlei voorwaarden in mobiele apps die bedrijven beschikking geven over hoogst persoonlijke data, zoals contact- en locatie gegevens. Er bestaat dus een grote kans dat ook met betaalgegevens een grotere mate van gewenning zal optreden, waardoor consumenten er – al dan niet bewust – voor kiezen om deze te delen. Privacy is een glijdende schaal, waarbij eenmaal gedeeld er geen mogelijkheid is om gedane zaken terug te draaien. Eenmaal publiek wordt informatie nooit meer privaat. Er is geen weg terug.

De initiatiefnemers zijn van mening dat voorkomen moet worden dat grote hoeveelheden betaaldata massaal gedeeld gaan worden. De overheid heeft een verantwoordelijkheid om hier een leidende rol in te nemen. Privacy is geen individueel goed, integendeel, het is een grondrecht dat alleen gewaarborgd blijft wanneer er binnen de samenleving

---

[3] Zie bijvoorbeeld BankofAmerideals, https://promotions.bankofamerica.com/deals/.
[4] https://www.nrc.nl/nieuws/2014/03/10/ing-start-proef-met-delen-betalingsgedrag-klanten-a1426630

keuzes worden gemaakt over wat wel en onder welke specifieke voorwaarden; en wat niet gedeeld en gebruikt mag worden.

Privacy is niet te koop en zou dat ook niet moeten zijn.

2.2. Big data in de financiële sector

De financiële sector is van oudsher een zeer data-gedreven sector. Geen wonder dus dat big data toepassingen ook hier een grote vlucht nemen. Vooralsnog is de sector nog voorzichtig met het delen van data met derde partijen. Tegelijkertijd laten de recente voorbeelden van ING en ANWB zien dat er wel degelijk een neiging is om meer met big data te gaan doen. Daarnaast heeft de financiële sector nog te maken met een zogenoemde *legacy*: een veelvoud aan oude datasystemen die niet op elkaar aansluiten. Dit maakt het combineren en analyseren van data niet alleen ingewikkeld, maar ook risicovol. Ook zien we de opkomst van zogenoemde «datagraaiers.» Dit zijn bedrijven die gespecialiseerd zijn in het verzamelen, bundelen en analyseren van klant-specifieke data die vervolgens verkocht kunnen worden aan financiële partijen, bijvoorbeeld voor het beoordelen van de kredietwaardigheid van een klant.

Zoals reeds gesteld zijn datavergaring en -analyse geen nieuwe activiteit binnen de financiële sector. Banken maken al decennia gebruik van modellen om de risico's van investeringen in te schatten. Ook binnen de verzekeringsbranche geldt dat goede inschattingen van risico's van essentieel belang zijn voor de correcte beprijzing ervan. De huidige ontwikkelingen zijn in die zin dus niet bijzonder. Wel onderscheiden de ontwikkelingen met big data zich in termen van de hoeveelheid, variatie aan data die verzameld worden en de snelheid waarmee vervolgens verwerking en analyse plaatsvindt. Dit stelt bedrijven in staat om veel sterkere assumpties te maken over klantgedrag.[5]

2.3. Toekomstige ontwikkelingen voor financiële sector

De initiatiefnemers hebben de verwachting dat big data zich op een vijftal manieren verder zal ontwikkelen binnen de financiële sector: 1) door analyse van klantpatronen; 2) door het intensiever monitoren van klanten; 3) en door het koppelen van verschillende bronbestanden. Daarnaast valt te verwachten dat binnen het PSD2-raamwerk 4) meer data gedeeld gaan worden tussen verschillende partijen, en 5) dat er nieuwe spelers intrede op de betaalmarkt zullen gaan doen.

Ten eerste kunnen financiële instellingen op basis van big data klantpatronen beter blootleggen. Een recentelijk voorbeeld komt van een Amerikaanse bank die via big data analyse bevond dat mensen die kredietaanvragen met hoofdletters invullen gemiddeld vaker betalingsachterstanden hebben.[6] Door dit soort analyses neemt de kans toe op discriminatie op basis van observeerbare karakteristieken. Klanten worden op basis van aangeleverde data ingedeeld in een bepaalde groep, het zogenoemde *profiling*. Het gevaar daarbij is dat observeerbare karakteristieken correleren, maar in werkelijkheid niet verklarend zijn. Hierdoor ontstaat de kans dat bepaalde groepen in de samenleving uitgesloten worden van diensten op basis van ongefundeerde aannames. Bijvoorbeeld wanneer een kredietaanvraag of verzekering alleen wordt afgewezen op basis van het postcodegebied waarin een klant woont. Een

---

[5] Zie van der Sloot en van Schendel, International and Comparative Legal Study on Big Data, p. 15.

[6] https://www.washingtonpost.com/business/zestfinance-issues-small-high-rate-loans-uses-big-data-to-weed-out-deadbeats/2014/10/10/e34986b6–4d71–11e4-aa5e-7153e466a02d_story.html

vraag die daarnaast speelt is in hoeverre het mogelijk is in latere fases nog van zo'n profiel af te komen. Hierbij spelen ook eerdergenoemde datagraaiers een rol die financiële instellingen uitgebreide klantprofielen kunnen aanbieden.[7] Het kan voorkomen dat klanten op basis van hun instagram en facebook profielen bepaalde diensten worden geweigerd.

Op zich is er natuurlijk niets mis mee dat bedrijven zoveel mogelijk informatie meenemen bij het beoordelen van aanvragen. De initiatiefnemers zijn echter wel van mening dat klanten altijd beoordeeld moeten worden op basis van rationale afwegingen en dat klanten volledig inzicht moeten krijgen in de overwegingen die aan deze besluitvorming ten grondslag liggen. Dat algoritmes kunnen bijdragen aan afgewogen besluitvorming is prima, maar klanten moeten hier ten alle tijden van op de hoogte zijn en een beslissing kunnen aanvechten. Net als dat bankmedewerkers aan strenge eisen zijn verbonden bij het toekennen van kredieten, moet ook het beleid met betrekking tot automatische besluitvorming aan de hoogste eisen voldoen. De initiatiefnemers zijn van mening dat de sector hier een actieve rol in moet spelen.

Ten tweede kunnen klanten in de toekomst intensiever gemonitord worden. Een voorbeeld is de polis van de ANWB waarbij veilige rijders 30% korting krijgen op een premie. Klanten geven de bank of verzekeraar ruim inzicht in de persoonlijke levenssfeer, in ruil zijn bedrijven in staat om klanten specifieker te bedienen. Een grote zorg met betrekking tot de financiële sector is dat klanten in toenemende mate verleid worden om privacy in te ruilen voor lagere prijzen. Privacy is dan te koop. Hierdoor dreigt een tweedeling in de samenleving. Hogere inkomens kunnen zich permitteren om hun privacy te waarborgen terwijl lagere inkomens gedwongen worden privacy op te geven in ruil voor een lagere premie. Wat de initiatiefnemers betreft moet er voor iedereen een minimum niveau van privacy gewaarborgd blijven, ongeacht inkomensniveau. Daarnaast vinden de initiatiefnemers dat iedereen toegang moet hebben tot bepaalde voorzieningen. Ook als iemand ervoor kiest geen persoonlijke informatie te willen delen.

Ten derde zullen financiële instellingen verschillende typen data meer kunnen gaan koppelen. Op dit moment hebben met name grote partijen te maken met veel verschillende en oude systemen, de bovengenoemde *legacy*. Dit bemoeilijkt een goede aansluiting van verschillende databestanden. Verwacht wordt dat deze koppeling in de toekomst meer en meer zal plaatsvinden. De initiatiefnemers zijn van mening dat het koppelen van data voor intern gebruik allerlei voordelen kan opleveren. Zo kan een bank op basis van deze analyse een klant stimuleren spaargeld bij te storten om rood staan te voorkomen. Dit kan de klant kostenbesparingen opleveren. Ook maakt big data analyse bijvoorbeeld fraudedetectie een stuk gemakkelijker. De initiatiefnemers vinden dat deze analyse altijd in het belang moet zijn van de klant. Er moet ook hier een zorgplicht gelden voor banken. De initiatiefnemers zijn van mening dat deze systemen niet alleen ingericht mogen worden, opdat financiële instellingen er zelf profijt van hebben.

Ten vierde zullen verschillende partijen onderling meer data gaan delen, vrijwillig, of op commerciële basis. Hierbij kan enerzijds gedacht worden aan een bank die klantdata verkoopt aan marketing bedrijven die hier vervolgens zeer specifieke reclame mee kunnen ontwikkelen. Anderzijds zien de initiatiefnemers een belangrijke rol voor de datagraaiers: bedrijven die gespecialiseerd zijn in het verzamelen van grote hoeveelheden data. In toenemende mate zien we het ontstaan van een wholesale markt voor

[7] Zie bijvoorbeeld http://www.experian.nl/zakelijke-dienstverlening/zakelijke-dienstverlening.html

klant-specifieke data. De initiatiefnemers zijn tegen de verkoop van data door financiële instellingen. Data die op basis van een nutsfunctie zijn vergaard, mogen wat betreft de initiatiefnemers niet gedeeld worden. De initiatiefnemers zijn van mening dat met name banken en verzekeraars, door hun bijzondere positie in de economie, een veel grotere datamacht hebben dan andere bedrijven. Doormiddel van betaaldata is het mogelijk om in vergaande mate inzicht te krijgen in het leven van een klant. Zelfs wanneer deze data anoniem gedeeld worden, blijkt dat het nog altijd zeer gemakkelijk is om te achterhalen om welke betreffend individu het gaat. Ook vinden de initiatiefnemers dat financiële instellingen die data uit andere bronnen vergaren de klant hier volledig inzicht in moeten geven. Vanuit dit perspectief zijn de initiatiefnemers van mening dat er te veel onduidelijk bestaat omtrent de datagraaiers. Uit onderzoeken blijkt dat zij een grote rol spelen in de dataeconomie. Deze bedrijven bezitten grote hoeveelheden data van klanten en verkopen deze door aan bedrijven, bijvoorbeeld voor het beoordelen van de kredietwaardigheid van een klant. Onduidelijk is welke rol deze bedrijven spelen in de Nederlandse financiële sector, en in welke mate zij in het algemeen conformeren aan de privacy wetgeving.[8]

Door alle ophef zijn met name banken op dit moment voorzichtig geworden met het delen van data met derden. Nieuwe Europese wetgeving (PSD2) biedt echter de ruimte aan derde partijen om betaaldata te gaan gebruiken voor bijvoorbeeld het uitvoeren van betalingen. Vraag is of dit soort bedrijven even voorzichtig zullen zijn met de data van klanten. De verkoop is immers erg lucratief en wanneer een klant eenmaal toestemming geeft kan en mag er veel. Een zorg is dat persoonsgevoelige informatie terecht komt in databases in andere landen in Europa, waar wellicht niet voorzichtig wordt omgegaan met deze informatie. Binnen de kaders van PSD2 mogen klanten er nu zelf voor kiezen deze data te delen. De initiatiefnemers maken zich zorgen over de veiligheid van deze bestandsoverdracht. De initiatiefnemers verwijzen naar de problemen die nu optreden met het Europees paspoort voor financiële instellingen met bepaalde beleggingsproducten waarbij toezichthouders met handen en voeten gebonden zijn omdat autorisatie plaatsvindt in een andere Europese lidstaat. De initiatiefnemers zijn van mening dat hierdoor de kans op datalekken toeneemt. Zo kunnen bijvoorbeeld de uitgavenpatronen of salarissen van Nederlanders op straat komen te liggen. Naast dat deze datalekken het vertrouwen in het financieel systeem kunnen ondermijnen, speelt ook de vraag welke partij in de betaal- of informatieketen verantwoordelijk zal zijn in geval van een datalek. De vergelijking met IceSave doemt hier op. Ook toen werden Nederlandse autoriteiten verantwoordelijk gesteld voor het falen van buitenlandse toezichthouders.

De problematiek omtrent PSD2 laat tevens het internationale karakter van de huidige ontwikkelingen met big data zien. Servers van financiële instellingen met data van Nederlandse klanten kunnen overal op de wereld geplaatst worden, het internet kent wat dat betreft geen grenzen. Enerzijds vraagt dit van de Nederlandse politiek en toezichthouders om ervoor te waken dat de privacy gewaarborgd blijft, ook wanneer data in een ander land worden opgeslagen. Anderzijds vereist dit ook dat op Europees en internationaal niveau meer wordt samengewerkt tussen verschillende toezichthouders. Het is in die zin positief dat de aankomende Europese privacy verordening voorziet in verdere harmonisatie tussen de privacy wetgeving in verschillende lidstaten.

[8] Zie bijvoorbeeld «Je hebt wél iets te verbergen» van Maurits Martijn en Dimitri Tokmetzis.

Tot slot zien we dat mede met dank aan wet- en regelgeving nieuwe spelers hun intrede zullen doen op de bancaire markt. Enerzijds zijn dit spelers die op basis van bijvoorbeeld PSD2 inspringen op behoeftes vanuit de markt. Anderzijds zien we ook dat bedrijven als Facebook en Google wellicht hun intrede op de Europese bankenmarkt doen. De initiatiefnemers zijn van mening dat de intrede van nieuwe spelers positieve effecten op het Nederlandse financiële landschap kan hebben. Wel zijn de initiatiefnemers bezorgd over de zorgvuldigheid waarmee deze partijen om zullen gaan met de data van Nederlandse klanten. De initiatiefnemers zijn voorts van mening dat er meer discussie moet komen over de Europese paspoortconstructie en de gevolgen voor privacy bij invoering van PSD2.

De initiatiefnemers zijn van mening dat bovenstaande ontwikkelingen de privacy in toenemende mate onder druk zetten. Daarnaast hebben de initiatiefnemers zorgen over de gevolgen van aankomende Europese wetgeving en de gevolgen voor de bescherming van persoonsgegevens. Tot slot zijn de initiatiefnemers van mening dat deze nieuwe ontwikkelingen niet tot gevolg mogen hebben dat privacy een handelsgoed wordt. Het mag nooit zo zijn dat alleen de welgestelden zich privacy kunnen permitteren.

3. Wettelijk- en toezichtskader

3.1. Bestaan wettelijk- en toezichtskader

Persoonsgegevensbescherming is op dit moment in Nederlandse wet geregeld via de Wet Bescherming Persoonsgegevens (WBP). De WBP is van toepassing op elke vorm van gegevensverwerking en geldt dus ook voor de financiële sector. De WBP kent een aantal belangrijke bepalingen die ingaan op bovengenoemde zorgen met betrekking tot het gebruik van persoonsgegevens. [9]

Art. 8 legt voorwaarden vast op basis waarvan gegevens verwerkt mogen worden. Verwerking vereist «ondubbelzinnige toestemming» van de betrokkene; en moet noodzakelijk zijn (in het geval van de financiële sector) voor de uitvoering van een overeenkomst of het nakomen van wettelijke verplichting. Art.9 legt vast dat de verwerking verenigbaar moet zijn met de doeleinden waarvoor de gegevens zijn verkregen. Art. 13 stelt dat persoonsgegevens afdoende beveiligd dienen te worden. Art. 27 schrijft voor dat automatische besluitvorming wordt gemeld aan de Autoriteit Persoonsgegevens (AP). Artikel 33 en 34 leggen vast dat een betrokkene geïnformeerd zal worden wanneer gegevens verzameld worden, ook wanneer dat gedaan wordt via andere bronnen dan de klant zelf. Verder kunnen betrokkenen op basis van artikel 35 en 36 eisen dat gegevens veranderd of verwijderd worden. Tot slot verplicht art. 42 een organisatie een betrokkene mede te delen welke logica ten grondslag ligt aan automatische besluitvorming. Hiermee dekt de WBP dus een groot aantal mogelijke inbreuken op privacy af.

Art. 25 van het WBP opent ook de mogelijkheid voor organisaties of sectoren om een door de Autoriteit Persoonsgegevens (AP) goedgekeurde gedragscode op te stellen. De financiële sector heeft ook zo'n gedragscode. Voor een groot deel bestendigt deze gedragscode de provisies uit de WBP. Tegelijkertijd biedt de gedragscode financiële instellingen ook expliciet ruimte voor bepaalde vormen van gegevensverwerking.

[9] http://wetten.overheid.nl/BWBR0011468/2016-01-01

3.2. Rol van Autoriteit Persoonsgegevens

De WBP dicht de Autoriteit Persoonsgegevens (AP), voorheen het College Bescherming Persoonsgegevens, een aantal taken toe. De AP heeft de verantwoordelijkheid om gedragscodes te toetsen, onderzoek te doen naar gegevens verwerking en mogelijke overtredingen, en klachten van burgers te behandelen. Daarnaast houdt het AP sinds 2016 meldpunt datalekken bijhouden. Verder heeft het AP sinds 2016 de mogelijkheid om boetes op te leggen die kunnen oplopen tot 10% van de jaaromzet.[10]

3.3. Toekomstig wettelijk kader

Daarnaast is er Europese wetgeving op komst die ook van invloed is op de manier hoe de financiële sector om kan gaan met persoonsgegevens. Dit gaat om de Europese privacy verordening, en bovengenoemde PSD2.[11]

PSD2 is een nieuwe Europese richtlijn die per januari 2018 een aantal zaken regelt omtrent het betalingssysteem, maar ook specifieke bepalingen bevat aangaande het delen van privacygevoelige informatie met derden. Belangrijkste in de context van deze initiatiefnota zijn de regels betreffende *payment initiation services* en de *account information services*. PSD2 opent de betaalmarkt en stelt derde partijen in staat om beide type activiteiten te gaan ontplooien. Payment initiation services zoals het Duitse sofort voeren transacties tussen klant en bedrijf uit. Account information services krijgen toegang tot betaalgegevens van klanten en kunnen hen op basis daarvan meer inzicht in financiën verschaffen. Het belangrijkste aspect is de mogelijkheid voor deze bedrijven om Europa-wijd de opereren. De autorisatie van deze dienstverleners gebeurt nationaal. Art. 11 van PSD2 stelt dat lidstaten de mogelijkheid hebben om betaaldienstverleners de autoriseren. Hiermee breekt PSD2 dus de betaalmarkt open, en vraagt zij van banken om inzicht te verschaffen (na toestemming van de klant) in de betaalrekening.

Ten tweede zal de privacy verordening in 2018 de WPB vervangen en geharmoniseerde vereisten opleggen wat betreft de verwerking van persoonsgegevens.[12] Voor Nederland zal deze wetgeving slechts beperkt van invloed zijn omdat de meeste provisies reeds in de Nederlandse wet zijn verankerd (in de WBP). Wel is de verordening op bepaalde vlakken specifieker wat betreft vereisten. Zo stellen art. 13 en 14 van de verordening dat bedrijven een informatieplicht hebben bij elke vorm van informatiegaring, zij het direct, zij het indirect. Een nieuw aspect is art. 35 dat van bedrijven vraagt om voor de inzet van een nieuwe technologie de impact hiervan voor persoonsgegevens te onderzoeken. Tot slot legt de verordening de taken en verantwoordelijkheden van nationale toezichtsorganen vast. Ook hier heeft de verordening geen grote impact op de Nederlandse situatie.

Lacunes in bestaande wetgeving

Deze zorgen met betrekking tot vergaande datavergaring, profiling, uitsluiting, en data lekken worden reeds in de wet behandeld en geregeld. Ook legt de wet, in combinatie met de gedragscode, enige verantwoordelijkheid bij financiële instellingen om klanten actief te informeren. Toch biedt het wettelijk kader erg veel ruimte om maar zo veel mogelijk data te

---

[10] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN

[11] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_van_de_autoriteit_persoonsgegevens_van_15_december_2015.pdf

[12] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf

verzamelen wanneer beargumenteerd kan worden dat de vergaring doelmatig is. Hierdoor biedt het huidige raamwerk onvoldoende bescherming. Bovendien is de handhaving van privacywetgeving op dit moment niet afdoende. Daarbij zij opgemerkt dat dit ook een uiterst moeizame zaak is, waarbij de vraag zelfs is in hoeverre handhaving van deze wetgeving in de online samenleving überhaupt mogelijk is.

De initiatiefnemers zijn van mening dat de verantwoordelijkheid voor bescherming van privacy op dit moment te veel bij de burger ligt. Burgers zijn eigenhandig niet in staat om hun rechten voldoende de waarborgen. De initiatiefnemers stellen dat hierdoor een grote informatie-asymmetrie is ontstaan tussen de burger en bedrijven. Burgers hebben weinig tot geen inzicht in de mate waarin hun persoonsgegevens door bedrijven worden verwerkt. Zij geven vaak gemakkelijk toestemming aan privacy-voorwaarden zonder deze grondig te lezen. Maar ook bij grondige bestudering is veelal niet duidelijk waarvoor nu uiteindelijk toestemming is verleend en wat bedrijven materieel vermogen met de data.

Daarnaast zijn burgers zich wellicht bewust van de rechten die zij hebben, maar is het voor elk individu te tijdrovend om voor deze rechten op te komen. De initiatiefnemers zijn van mening dat juist deze informatie-asymmetrie ervoor zorgt dat privacy voor grote bedrijven een afvinklijstje wordt waarbij, na toestemming van de betrokkenen, zoveel mogelijk data worden verzameld. Daarom moet er een grotere verantwoordelijkheid komen te liggen bij financiële instellingen om consumenten actief te informeren, alsmede bij de AP om hard tegen overtredingen op te treden. Daarnaast moeten consumenten de keuze hebben om informatie ook meer gradueel te delen.

Voortvloeiend uit het bovenstaande doen de initiatiefnemers in volgende paragrafen een aantal voorstelen die ertoe strekken het wetgevend- en toezichtskader met betrekking tot privacy in de financiële sector sterken.

4. Delen van persoonsgevoelige informatie

De initiatiefnemers zijn van mening dat financiële instellingen data verkrijgen op basis van hun nutsfunctie in de samenleving. Niemand kan immers zonder bankrekening en enkele verzekeringen. De initiatiefnemers zijn voorts van mening dat de gegevens van de klant zijn en daarom niet mogen worden gedeeld met derde partijen. Daarnaast zijn de initiatief-nemers van mening dat ook op Europees niveau gewaarborgd dient te worden dat data die gedeeld worden binnen het kader van PSD2 alleen voor die doeleinden worden gebruikt. De initiatiefnemers zijn van mening dat als algemeen uitgangspunt moet gelden dat dataverwerking voor de klant een transparant proces is. Dit valt samen te vatten in de term «surprise minimization»: de klant mag niet worden verrast.[13] De verwerking van persoonsgegevens moet voldoen aan de verwachtingen van de klant.

I. *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. 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.*
II. *Ook data die gedeeld worden in het kader van PSD2 met derde partijen (de zogenaamde payment initiation services of account*

[13] Zie bijvoorbeeld https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/speech_big_data_nationale_denktank_versie_3_okt_2014_website.pdf.

information services) mogen door deze derde partijen niet verder gedeeld worden. Dit willen wij Europees regelen.

III. *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.*

5. Gebruik van data en informatieplicht

Voor individuen is het ondoenlijk om inzicht te krijgen in alle gegevens die door financiële instellingen worden verzameld. De initiatiefnemers zijn daarom van mening dat een actieve houding van financiële instellingen gevraagd mag worden ten aanzien van informatie over gegevensverzameling en automatische besluitvorming. Daarnaast zijn de initiatiefnemers van mening dat privacyvoorwaarden op dit moment onoverzichtelijk zijn. Met één druk op de knop geven klanten toestemming voor de verzameling van grote hoeveelheden data. De initiatiefnemers zijn van mening dat klanten de mogelijkheid moeten krijgen om bepaalde typen data niet te delen.

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

V. *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.*

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

VII. *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.*

6. Rol van de Autoriteit Persoonsgegevens

Eerder gaven de initiatiefnemers al aan dat er behoefte is aan tegenmacht. Het vertrouwen op het individu leidt ertoe dat privacy van burgers onvoldoende gewaarborgd blijft. Privacy is een grondrecht en verdient daarom voldoende bescherming vanuit de overheid. Privacy mag nooit te koop zijn. Daarnaast vragen de ontwikkelingen met betrekking tot big data meer en meer van de AP. De initiatiefnemers willen bewerkstelligen dat het AP beter in staat is om privacy principes die zijn vastgelegd in de wet te beschermen. De AFM heeft gevraagd om meer samenwerking op het gebied van privacy tussen toezichthouders mogelijk te maken. De initiatiefnemers zijn van mening dat dit verzoek gehonoreerd moet worden.[14] Hierdoor kan een samenhangende aanpak van het privacyvraagstuk bereikt worden.

VIII. *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.*

IX. *De Minister moet bewerkstelligen dat de verschillende toezichthouders (ACM, AFM, AP, DNB) meer gaan samenwerken en informatie delen.*

[14] Zie AFM wetgevingsbrief 2016.

7. Passporting

Onder andere in het geval van beleggingsproducten zoals de binaire opties en contracts-for-difference hebben we gezien dat er bedrijven in Nederland actief zijn die met agressieve verkooptechnieken zeer risicovolle beleggingsproducten aanbieden. De AFM is met handen en voeten gebonden in de aanpak van deze bedrijven omdat zij in Nederland actief zijn via een Europees paspoort constructie. Met de komst van PSD2 bestaat ook het risico dat derde partijen die actief zijn vanuit andere Europese landen payment initiation services, of account information services gaan aanbieden, maar daarbij minder strikte privacy principes naleven dan die in Nederland gangbaar zijn. De initiatiefnemers vinden daarom dat de Minister de Europese paspoort constructie in Europa ter discussie moet stellen. Passporting leidt tot veel problemen inzake bepaalde financiële diensten, en zal ook in de toekomst problemen veroorzaken met betrekking tot dienstverleners die betaaldiensten gaan uitvoeren in het kader van PSD2.

X. *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.*

8. Conclusies

Technologische ontwikkelingen kunnen in potentie grote voordelen opleveren. De voortschrijdende rekenkracht van computers maakt dat grote hoeveelheden en verschillende typen data razendsnel geanalyseerd worden. Financiële instellingen zullen door deze technologie steeds beter in staat zijn om risico's in te schatten. Ook biedt de grootschalige analyse van persoonsgegevens hen de kans om klanten specifieker en beter te bedienen. De initiatiefnemers zijn voorstander van het gebruik van deze technologieën ten gunste van de klant.

Tegelijkertijd zet grootschalige verzameling van persoonsgegevens de privacy van burgers in toenemende mate onder druk. Van klanten wordt gevraagd in vergaande mate inzicht te geven in hun persoonsgegevens. Vanuit hun nutsfunctie zijn bijvoorbeeld banken en verzekeraars als vanzelfsprekend reeds in bezit van grote hoeveelheden zeer specifieke klantdata. Deze data zijn commercieel zeer aantrekkelijk en mede hierom zien we dat bijvoorbeeld banken in de VS deze data al veelvuldig delen met derden. Deze data zijn echter verkregen vanuit de nutsfunctie en mogen wat de initiatiefnemers betreft nooit commercieel worden gebruikt.

Hoewel wet- en regelgeving in Europa bescherming biedt tegen de meeste vormen van datamisbruik, zijn er teveel mogelijkheden om grote hoeveelheden data te verzamelen en te gebruiken. We zien dat hierdoor de privacy onder druk staat. De wet wordt bovendien onvoldoende gehandhaafd. Ook beweegt nieuwe Europese wetgeving, PSD2, juist de kant op van meer datadeling. Dit brengt grote, nieuwe risico's mee voor burgers.

Deze nota strekt ertoe de privacy van burgers te beschermen via een aantal maatregelen. De initiatiefnemers beogen niet om elke vorm van datagebruik in de kiem te smoren. Deze nota strekt om de discussie over het gebruik van data in en door de financiële sector in te kaderen. Privacy is een grondrecht. Dat recht verdient publieke bescherming. Eenmaal publiek gemaakte gegevens, worden nooit meer privaat. Eenmaal openbaar is er geen weg terug. Dat vergt een actieve overheid, heldere

regels, eenduidige keuzes voor burgers en handhaving bij overtreding. Bovendien dienen data veilig bewaard en beheerd te worden.

Om te voorkomen dat de privacy van mensen onvoldoende wordt geborgd willen de initiatiefnemers een aantal zaken per wet regelen. Ten eerste willen de initiatiefnemers bewerkstelligen dat de overheid voldoende tegenmacht creëert om privacy van burgers beter te waarborgen en namens de burger opkomt voor de rechten die vastgelegd zijn in de wet. Hiermee waarborgt zij dat burgers rechtvaardig behandeld worden en voorkomt zij dat het overmatig gebruik van big data leidt tot uitsluiting, discriminatie, en ongelijkheid. Tevens beogen de initiatiefnemers bepaalde vormen van datagebruik in de financiële sector in te perken. Data verkregen vanuit de nutsfunctie mogen niet commercieel worden gebruikt. Tot slot vragen de initiatiefnemers een actieve houding van de financiële sector zelf.

Oosenbrug
Nijboer