Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

34 813 Wijziging van de Wet op het financieel toezicht, de Wet bekostiging financieel toezicht, het Burgerlijk Wetboek en de Wet handhaving consumentenbescherming ter implementatie van richtlijn nr. 2015/2366/EU van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PbEU 2015, L 337) (Implementatiewet herziene richtlijn betaaldiensten)

Nr. 11 **NOTA NAAR AANLEIDING VAN HET VERSLAG**

Ontvangen 20 juni 2018

Aanleiding

Het kabinet is de vaste commissie voor Financiën erkentelijk voor de aandacht die zij het onderhavige wetsvoorstel heeft geschonken en voor de door haar daarover gestelde vragen. Deze vragen worden, mede namens de Minister voor Rechtsbescherming, beantwoord in de volgorde van het door de commissie uitgebrachte verslag. Voor zover vragen, vanwege overeenkomst in onderwerp, gezamenlijk beantwoord zijn, is dit vermeld.

Inleiding

1) De leden van de SP-fractie zien dat ten tijde van de behandeling van de richtlijn en het aannemen ervan een sentiment was dat de positie van banken – als het gaat om data – gebroken of doorbroken moest worden en dat het aspect van privacy van burgers niet voldoende heeft meegewogen. Deze leden vragen hoe de regering dit ziet. Zij vragen voorts hoe de regering reflecteert op het feit dat we inmiddels, door schade en schande, meer kennis hebben van risico's die volgen uit hacks, leaks of het verhandelen van data van burgers voor criminele doeleinden. Zij willen weten of deze risico's voldoende onderkend worden volgens de regering.

De regering onderkent dat onder meer door de opkomst van internet en mobiele betalingen sprake is van een toename van potentiële veiligheidsrisico's. Het gaat hierbij om risico's, zoals fraude met betaalkaarten, en phishing. Dit is een belangrijke aanleiding geweest voor het uitbrengen

kst-34813-11
ISSN 0921 - 7371
's-Gravenhage 2018

van richtlijn 2015/2366/EU van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2313/36/EU en Verordening (EU) nr. 1093–2010 en houdende intrekking van Richtlijn 2007/64/EG (hierna: PSD II of de richtlijn). Met het oog hierop bevat PSD II voor vergunningverlening voor het verlenen van betaaldiensten extra eisen op het gebied van beveiliging, zoals de verplichting om over een beveiligingsbeleid te beschikken en maatregelen te nemen om fraude en illegaal gebruik van gevoelige (persoons)gegevens te voorkomen. Tevens wordt sterke cliëntauthenticatie geïntroduceerd als één van de maatregelen om de veiligheid van het betalingsverkeer te vergroten. Er is sprake van sterke cliëntauthenticatie indien authenticatie plaatsvindt met gebruikmaking van minimaal twee factoren die onderling onafhankelijk van elkaar zijn. Deze onafhankelijkheid garandeert dat als één van de factoren onbetrouwbaar blijkt te zijn, dit niet automatisch leidt tot onbetrouwbaarheid van de andere factor. Authenticatie met minder dan twee, of door middel van van elkaar afhankelijke factoren, wordt daarom niet aangemerkt als sterke cliëntauthenticatie. Daarnaast geldt een groot aantal aanvullende eisen om de veiligheid van de data van burgers te beschermen tijdens uitwisseling en verwerking, zoals de eis dat er niet meer gegevens mogen worden verwerkt dan de gegevens die nodig zijn om de betaaldienst te kunnen verlenen. Tevens worden de risico's beperkt door de ingevolge PSD II opgestelde technische standaarden over sterke cliëntauthenticatie, waarin de voorwaarden zijn opgenomen voor toegang tot de betaalrekening. Hierin is bijvoorbeeld geregeld dat een rekeninginformatiedienstverlener niet langer dan 90 dagen toegang mag hebben tot de betaalrekening voordat de betaaldienstgebruiker opnieuw uitdrukkelijke toestemming moet geven.

2) De leden van de SP-fractie willen verder weten waarom de regering het belangrijk vindt dat onder PSD II ieder bedrijf dat online actief is, toegang kan vragen tot iemands betaalrekening. Zij vragen zich af wat de toegevoegde waarde is voor burgers en of dit opweegt tegen de nadelen. Deze leden vragen verder of er onafhankelijk onderzoek bekend is over dit onderwerp en of de regering de mening deelt dat het prudent is om onderzoek te doen alvorens het parlement instemt met de inwerkingtreding van dit gedeelte van PSD II.

Het wetsvoorstel ter implementatie van PSD II leidt de ontwikkeling van innovatieve nieuwe betaaldiensten in goede banen, onder meer door het reguleren van verschillende betaaldiensten die zijn ontstaan na PSD I[1], zoals betaalinitiatiediensten en rekeninginformatiediensten. Een consument kan aan een betaalinitiatiedienstverlener de opdracht geven tot het uitvoeren van een betaling vanaf zijn rekening, bijvoorbeeld voor de afrekening van een product in een webwinkel. Een consument kan daarnaast een rekeninginformatiedienstverlener toegang geven tot de transactiegegevens van zijn betaalrekening(en). De rekeninginformatiedienstverlener kan deze gegevens bijvoorbeeld verzamelen en bundelen in een overzicht. De regulering van deze typen diensten – die werken op basis van toegang tot iemands rekening – kan leiden tot nieuwe klantgerichte en innovatieve oplossingen, zoals nieuwe betaalmogelijkheden of digitale huishoudboekjes. De consument zal hierdoor makkelijker, goedkoper en veiliger (grensoverschrijdende) betalingen kunnen doen en meer dan wel beter inzicht krijgen in zijn uitgaven en inkomsten (zie ook het antwoord op vraag 15). Naast voordelen brengen deze nieuwe betaaldiensten ook risico's met zich mee, met name voor de veiligheid van het betalingsverkeer. In zowel PSD II, het onderhavige wetsvoorstel als de

[1] Richtlijn nr. 2007/64/EG van het Europees Parlement en de Raad van de Europese Unie van 13 november 2007 betreffende betalingsdiensten in de interne markt (PbEU L 319).

Algemene Verordening Gegevensbescherming (hierna: de AVG) zijn waarborgen opgenomen om potentiële risico's effectief te ondervangen en is sprake van streng en doorlopend toezicht op betaaldienstverleners. Voorbeelden van waarborgen in PSD II en het wetsvoorstel zijn vermeld bij de beantwoording van vraag 1. Voorbeelden van waarborgen in de AVG zijn dat gegevens enkel mogen worden verwerkt voor bepaalde doelen (doelbinding). Dit betekent dat voor het gebruik van die gegevens voor andere doelen of voor het verder delen van die gegevens apart toestemming moet worden gegeven. Andere waarborgen zijn dat niet meer gegevens mogen worden verwerkt dan nodig voor het doel (gegevensminimalisering) en dat een verleende toestemming voor het verwerken van persoonsgegevens op elk moment kan worden ingetrokken.

De regering en de betrokken onafhankelijke toezichthouders erkennen zowel de voordelen als de genoemde risico's van het verlenen van toegang tot iemands rekening. Voor een onderzoek naar de afweging tussen de voordelen en risico's van PSD II verwijst de regering naar het impact assessment dat is uitgevoerd door de Europese Commissie.[2] In het algemeen geldt dat bij de totstandkoming van PSD II is gezocht naar een manier om innovatie van de betaaldienstverlening te stimuleren binnen de kaders van eisen die gelden op het gebied van veiligheid van het gebruik van betaaldiensten en consumentenbescherming. De regering is van mening dat met de waarborgen die zowel in PSD II, het wetsvoorstel als in de AVG worden geboden op het gebied van veiligheid en consumentenbescherming, de genoemde risico's zodanig worden beperkt dat deze niet opwegen tegen de genoemde voordelen.

3) De leden van de SP-fractie maken zich grote zorgen dat banken verplicht worden vanaf begin 2018 hun gegevens gratis te delen met zogenaamde Fintech-bedrijven, zij het met instemming van de rekeninghouder. Deze leden vragen of de regering vindt dat er geld mag worden verdiend aan bankgegevens.

Het staat vergunninghoudende marktpartijen, inclusief zogenaamde Fintech-bedrijven, binnen de bestaande juridische kaders vrij om een verdienmodel te baseren op het verlenen van betaaldiensten. Dat geldt ook voor de nieuwe betaalinitiatie- en rekeninginformatiediensten. Hiervoor geldt uiteraard dat bedrijven zich bij het gebruik van bankrekeninggegevens (veelal persoonsgegevens) moeten houden aan zowel de regelgeving ter implementatie van PSD II en de Wet bescherming persoonsgegevens (en vanaf 25 mei 2018 de AVG) alsook aan eventuele civiele contractuele bepalingen tussen bedrijf en rekeninghouder. PSD II bepaalt dat de betaaldienstgebruiker voor zowel de toegang tot de betaalrekening als voor de verwerking (inclusief toegang) van zijn persoonsgegevens uitdrukkelijk toestemming moet geven. Net als bij de AVG is bij PSD II het uitgangspunt dat de betaaldienstgebruiker de controle heeft over zijn (persoons)gegevens. De consument heeft waar het gaat om het verlenen van betaaldiensten de vrijheid om te bepalen van welke partijen hij gebruik wil maken, welke partijen hij toegang wil geven tot zijn betaalrekening en met wie hij zijn (betaal- en /of transactie)gegevens wil delen.

Overigens heeft de ACM in een recent onderzoek geconcludeerd dat het gratis toegang moeten verlenen tot prikkels voor banken leidt om Fintech-bedrijven uit te sluiten.[3] Banken zullen namelijk minder willen

[2] SWD/2013/0288.

[3] https://www.acm.nl/sites/default/files/documents/2017–12/acm-studie-fintechs-in-het-betalingsverkeer-het-risico-van-uitsluiting.pdf.

investeren in goede dienstverlening en systemen als zij niet de mogelijkheid hebben om die investeringen terug te verdienen. In haar rapport beveelt de ACM de EC aan om banken in staat te stellen een kostencompensatie te verlangen voor (ten hoogste) de kosten die zij moeten maken voor het toegang verlenen. De ACM zal de aanbevelingen in het rapport onder de aandacht brengen bij de hiervoor relevante partijen, waaronder de EC. Daarnaast gaat de ACM nauwlettend in de gaten houden of banken toegang verlenen aan Fintech-bedrijven. De ACM kan daarbij optreden tegen anti-competitief gedrag op basis van haar bevoegdheden op grond van de Mededingingswet. De regering kiest ervoor om de ontwikkelingen op het gebied van het verlenen van toegang door banken aan Fintech-bedrijven vooralsnog af te wachten en nu geen actie te ondernemen. Mocht voornoemde ontwikkeling zich inderdaad voordoen, dan beziet de regering of en zo ja welke actie hierop ondernomen moet worden.

4) De leden van de SP-fractie constateerden dat tijdens het rondetafelgesprek van 15 november 2017 experts niet weten wat de uitwerking zal zijn, niet duidelijk is wat zich gaat afspelen en dat de sector, toezichthouders en het Ministerie van Financiën niet klaar zijn voor de inwerkingtreding van deze richtlijn. Zij vragen de regering of zij bereid is de inwerkingtreding te vertragen totdat op zijn minst de bekende risico's afgedekt kunnen worden.

De sector en de toezichthouders bereiden zich op dit moment voor op de inwerkingtreding van de wetgeving ter implementatie van PSD II. Het is gebruikelijk dat partijen zich gedurende hun voorbereiding richten op de gecommuniceerde dan wel beoogde implementatiedatum. Aangezien afgelopen najaar bleek dat de implementatiewetgeving vertraagd is – en daarnaast ook duidelijkheid over de technische standaarden en richtsnoeren, zoals door de Europese Bankenautoriteit (EBA) zijn opgesteld, later beschikbaar is gekomen – zitten partijen nog in het proces van voorbereiding. Bij de omzetting van PSD II in Nederlandse wetgeving is grote zorgvuldigheid betracht en is veel aandacht geweest voor privacyaspecten en potentiële risico's. Zo heeft de afstemming over het toezicht op het vereiste van «uitdrukkelijke toestemming» voor de verwerking van persoonsgegevens veel tijd gekost. Inmiddels hebben de Autoriteit Persoonsgegevens (hierna: AP) en de Nederlandsche Bank (hierna: DNB) hierover duidelijke afspraken gemaakt en is wettelijk vastgelegd dat de AP hier toezicht op zal gaan houden. Dit is de voornaamste reden geweest voor de vertraging van het wetsvoorstel. Voor uitstel van inwerkingtreding zie ik geen aanleiding, te meer omdat Nederland gehouden is te zorgen voor een zo snel mogelijke omzetting van de richtlijn. Bij niet-tijdige implementatie kan de Europese Commissie (hierna: EC) het Europese Hof van Justitie tijdens een inbreukprocedure verzoeken om, naast een dwangsom, ook een boete op te leggen. Deze boete bedraagt voor Nederland ten minste 3,7 miljoen euro.

5) De leden van de SP-fractie vragen de regering in het kader van risicodekking, hoeveel en welke EU-lidstaten wel klaar zijn voor de implementatie van PSD II.

Op 13 januari 2018, de datum waarop de richtlijn dient te zijn geïmplementeerd in nationale wetgeving, waren naast Nederland nog negentien lidstaten niet op tijd klaar met de implementatie van PSD II in hun nationale wetgeving. Thans zijn nog tien lidstaten niet klaar met de implementatie. België, Bulgarije, Tsjechië, Denemarken, Duitsland, Estland, Ierland, Frankrijk, Italië, Cyprus, Hongarije, Malta, Oostenrijk, Slovenië, Slowakije, Finland, Zweden en het Verenigd Koninkrijk hebben op dit moment de implementatie afgerond. Nederland is inmiddels door

de EC in gebreke gesteld. De Nederlandse regering heeft twee maanden de tijd om haar opmerkingen over de termijnoverschrijding aan de EC kenbaar te maken.

6) De leden van de SP-fractie constateren overigens dat de Europese Commissie nog bezig is met het vaststellen van Europese standaarden. Deze leden vragen welke positie de Nederlandse regering in heeft genomen in de discussie over deze standaarden.

Op grond van de richtlijn heeft de Europese Bankautoriteit (EBA) de bevoegdheid om diverse voorstellen voor technische standaarden en richtsnoeren te ontwikkelen. De EBA doet dit in overleg met de nationale toezichthouders die bij EBA zijn aangesloten; voor Nederland is dit DNB. Vervolgens worden de technische standaarden voorgelegd aan de Raad en het Europese Parlement (EP), die bezwaar kunnen maken. Indien geen bezwaar wordt gemaakt, kan de technische reguleringsnorm in werking treden. Nederland kan eventuele bezwaren via de Raad kenbaar maken. Vooralsnog heeft de Nederlandse regering bij geen van de technische standaarden en richtsnoeren reden gezien om bezwaar aan te tekenen. Op grond van de richtlijn worden er in totaal vijf technische standaarden en zes richtsnoeren ontwikkeld. Twee technische standaarden zijn reeds in werking getreden in de vorm van een gedelegeerde verordening. Verder heeft de EBA kort geleden het definitieve ontwerp van twee andere technische standaarden gepresenteerd. De laatste technische standaard bevindt zich nog in de consultatiefase. Daarnaast heeft EBA voor vijf van de zes richtsnoeren een definitief ontwerp gepubliceerd. De laatste richtsnoer bevindt zich nog in de consultatiefase.

Algemeen

§1. Inleiding

7) De leden van de VVD-fractie zouden graag vernemen hoe PSD II zo techniekneutraal mogelijk wordt vormgegeven. Op welke wijze wordt voorkomen dat er over een aantal jaar een noodzaak bestaat voor PSD III, omdat de wetgeving achterloopt op de techniek? Welke mogelijkheden biedt PSD II flexibel in te springen op veranderende technologische mogelijkheden?

De definitie van betaaldienst in PSD II is technologieneutraal, zodat deze ruimte biedt voor de ontwikkeling van nieuwe soorten betaaldiensten. Dit komt tot uitdrukking in het feit dat met PSD II twee nieuwe betaaldiensten zijn toegevoegd aan de bijlage bij de richtlijn. Hierdoor hoeft de definitie van betaaldienst in de richtlijn en nationale wetgeving niet steeds te worden aangepast in geval de wens bestaat om nieuwe diensten als betaaldienst aan te merken. Nieuwe betaaldiensten zullen wel moeten worden opgenomen in bijlage 1 bij de richtlijn, waarin alle betaaldiensten worden opgesomd. De definitie van betaaldiensten kan echter ongewijzigd blijven indien een nieuwe betaaldienst via deze tabel onder de reikwijdte van de richtlijn wordt gebracht.

Verder zijn ook de technische standaarden en richtsnoeren zoveel mogelijk technologieneutraal geformuleerd. Daarbij heeft de Europese Commissie op een aantal deelonderwerpen gekozen voor een regelgevend kader, dat partijen zelf nader kunnen invullen. Deze kaders zijn zoveel mogelijk techniekneutraal vormgegeven. Dit betekent dat als de techniek verandert, de invulling kan wijzigen, maar dat het regelgevend kader niet aangepast hoeft te worden. Een voorbeeld hiervan is de manier waarop de toegang tot de betaalrekening technisch wordt vorm gegeven.

8) De leden van de VVD-fractie willen verder weten of deze wetgeving ook proportioneel is voor kleine aanbieders en of de mogelijkheid bestaat om te differentiëren en dus «too small to comply» tegen te gaan.

PSD II bepaalt eveneens dat controles proportioneel en passend moeten zijn en moeten aansluiten bij de risico's waaraan de betaaldienstverleners blootstaan. Kleinere ondernemingen, waarbij de risico's doorgaans kleiner zijn, hoeven aan minder strenge eisen te volden. Voor kleine betaaldienstverleners bestaat daarnaast de mogelijkheid van vrijstelling van de vergunningplicht.

In de Wft en lagere regelgeving is bepaald dat de bedrijfsvoering voor onder andere betaaldienstverleners is afgestemd op de aard, omvang, risico's en complexiteit van de financiële onderneming of bijkantoor. Verder hebben de toezichthouders hun toezicht risicogebaseerd ingericht.

9) De leden van de CDA-fractie vragen naar de totstandkoming van het advies van de Afdeling advisering van de Raad van State (de Afdeling). Heeft de regering om een spoedadvies gevraagd en zo ja, wat was de aanleiding hiervoor? Acht de regering het reëel en zorgvuldig dat de Afdeling in één dag een advies uitbrengt over een dergelijk omvangrijk wetsvoorstel?

10) Ook de leden van de GroenLinks-fractie vragen of de Afdeling voldoende gelegenheid heeft gehad om het wetsvoorstel te bestuderen.

Bij Kabinetsmissive van 3 oktober 2017 is het wetsvoorstel middels de reguliere procedure voor advisering voorgelegd aan de Afdeling advisering van de Raad van State. Dat de Afdeling reeds op 4 oktober een advies heeft uitgebracht is snel. Naast het feit dat een eerdere versie van het wetsvoorstel reeds openbaar is geconsulteerd, is gelet op de omvang en het belang van dit wetsvoorstel en de noodzaak van een spoedige implementatie, reeds in een vroegtijdig stadium contact gezocht met de Raad van State. De Raad van State heeft daarbij, vooruitlopend op de formele adviesaanvraag, reeds de beschikking gehad over het concept-wetsvoorstel en memorie van toelichting. Zoals ik in mijn brief van 23 oktober 2017 al heb aangegeven heeft de voorbereiding van het wetsvoorstel meer tijd gevergd dan was voorzien, waardoor pas laat advies is gevraagd aan de Afdeling. Ik heb geen enkele aanleiding te veronderstellen dat de Raad van State in haar beoordeling snelheid heeft laten prevaleren boven zorgvuldigheid.

11) De leden van de D66-fractie constateren dat de implementatiedatum niet behaald zal worden. De Nederlandsche Bank (DNB) heeft in het rondetafelgesprek van 15 november 2017 over PSD II gewaarschuwd dat dienstverleners hierdoor geneigd zullen zijn een vergunning in een ander land aan te vragen en dat hierdoor toezicht op deze dienstverleners wordt bemoeilijkt. Ziet de regering deze beweging naar andere EU-lidstaten ook? Deelt het kabinet de mening van DNB over het toezicht?

Indien een betaalinstelling in een andere lidstaat een vergunning aanvraagt, betekent dit dat haar hoofdkantoor zich in die lidstaat moet bevinden en dat ten minste een deel van haar dienstverlening in die lidstaat wordt uitgevoerd. Dit maakt het minder aantrekkelijk om uit te wijken naar een andere lidstaat. De consequentie van vestiging in een andere lidstaat is dat de betaalinstelling in die lidstaat onder toezicht komt te staan en moet voldoen aan de eisen die PSD II stelt. Het toezicht op betaaldienstverleners wordt met PSD II versterkt en geharmoniseerd. De harmoniserende werking die de implementatie van PSD II door de lidstaten met zich mee brengt, garandeert een bepaald (minimum)niveau

van eisen, waardoor het toezicht inhoudelijk in alle lidstaten aan dezelfde eisen gebonden is. De regering heeft vooralsnog geen signalen ontvangen dat betaaldienstverleners daadwerkelijk uitwijken naar andere lidstaten. Daarnaast stelt EBA een centraal register op, waarin alle vrijgestelde en vergunninghoudende partijen worden geregistreerd. PSD II maakt tevens mogelijk dat informatie kan worden uitgewisseld tussen toezichthouders. De regering meent dat PSD II voldoende voorwaarden bevat voor een goede samenwerking tussen toezichthouders, zodat het toezicht voortdurend gewaarborgd is.

12) De leden van de D66-fractie willen weten welke waarborgen er zijn om te verzekeren dat de kwaliteit van het toezicht tussen EU-lidstaten niet in die mate verschilt dat het voor aanbieders reden kan zijn een land te verkiezen waar toezicht als minder intensief kan worden ervaren?

Alle lidstaten zijn gehouden dezelfde richtlijnbepalingen van PSD II in nationale regelgeving te implementeren. PSD II regelt, met uitzondering van de lidstaatopties, maximumharmonisatie, waardoor lidstaten deze bepalingen niet afwijkend mogen implementeren en geen strengere eisen mogen stellen. Afwijking is alleen mogelijk indien er sprake is van een lidstaatoptie of als de richtlijn de lidstaat een keuze biedt (dit is bijvoorbeeld het geval bij de te hanteren methode voor het berekenen van het eigen vermogen van een betaalinstelling). Bij de implementatie van PSD II is de regering, overeenkomstig de Aanwijzingen van de regelgeving[4], zoveel mogelijk uitgegaan van zuivere implementatie. Dit betekent dat Nederland voldoet aan de eisen van PSD II en in beginsel geen gebruik maakt van lidstaatopties, tenzij hier gegronde redenen voor zijn. Vanwege de maximumharmonisatie die PSD II voorschrijft, is uitwijken naar een lidstaat met minder strenge eisen dan Nederland niet waarschijnlijk. Verder is van belang dat de EBA de taak heeft om harmonisatie van het toezicht op PSD II te bevorderen. De richtlijn regelt bijvoorbeeld dat in geval een in een andere lidstaat gevestigde betaaldienstverlener in Nederland betaaldiensten wil aanbieden, de toezichthouder van de lidstaat van ontvangst, in dit geval DNB, maatregelen kan nemen als een betaaldienstverlener niet voldoet aan de eisen van PSD II. DNB kan in dergelijke situaties zo nodig de European Banking Authority (hierna: EBA) verzoeken om bijstand te verlenen.

13) De leden van de SP-fractie vragen de regering een overzicht te leveren van betaalproviders in Nederland, in de EU en internationaal die hun diensten nu al aanbieden zonder het van toepassing zijn van PSD II. Deze leden menen dat deze informatie tot op heden nog niet beschikbaar is gesteld.

Omdat de diensten nu nog ongereguleerd worden aangeboden is een dergelijk overzicht thans niet beschikbaar.

In Nederland zijn momenteel in het openbare register van De Nederlandsche Bank 38 betaalinstellingen geregistreerd (zie https://www.dnb.nl/toezichtprofessioneel/openbaar-register/WFTBI/index.jsp). Geen van deze bestaande, geregistreerde instellingen biedt de nieuwe diensten nu al aan. Het is de regering niet bekend welke en hoeveel van deze betaaldienstverleners voornemens zijn om de nieuwe betaaldiensten aan te gaan aanbieden.

14) De leden van de SP-fractie beseffen dat de komende jaren vele derde partijen in Europa een vergunning zullen aanvragen om bancaire diensten te mogen aanbieden. Deze leden vragen de regering of zij de vergroting

[4] http://wetten.overheid.nl/BWBR0005730 (aanwijzing 9.4)

van de reikwijdte van deze richtlijn ten opzichte van PSD I kan verklaren, gezien de grote zorgen die consumenten hebben over deze regeling.

Sinds de vaststelling van PSD I zijn er nieuwe soorten betaaldiensten ontstaan, vooral op het gebied van internetbetalingen. Met name de betaalinitiatiediensten op het gebied van elektronische handel zijn geëvolueerd. Daarnaast is, dankzij technologische ontwikkelingen, de afgelopen jaren ook een aantal aanvullende diensten ontstaan, zoals rekeninginformatiediensten. Deze diensten zijn nu niet gereguleerd. PSD II leidt ertoe dat deze partijen aan dezelfde eisen voor vergunningverlening moeten voldoen en onder toezicht komen te staan. Tevens waarborgt PSD II de continuïteit in de markt, doordat bestaande en nieuwe dienstverleners hun diensten kunnen aanbieden in een duidelijk en geharmoniseerd regelgevingskader. Ten opzichte van de huidige situatie, waarin de nieuwe betaaldiensten ongereguleerd zijn en niet onder toezicht staan, zijn betaaldienstgebruikers onder PSD II daarmee beter beschermd.

§2. Aanleiding en doelstelling PSD II

15) Kan een concrete casus geschetst worden van de problemen die met PSD II worden opgelost maar onder PSD I niet, zo vragen de leden van de VVD-fractie. Deze leden vragen verder welke directe voordelen de consument zal gaan merken van PSD II.

Eén van de belangrijkste voordelen van PSD II voor de consument is dat PSD II nieuwe diensten mogelijk maakt. Zo zijn betaalinitiatiediensten een alternatief voor onder meer iDEAL-, creditcard- of Paypalbetalingen bij internetaankopen bij webwinkels uit andere lidstaten. Als de bank van de webwinkel niet is aangesloten bij iDEAL, waardoor de klant dus niet met iDEAL kan betalen, of als de klant geen creditcard- of Paypalrekening heeft, kan een betaalinitiatiedienst het verrichten van een dergelijke betaling een stuk makkelijker en goedkoper maken. Ook kan een webwinkel met een vergunning voor het verlenen van betaalinitiatiediensten zelf de betaling van de betaalrekening van de klant starten. De Nederlandse consument die iets bestelt bij een buitenlandse webwinkel die geen iDEAL aanbiedt, kan hiervan profiteren doordat hij naar verwachting meer keuze heeft uit goedkopere en veilige betaalmethoden.

De rekeninginformatiedienst maakt onder andere een digitaal huishoudboekje mogelijk. Dit kan handig zijn als een klant meerdere betaalrekeningen bij een of meer banken heeft of als de klant niet afhankelijk wil zijn van de applicatie van zijn eigen bank. Dat geeft de klant een overzicht van diens betalingen per categorie, zoals voor wonen, levensmiddelen, kleding, vervoer, abonnementen, verzekeringen, etc. Ook kan een overzicht gemaakt worden van ontvangsten, uitgaven en besparingen. Dit kan nuttig zijn als de klant een financieel product nodig heeft, zoals een hypotheek of consumptief krediet. Zonder PSD II is het verkrijgen van dergelijke overzichten alleen mogelijk via de eigen bank of als de klant zelf de gegevens van zijn bankrekeningen downloadt en deze analyseert.

16) De leden van de VVD-fractie vragen of PSD II waarborgen biedt tegen de risico's van cybercrime bij betalingsdiensten, anders dan fraude door een van de gebruikers zelf. Kan de regering hierbij ingaan op de zorgen van de Autoriteit Financiële Markten (AFM) dat PSD II tot meer cybercriminaliteit kan leiden?

PSD II, maar ook daarvan afgeleide regelgeving, zoals de technische reguleringsnormen over sterke cliëntauthenticatie en de beveiligingsrichtsnoeren, bevatten tal van veiligheidsvereisten. Bij situaties waarin een verhoogd risico bestaat op betaalfraude of andere vormen van misbruik,

stelt PSD II extra beveiligingseisen. Een verhoogd risico bestaat in ieder geval als de betaler zich online toegang tot zijn betaalrekening verschaft, een elektronische betalingstransactie initieert (zoals pinnen), gebruik maakt van een communicatiemiddel op afstand (zoals een tablet of mobiele telefoon) of gebruik maakt van een betaalinitiatie- of rekeninginformatiedienstverlener. In al deze gevallen moet sterke cliëntauthenticatie worden toegepast. Alle betaaldienstverleners moeten bovendien voorzien in risicobeperkende maatregelen en controlemechanismen ter beheersing van beveiligingsrisico's. Verder moeten statistische gegevens over onder meer fraude worden verzameld. Tevens stelt PSD II eisen aan het risicomanagement: als er incidenten plaatsvinden moet dit direct worden gerapporteerd aan DNB die corrigerende maatregelen kan verlangen. Ten aanzien van de risico's van phishing bevatten de beveiligingsrichtsnoeren vereisten om actief de ontwikkelingen met betrekking tot cybercriminaliteit te volgen en zo nodig actief de gebruikers te informeren. PSD II bevat daarmee volgens de regering voldoende waarborgen tegen cybercriminaliteit.

Naast veiligheidseisen is ook het toezicht op de naleving daarvan geregeld, zowel op nationaal als Europees niveau, in verband met grensoverschrijdende dienstverlening. Hierbij is het van belang dat nationale toezichthouders zowel onderling afspraken maken alsook binnen hun Europese samenwerkingsverbanden. Op Europees niveau zijn deze samenwerkingsverbanden hiervoor reeds geëquipeerd; op nationaal niveau worden de huidige samenwerkingsconvenanten die bestaan tussen DNB, de Autoriteit Financiële Markten (hierna: AFM) en de Autoriteit Consument en Markt (hierna: ACM) en de Autoriteit persoonsgegevens (hierna: AP) momenteel herzien met het oog op PSD II.

Tot slot geldt dat ook het gedrag van betaaldienstgebruikers kan bijdragen aan het voorkomen en zoveel mogelijk beperken van cybercriminaliteit. Zowel banken als het Maatschappelijk Overleg Betalingsverkeer (MOB) zijn voornemens hierover voorlichtingscampagnes te starten. Daarnaast start DNB in het najaar van 2018 met een voorlichtingscampagne voor consumenten en bedrijven om de bewustwording over veranderingen in het betalingsverkeer als gevolg van PSD II te vergroten.

17) De leden van de SP-fractie vragen de regering met voorbeelden van nieuwe betaaldiensten te komen die niet kunnen functioneren zonder PSD II. Het is deze leden namelijk onbekend of er klachten te vinden zijn van het niet kunnen introduceren van nieuwe betaaldiensten. In het kader van transparantie vragen zij de regering welke bedrijven en/of organisaties hun beklag hierover hebben gedaan.

Betaalinitiatie- en rekeninginformatiediensten kunnen ook zonder PSD II verleend worden, maar dit is afhankelijk van het kunnen verkrijgen van toegang tot de betaalrekening van de klant door verleners van deze betaaldiensten. Omdat alleen banken deze toegang kunnen verlenen, hebben banken nu een spilfunctie. PSD II reguleert deze betaaldiensten, stelt veiligheidseisen aan banken en derde dienstverleners en verplicht banken om – onder de waarborg van deze veiligheidseisen – die toegang te verlenen. Een bekend voorbeeld uit de media is de rechtszaak tussen ING en softwareontwikkelaar AFAS, waarbij de rechtbank Midden-Nederland oordeelde dat het online huishoudboekje van AFAS geen automatische koppeling naar internetbankieren van de ING mag bevatten.[5] De ACM heeft daarnaast in de afgelopen jaren een aantal meldingen ontvangen over de weigering van diverse banken om toegang

[5] http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBMNE:2014:3250

tot de bankrekeninggegevens van klanten tot stand te brengen. De ACM maakt specifieke informatie hierover niet openbaar.

18) De leden van de CDA-fractie vragen naar het wettelijk kader dat van toepassing is op betaaldiensten of rekeninginformatiediensten indien PSD II niet wordt geïmplementeerd. Mag bijvoorbeeld een rekeninginformatiedienst nu al zelfstandig afspraken maken met banken over het delen van rekeninginformatie?

Betaalinitiatie- en rekeninginformatiedienstverleners kunnen zonder PSD II hun diensten verlenen, maar ze zijn daarbij afhankelijk van medewerking van de bank voor de toegang tot de betaalrekening. Indien de bank hiertoe bereid is, kan de betaalinitiatie- of rekeninginformatiedienstverlener afspraken maken met de bank over het verlenen van toegang tot de betaalrekening. Dit gebeurt nu al, met name door een aantal banken aan de zakelijke kant. Na PSD II zijn de nieuwe dienstverleners niet meer afhankelijk van de bank, aangezien PSD II de banken verplicht om toegang te verlenen als de consument daarmee instemt. Voorts regelt PSD II dat de nieuwe partijen een vergunning moeten aanvragen. Dit betekent dat zij aan allerlei eisen moeten voldoen en onder doorlopend toezicht komen te staan.

19) De leden van de CDA-fractie vragen voorts welke grote verschillen tussen EU-lidstaten zijn geconstateerd, waardoor harmonisatie van regels noodzakelijk is gebleken.

De in PSD II geïntroduceerde nieuwe betaaldiensten zijn onder PSD I niet gereguleerd. Voor die diensten is harmonisatie van regels nodig, omdat op die manier een gelijk speelveld wordt gecreëerd voor zowel bestaande spelers als nieuwe partijen die deze diensten willen aanbieden in de Unie.

Daarnaast heeft nadere harmonisatie plaatsgevonden door de uitzonderingen op PSD I te beperken. Allereerst is de uitzondering voor betaaldiensten die worden verricht binnen een beperkt netwerk verder beperkt. Vaak is er binnen beperkte netwerken alsnog sprake van significante betalingsvolumes en bedragen, waarbij de consument honderden of duizenden verschillende producten en diensten worden aangeboden. Dat is in strijd met de doelstelling van de vrijstelling voor beperkte netwerken van PSD I. In PSD II is de vrijstelling beperkt tot gevallen waarin het gaat om de aankoop van een zeer beperkte reeks goederen of diensten bij een welbepaalde detailhandelaar of keten van detailhandelaren, mits wordt voldaan aan een aantal voorwaarden. Bovendien moet het gebruik van deze vrijstelling verplicht worden gemeld bij DNB. Ten aanzien van de uitzondering voor betaaldiensten die worden verricht via telecomapparatuur of -netwerken is sprake van een onduidelijke formulering van de uitzonderingsgrond in PSD I. Hierdoor hebben lidstaten haar op uiteenlopende wijze ten uitvoer gelegd, hetgeen zich vertaalt in een gebrek aan rechtszekerheid voor exploitanten en consumenten. Tevens kan dit een aanleiding vormen voor intermediairdienstaanbieders op het gebied van betalingen om onterecht een beroep te doen op een onbeperkte uitzondering van het toepassingsgebied van PSD I. Tenslotte is voor de uitzondering voor handelsagenten gebleken dat sommige lidstaten toestaan dat deze uitzondering ook wordt gebruikt voor platformen voor elektronische handel die als intermediair optreden voor rekening van zowel individuele kopers als verkopers, zonder echte marge om te onderhandelen over de verkoop of aankoop van goederen of diensten of deze af te sluiten. Deze toepassing gaat verder dan beoogd in PSD I. In PSD II is dit daarom verduidelijkt.

20) De leden van de GroenLinks-fractie zouden graag meer horen over de risicoanalyse die vooraf is gegaan aan dit wetsvoorstel. Wat zijn volgens de regering de grootste risico's van PSD II? Hoe zijn deze risico's afgewogen? Wat is de kans dat een dergelijk risico optreedt en wat is de impact?

In de eerste plaats heeft de Europese Commissie in 2013 een impact assessment uitgevoerd bij het voorstel voor PSD II [1], waarin onder meer een analyse is gemaakt van de impact van verschillende onderzochte beleidsopties. De daarin door de Europese Commissie gemaakte afweging heeft geleid tot het voorstel voor PSD II. Daarnaast is ten behoeve van de implementatie van de richtlijn door middel van dit wetsvoorstel een inventarisatie gemaakt van mogelijke risico's van implementatie van PSD II. Het gaat daarbij om risico's op het gebied van veiligheid, privacy, consumentenbescherming en toezicht. Enkele belangrijke risico's zijn naar het oordeel van de regering: de (on)veiligheid van de wijze waarop een derde partij verbinding maakt met de systemen van de rekeninghoudende bank (inloggegevens, datalekken, etc.), onduidelijkheid over of het onrechtmatig gebruik van persoonsgegevens (privacy), de voorwaarden van de door rekeninghoudende banken gecreëerde toegangsmogelijkheden (prijs, kwaliteit, beschikbaarheid) en eventuele overlap/samenloop van bevoegdheden van toezichthouders (onduidelijkheid, afbakening). Een deel van deze risico's wordt geadresseerd met het wetsvoorstel en met toekomstige Europese wet- en regelgeving (de AVG voor wat betreft privacy risico's en de technische standaarden over sterke cliëntauthenticatie voor wat betreft de veiligheid van de verbindingen tussen rekeninghoudende banken en derde partijen). Een ander deel zal geadresseerd worden door het toezicht op de naleving van PSD II. De betrokken toezichthouders bereiden zich momenteel voor op de implementatie van PSD II en besteden daarbij nadrukkelijk aandacht aan waarborgen en te nemen maatregelen met het oog op de voorgenoemde risico's. Onder regie van de Ministeries van Financiën en Justitie en Veiligheid wordt daarnaast het toezicht op PSD II onderling afgestemd, zodat mogelijke overlap/samenloop van bevoegdheden wordt voorkomen. Tot slot is het voor het adresseren van de voorgenoemde risico's ook belangrijk dat marktpartijen, consumenten en andere betaaldienstgebruikers zich bewust zijn van mogelijke risico's die inwerkingtreding van PSD II met zich mee kan brengen. Om deze partijen daarbij te helpen zetten zowel DNB als het Maatschappelijk overleg Betalingsverkeer (MOB) in op voorlichting. Zo organiseert DNB in de aanloop naar de implementatie seminars voor marktpartijen en publiceert zij met regelmaat informatie over onder meer de vergunningeisen op haar website. Daarnaast zal het MOB in 2018 algemene voorlichting verzorgen over PSD II, met onder meer aandacht voor veiligheids- en privacy risico's, en zal zij onderzoeken of het ontwikkelen van een heldere en toegankelijke manier van toestemming verlenen mogelijk is, specifiek voor kwetsbare groepen (zoals ouderen en mensen met een beperking).

21) De leden van de GroenLinks-fractie vragen tevens hoe de regering aankijkt tegen de analyse van de AFM, daterend van 30 november 2016, dat er meer cybercriminaliteit kan ontstaan door deze nieuwe Europese richtlijn?

Voor de beantwoording van deze vraag wordt verwezen naar het antwoord op vraag 16.

22) De leden van de SP-fractie verbazen zich over de doelstellingen van PSD II. Deze leden vragen de regering hoe zij de interne markt denkt te

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013SC0288&from=EN

versterken met deze richtlijn. Zij vragen de regering hoe deze regeling innovatie stimuleert. Kan de regering dit toelichten?

Door PSD II wordt het mogelijk voor nieuwe partijen om toe te treden tot de Europese betaalmarkt en wordt een gelijk speelveld gecreëerd voor zowel bestaande als nieuwe partijen op de betaalmarkt, waardoor zij onder gelijke voorwaarden hun diensten kunnen aanbieden. Alle partijen die betaaldiensten willen aanbieden op de Europese markt moeten voldoen aan dezelfde regels, moeten in het bezit zijn van een vergunning om hun diensten te mogen aanbieden en staan onder permanent toezicht. De essentie van PSD II is dat betaaldienstgebruikers in de Europese betaalmarkt ervoor kunnen kiezen om gebruik te maken van nieuwe betaaldiensten. In dat geval heeft de betaaldienstverlener, om deze nieuwe diensten te kunnen verlenen, toestemming nodig van de betaaldienstgebruiker om toegang te krijgen tot diens betaalrekening(en) bij een bank. De door PSD II gereguleerde nieuwe betaaldiensten zijn vooral ontstaan in reactie op technische innovaties, met name op het gebied van elektronische en mobiele betalingen. Daarmee ontstaan alternatieve betaalvormen en informatiediensten. Dit opent nieuwe mogelijkheden voor de dienstverleners binnen de Unie en betekent meer concurrentie voor banken binnen de Unie. Omgekeerd worden ook banken daardoor gestimuleerd om nieuwe mogelijkheden aan te bieden. Langs deze weg bevordert PSD II innovaties in het betalingsverkeer en in de digitale dienstverlening aan consumenten.

PSD II draagt daarnaast bij aan een versterking van de interne markt doordat het eenvoudiger wordt om (grensoverschrijdende) online betalingen te doen. Er zullen meer en goedkopere mogelijkheden komen om te betalen, bijvoorbeeld voor een klant die in het buitenland een aankoop wil doen en niet beschikt over Paypal-rekening of creditcard. Bovendien wordt door PSD II de veiligheid van deze (grensoverschrijdende) betalingen vergroot.

23) De leden van de SP-fractie vragen de regering voorts in te gaan op de aanname dat deze richtlijn een bijdrage zal leveren aan de totstandkoming van één Europese betaalmarkt. Deze leden zien dat juist in het betalingsverkeer grenzen nog lijken te bestaan en dat een initiatief om te komen tot éénvormige bankrekeningnummers gestrand is in de invulling per land. Dat maakt dat de leden zich afvragen voor wie dit nu precies wordt geregeld. Is het betalingsgedrag van burgers in Europa lidstaatgrensoverschrijdend? Waarom wordt verondersteld dat dit het geval zal worden door deze richtlijn?

In de afgelopen jaren is er op Europees niveau de nodige wet- en regelgeving vastgesteld die een bijdrage heeft geleverd aan de totstandkoming van één Europese betaalmarkt, waaronder PSD I en de SEPA-Verordening (betreffende overmakingen en automatische overschrijvingen). In dat verband is de systematiek voor bankrekeningnummers geharmoniseerd, conform ISO-standaarden. De regering deelt dan ook niet de opvatting dat het Europese initiatief om te komen tot harmonisatie van bankrekeningnummers is gestrand. Wel erkent zij dat het betaalgedrag van burgers en bedrijven in Europa in de praktijk nog van land tot land verschilt. Dankzij iDEAL – een samenwerking tussen banken die uniek is in Europa – worden er in Nederland bijvoorbeeld veel elektronische betalingen verricht en weinig credit card betalingen. Dit in tegenstelling tot andere lidstaten, waar er meer contante of credit card betalingen plaatsvinden. Door de komst van PSD II zullen dergelijke verschillen tussen lidstaten kleiner worden. Verder is ook Verordening 2015/751 (betreffende afwikkelvergoedingen voor kaartbetalingen) vastgesteld.

Vervolgens is PSD II geïntroduceerd. PSD II beoogt de werking van de interne markt te versterken door het creëren van een gelijk speelveld voor zowel bestaande als nieuwe type spelers op de betaalmarkt, met name voor het online betalingsverkeer voor consumenten. Juist online zijn bestedingen en betalingen daarvoor niet meer aan nationale grenzen gebonden. De nieuwe betaalvormen die PSD II in geheel Europa mogelijk maakt zijn een alternatief naast iDEAL-, creditcard- of Paypalbetalingen. Het is in het belang van Europese consumenten dat zij online gemakkelijk aankopen kunnen doen en kunnen betalen. Hetzelfde geldt voor de informatiediensten. Hier wordt voorts verwezen naar het antwoord op vraag 22.

24) De leden van de SP-fractie wijzen de regering erop dat het betalingssysteem in Nederland robuust en betrouwbaar is. Hoe waarborgt de regering dat deze hoge standaard niet ondermijnd wordt door de richtlijn? Is zij bereid dit in haar toelatingscriteria tot uiting te laten komen?

De regering onderschrijft dat het betalingssysteem in Nederland robuust en betrouwbaar is. Er zijn wettelijke normen die dit waarborgen. Op grond van artikel 3:17 van de Wet op het financieel toezicht (hierna: Wft) worden regels gesteld voor een beheerste bedrijfsvoering, integriteit en soliditeit van financiële instellingen, alsook regels en normen voor een goede werking van het betalingsverkeer, zoals beschikbaarheidsnormen. Deze reeds bestaande regels blijven met de komst van de richtlijn onverminderd van kracht. DNB ziet toe op de naleving hiervan. Daarnaast besteden de richtlijn en daarop gebaseerde lagere regelgeving ook zelf aandacht aan veiligheid en betrouwbaarheid. De regelgeving die voortvloeit uit PSD II beoogt het bovenstaande immers nog verder te versterken. De ingezette weg naar open banking, waarbij ook andere partijen dan de bank toegang kunnen krijgen tot de betaalrekening van klanten van de bank, gaat immers gepaard met stringente vereisten op het gebied van beveiliging en cliëntauthenticatie. De vergunningeisen voor betaaldienstverleners, de regels inzake toegang tot betaalrekeningen ingeval van betaalinitiatiediensten en de regels voor toegang tot en het gebruik van informatie over betaalrekeningen in geval van rekeninginformatiediensten, zijn onderwerp van maximumharmonisatie en ingebed in vergaande technische reguleringsnormen en richtsnoeren. Zo voorziet een van de richtsnoeren (Guidelines on major incident reporting (EBA-GL-2017–10)) in een systeem van rapportage door betaaldienstverleners van majeure operationele en veiligheidsincidenten, waarop de toezichthouder vervolgens maatregelen kan eisen. Eén van de technische standaarden betreft de veiligheid en betrouwbaarheid van de onderlinge communicatie tussen banken en betaaldienstverleners. Hierop wordt meer in detail ingegaan in de beantwoording van de vragen 60 en 62.

§3. Belangrijke veranderingen

1. Vergroting reikwijdte

25) 26) De leden van de VVD-fractie vernemen graag in hoeverre zogenaamde «cryptocurrencies», zoals Bitcoin, ook onder de reikwijdte van het wetsvoorstel vallen en welke bijzonderheden daarop van toepassing zijn. De leden van de SP-fractie vragen de regering hoe PSD II zich verhoudt tot nieuwe valuta zoals Bitcoin en Ethereum.

Het aanbieden of verlenen van diensten met betrekking tot uitsluitend cryptovaluta, zoals Bitcoin en Ethereum, wordt niet aangemerkt als betaaldienst of betaalinstrument in de zin van PSD II. Deze diensten vallen daarom niet onder de reikwijdte van PSD II en dit wetsvoorstel. Zie ook de

brief over cryptovaluta die ik onlangs aan de Tweede Kamer heb gestuurd.[7]

27) De leden van de VVD-fractie vragen hoe wordt omgegaan met een overboeking vanuit de EU naar een niet-EU-lidstaat of vice versa. Valt deze dan niet onder reikwijdte van PSD II? Waarom is er voor gekozen de locatie van de transactie bepalend te laten zijn in plaats van de nationaliteit van de gebruiker? Wordt een Nederlander die gebruik maakt van een dienst buiten de EU nu niet beschermd?

PSD II is in beginsel van toepassing op betaaldiensten die worden aangeboden in de Europese Economische Ruimte (EER), waar de Europese Unie deel van uit maakt. Alleen de mogelijkheid van «toegang» tot de dienst vanuit de EU/EER is niet voldoende: de dienstverlener moet zich richten op de Europese markt. Dit betekent dat een Nederlandse consument die gebruik maakt van een Amerikaanse bank die zijn diensten aanbiedt in Nederland, om geld over te boeken naar een bank in een land dat ook buiten de EU/EER valt, beschermd is. De reikwijdte van PSD II geldt ongeacht de nationaliteit van degene die van de dienst gebruik maakt. De Nederlandse consument die gebruik maakt van een betaaldienstverlener die zijn diensten aanbiedt in de EU/EER, is altijd beschermd.

28) De leden van de CDA-fractie vragen naar de definitie van een transactie die binnen de EU plaatsvindt. Gaat het hierbij om het in gang zetten van een transactie door een gebruiker die zich op het grondgebied van de EU bevindt, een transactie door een inwoner van de EU die zich buiten de EU bevindt of een transactie waarbij de betaaldienstverlener zich binnen de EU bevindt. Of gaat het om nog een andere vorm? Kan de regering het principe van «one leg out» nader uitleggen?

Bij «one leg out» gaat het om transacties waarbij één (of de enige) bij de betalingstransactie betrokken betaaldienstverlener(s) zich in de EU/EER bevindt. Bepalend is waar de betaaldienstverlener van de betaler en/of begunstigde zich bevindt en of deze zich met het aanbieden van de betreffende betaaldienst richt op de Europese markt. Waar de gebruiker zich bevindt en of deze gebruiker een inwoner van de Unie is, speelt geen rol. Indien een Nederlander zich buiten de EU/EER bevindt, maar gebruik maakt van een Nederlandse bank (betaaldienstverlener) valt de transactie dus onder het «one leg out» principe.

29) De leden van de VVD-fractie vragen waarom is gekozen voor de genoemde uitzonderingsgronden. Welke eis of maatregel uit PSD II zou onredelijk bezwarend geweest zijn om een uitzonderingsgrond te rechtvaardigen? Welke bescherming heeft de consument nu er voor een uitzonderingsgrond gekozen is?

De gevallen waarin sprake is van uitsluiting van de toepassing van PSD II zijn in PSD II strikter geformuleerd, omdat de in PSD I geformuleerde uitsluitingsbepalingen in lidstaten op zeer uiteenlopende wijze worden toegepast. Dit betreft de in artikel 3 van PSD II genoemde uitzonderingen ten aanzien van beperkte netwerken, betaaldiensten via telecomapparatuur of -netwerken en handelsagenten. Door een striktere definiëring van deze uitzonderingen is het voor een consument duidelijker wanneer een dienstverlener onder de reikwijdte van PSD II valt en daarmee aan welke eisen een dienstverlener moet voldoen en welke rechten een consument als gevolg daarvan heeft. Bovendien geldt voor een dienstverlener die buiten de reikwijdte van PSD II valt een meldplicht. In het

[7] *Kamerstukken II*, 2017–2018, 32 013, nr. 168

wetsvoorstel is dit geïmplementeerd door te voorzien in een meldplicht bij de Nederlandsche Bank.

30) De leden van de VVD-fractie vragen voorts hoe de hier genoemde drempelwaarde wordt gemeten. Welke tijdseenheid wordt daarbij aangehouden? Hoe wordt omgegaan met meerdere kleine overboekingen die afzonderlijk niet, maar gezamenlijk wel de drempelwaarde overschrijden?

Tijdseenheden worden in PSD II gespecificeerd (zie artikel 3, onderdeel l, van de richtlijn). De genoemde tijdseenheid is een maand. Als tijdens deze maand de drempelwaarde van 50 euro per afzonderlijke betalingstransactie of een cumulatieve waarde van 300 euro wordt overschreden, valt de betreffende dienstverlener niet meer onder de uitzondering van PSD II en dient een vergunning te worden verkregen voor het aanbieden van deze diensten. Voor deze partijen geldt bovendien de verplichting om de Nederlandsche bank jaarlijks in kennis te stellen dat zij hun activiteiten verrichten met inachtneming van de hiervoor genoemde maximumbedragen.

31) De leden van de SP-fractie vragen de regering te onderbouwen waarom de reikwijdte vergroot wordt ten aanzien van financiële innovators en waarom deze gratis toegang tot bankdata krijgen. Deze leden horen graag een toelichting.

Voor het antwoord op deze vraag wordt verwezen naar de beantwoording van vraag 15.

2. Nieuwe betaaldiensten

32) Hoe worden diensten behandeld die onder beide definities (betaal- en rekeninginformatiedienst) zouden kunnen vallen, zo vragen de leden van de VVD-fractie.

Instellingen die een betaaldienst willen verlenen als bedoeld in de bijlage bij PSD II, dienen een vergunning aan te vragen, waarbij zij moeten specificeren welke specifieke dienst(en) zij willen verlenen. De vergunning ziet enkel op de aangevraagde typen diensten. Als een instelling zowel betaalinitiatie- als rekeninginformatiediensten wil verlenen, dient zij aan alle eisen voor beide diensten te voldoen. Betaaldiensten waarvoor een vergunningplicht geldt, maar waarvoor geen vergunning is afgegeven, mogen niet worden verleend.

33) De leden van de VVD-fractie vragen hoe het beschreven vereiste van een scheiding tussen de betaaldiensten en het aanhouden van tegoeden zich verhoudt tot diensten die aangeboden worden door banken en financiële instellingen.

Banken kunnen betaalrekeningen aanhouden en moeten aan alle vergunningvoorwaarden voldoen die worden genoemd in artikel 2:12 Wft. De meeste betaaldienstverleners, namelijk de betaaldienstverleners die diensten 1 t/m 6 van de bijlage bij PSD II verrichten, moeten ook aan dergelijke eisen voldoen. Betaaldienstverleners die ten minste de diensten 1 t/m 6 verrichten, kunnen ook geldmiddelen van betaaldienstgebruikers onder zich houden, maar uitsluitend voor het verrichten van betalingstransacties. Anders dan banken mogen zij die geldmiddelen niet gebruiken voor het verstrekken van kredieten voor eigen rekening. Voor deze categorie betaaldienstverleners is daarom voorzien in regels die waarborgen dat de eigendomsrechten van betaaldienstgebruikers zijn veiliggesteld (vermogensscheiding). Deze eisen zijn opgenomen in de

artikelen 3:29a Wft (vermogensscheiding) en 3:29c Wft (eis dat betaalrekeningen uitsluitend worden aangehouden voor het verrichten van betalingstransacties). Betaaldienstverleners die dienst 7 en/of 8 van de bijlage bij PSD II verrichten, hebben geen toegang tot de geldmiddelen van de betaaldienstgebruiker en kunnen ook geen geldmiddelen aanhouden. Daarom hoeven zij aan minder strenge eisen te voldoen. Zie ook de beantwoording van vraag 34.

34) De leden van de CDA-fractie vragen naar het principiële verschil tussen een betaaldienstverlener en een rekeninginformatiedienstverlener, waardoor de regels voor een vergunning voor een betaaldienstverlener strenger zijn dan die voor een rekeninginformatiedienstverlener. Deze leden menen dat de omgang met rekeninggegevens in zijn algemeenheid vraagt om strikte regels en zij zien nog niet waarom dat voor een rekeninginformatiedienstverlener minder strikt moet zijn. Kan de regering tevens uitleggen waarin de grootste verschillen zitten?

Een rekeninginformatiedienstverlener is niet betrokken bij betalingstransacties en is op geen enkel moment in het bezit van de geldmiddelen van een betaaldienstgebruiker. Om die reden hoeft een rekeninginformatiedienstverlener niet te voldoen aan de eisen omtrent het veiligstellen van ontvangen geldmiddelen uit betaaldiensten (artikel 3:29a Wft), het aanhouden van een minimum aan eigen vermogen (artikel 3:53 Wft) en omtrent solvabiliteit (artikel 3:57 Wft). Betaaldienstverleners die wel in het bezit (kunnen) komen van de geldmiddelen van een betaaldienstgebruiker dienen wel aan deze eisen te voldoen. De eisen met betrekking tot sterke cliëntauthenticatie, beveiliging, risicobeperkende maatregelen en controlemechanismen ter beheersing van beveiligingsrisico's gelden onverkort voor rekeninginformatiedienstverleners.

35) De leden van de SP-fractie zijn niet gerust op het feit dat slechts de toestemming van de betaler hem zal beschermen. Deze leden vragen de regering met een duidelijk onderbouwd verhaal te komen hoe de betaler toegang kan weigeren tot zijn gegevens en hoe misbruik bestreden kan worden.

Als een rekeninghouder geen dienst van een derde partij, zoals een betaalinitiatie- of rekeninginformatiedienstverlener, wenst af te nemen, dan komt er tussen beide partijen geen overeenkomst tot stand voor het verlenen van dergelijke diensten. Daardoor ontbreekt een juridische grondslag voor het verkrijgen van toegang tot de betaalrekening.

Daarnaast stelt PSD II als voorwaarde voor het verkrijgen van toegang tot de betaalrekening van een rekeninghouder, dat de rekeninghouder uitdrukkelijk toestemming moet verlenen aan de betaaldienstverlener voor het verlenen van de betaaldienst en daarmee voor toegang tot de betaalrekening. Daartoe moet de rekeninghouder zich eerst – via de derde partij – identificeren jegens de rekeninghoudende betaaldienstverlener door gebruik te maken van sterke cliëntauthenticatie. Dit is een speciale beveiligingsmethode met authenticatie met gebruik van twee of meer factoren die worden aangemerkt als kennis (iets wat alleen de gebruiker weet), bezit (iets wat alleen de gebruiker heeft) en inherente eigenschap (iets wat de gebruiker is) en die onderling onafhankelijk zijn (artikel 4(30) PSD II). Als een rekeninghouder zich niet op de hiervoor beschreven wijze heeft geïdentificeerd, krijgt een derde partij geen toegang tot de betaalrekening. Daarmee krijgt de derde partij geen inzicht in de betaalgegevens, kan hij deze niet gebruiken en kan hij geen betaling initiëren.

36) De leden van de SP-fractie willen tevens weten wat de regering vindt van «open banking».

«Open banking» houdt in dat banken hun toegangssoftware zo inrichten dat naast banken zelf ook derde partijen – na uitdrukkelijke toestemming van klanten van banken – op een veilige manier toegang krijgen tot deze software, zodat zij nieuwe, innovatieve diensten aan deze klanten aan kunnen bieden. Hierbij is het van belang dat de stabiliteit en integriteit van financiële markten en instituties en de veiligheid van het betalingsverkeer gewaarborgd blijven en de consument voldoende bescherming geniet.

37) Deze leden van de SP-fractie vragen de regering of mededingingsrecht van toepassing is op deze regeling. Bij positieve beantwoording vragen deze leden welke regels van toepassing zijn.

Het mededingingsrecht, zoals dit verankerd is in de Mededingingswet en het Verdrag betreffende de werking van de Europese Unie (VWEU), is van toepassing op alle ondernemingen die goederen of diensten op markten aanbieden en dus ook op rekeninginformatiediensten en betaalinitiatiediensten. Zo bevat de Mededingingswet een verbodsbepaling voor het sluiten van kartels (artikel 6 Mededingingswet) en een verbod op misbruik van een economische machtspositie (artikel 24 Mededingingswet). De ACM en de Europese Commissie houden onafhankelijk toezicht op de naleving van het mededingingsrecht.

38) De leden van de SP-fractie constateren dat de richtlijn een consument of bedrijf die een product of dienst koopt in een land dat niet lid is van de EU of de Europese Economische Ruimte (EER), niet kan garanderen dat sprake is van toezicht door de toezichthouders op de verkopende partij. Deze leden menen dat het Nederlands en Europees recht niet van toepassing is in niet-EU/EER landen. De leden van de SP-fractie vragen de regering hierover naar haar mening met daarbij een toelichting.

De richtlijn is van toepassing op betaaldiensten die worden aangeboden in de EU/EER. De bij of krachtens de Wft gestelde regels zijn slechts van toepassing op betaaldiensten aangeboden in Nederland (online of fysiek), tenzij in die regels anders is bepaald. Ook als een consument of bedrijf gebruik maakt van een betaaldienst die wordt aangeboden in Nederland door een betaaldienstverlener die is gevestigd in een land dat geen lid is van de EU/EER, is de Wft dus van toepassing. Als een product of dienst wordt gekocht in een land dat geen lid is van de EU/EER en voor het verrichten van de betaling gebruik wordt gemaakt van een betaaldienstverlener die valt onder de reikwijdte van PSD II, dan kan PSD II deels van toepassing zijn op de betalingstransactie, afhankelijk van de valuta waarin de betalingstransactie plaatsvindt en het land waarin de bij de transactie betrokken betaaldienstverleners zijn gevestigd. Zo is een aantal bepalingen van titel III en IV van PSD II tevens van toepassing op betalingstransacties in alle valuta waarbij slechts één van de betaaldienstaanbieders zich in de EU/EER bevindt, met betrekking tot die delen van de betalingstransactie die binnen de EU/EER worden uitgevoerd. Het gaat daarbij om de bepalingen die betrekking hebben op de betaling die wordt verricht door de in de EU/EER gevestigde betaaldienstverlener.

39) De leden van de SP-fractie menen dat het praktisch onmogelijk is om te eisen dat burgers en bedrijven binnen de EU-zone enkel zaken mogen doen bij bedrijven die een vergunning hebben. Zij vragen de regering naar haar mening.

Het staat burgers en bedrijven in beginsel vrij om zaken te doen met een ieder. In het belang van een goede werking van het betalingsverkeer en de bescherming van burgers en bedrijven wordt het in EU-verband noodzakelijk geacht dat het aanbieden van betaaldiensten onder toezicht staat. Voor het aanbieden van betaaldiensten in de EU/EER is daarom een

vergunning nodig. De richtlijn is van toepassing op betaaldiensten die worden aangeboden in de EU/EER. Als een burger of een bedrijf binnen de EU/EER gebruik wil maken van een betaaldienst die wordt aangeboden binnen de EU/EER en deze aanbieder vraagt daarvoor aan de bank toegang tot de betaalrekening van de betreffende betaaldienstgebruiker, dan controleert de bank in het register of de betreffende aanbieder een vergunning heeft voor het verlenen van de gevraagde betaaldienst. Als dat niet het geval is, mag de bank geen toegang verlenen tot de betaalrekening en kan de betaaldienstgebruiker geen gebruik maken van de aangeboden betaaldienst. Bovendien dient de betaaldienstverlener die toegang wil tot de betaalrekening zich te identificeren bij de bank waar deze betaalrekening wordt aangehouden. DNB houdt toezicht op de wijze waarop derde partijen (toestemming voor) toegang verkrijgen en op de wijze waarop banken toegang verlenen.

40) De leden van de SP-fractie vragen de regering voorts of een telecomprovider wel of niet een betaalprovider is onder PSD II. Is dit ook het geval als een aankoop gedaan wordt in een app van bijvoorbeeld Domino's Pizza of Uber? Deze leden vinden dat de richtlijn geen praktische kaders geeft, die aangeven of een betaaldienst nu wel of niet onder PSD II valt.

Een aantal typen betalingstransacties is in PSD II uitgezonderd en valt dus niet onder het bereik van de wet- en regelgeving waarmee PSD II wordt geïmplementeerd. Deze uitzonderingen bestaan ook al onder PSD I, die is geïmplementeerd in de Nederlands wet.

Eén van die uitzonderingen betreft bepaalde betalingstransacties door telecomaanbieders. Voordat bepaald kan worden of een dergelijke betalingstransactie onder de uitzonderingen van PSD II valt, moet eerst worden bepaald of de betalingstransactie een betaaldienst is in de zin van PSD II. Indien een telecomaanbieder de kosten voor diensten van een derde partij bij de abonnee (betaler) in rekening brengt, bijvoorbeeld via een maandelijkse factuur, en deze kosten vervolgens aan die derde partij doorbetaalt, is er sprake van een betaaldienst, waardoor deze dienstverlening van de telecomaanbieder binnen de reikwijdte van PSD II valt. Dit ligt anders in het geval dat een telecomaanbieder dezelfde diensten van een derde partij opkoopt, en deze (tegen een meerprijs) doorverkoopt aan de abonnee (betaler). Dan is er geen sprake van een betaaldienst en valt de dienstverlening valt buiten de reikwijdte van PSD II. Indien op grond van het bovenstaande geconcludeerd moet worden dat een telecomaanbieder betaaldiensten verleent, dan kan de telecomaanbieder alsnog worden uitgezonderd van de toepassing van PSD II, als op hem de uitzondering inzake microbetalingen van toepassing is (artikel 3, onderdeel l, van de richtlijn).

Overigens is het bij PSD II van belang om bij aanschaf van digitale diensten, zoals app-aankopen, onderscheid te maken tussen het verrichten van betalingen via de telefoonrekening en het verrichten van betalingen met behulp van een mobiele telefoon waarbij de betaling gewoon via de betaalrekening geschiedt. In de meeste gevallen gaat het om de tweede situatie waarbij de telecomprovider slechts de telecomdiensten (toegang tot mobiel internet) verleent en is er geen sprake van een betaaldienst.

Heeft een dienstverlener twijfel of zijn dienstverlening onder de reikwijdte van PSD II valt, dan kan deze desgewenst contact opnemen met DNB.

41) De leden van de PvdD-fractie vragen of de regering de mening deelt dat innovatie en vermarkting van betaaldiensten niet noodzakelijk is, terwijl dit wel ten koste gaat van het belang van de bescherming van financiële transacties van burgers? Zo nee, waarom niet?

Sinds de vaststelling van PSD I zijn op basis van zich ontwikkelende klantbehoeften nieuwe soorten betaaldiensten ontstaan, vooral op het gebied van internetbetalingen. Met name de betaalinitiatiediensten op het gebied van elektronische handel zijn geëvolueerd. Daarnaast is dankzij technologische ontwikkelingen de afgelopen jaren ook een aantal aanvullende diensten ontstaan, zoals rekeninginformatiediensten. Deze diensten bestaan deels al, maar zijn nu niet gereguleerd, waardoor de bescherming van betaaldienstgebruikers nu niet voldoende gewaarborgd is. PSD II moet ertoe leiden dat betaaldienstgebruikers beter worden beschermd, dat de continuïteit in de markt wordt gewaarborgd en dat bestaande en nieuwe dienstaanbieders, ongeacht hun bedrijfsmodel, in staat worden gesteld hun diensten aan te bieden in een duidelijk en geharmoniseerd regelgevingskader. Zo worden als gevolg van PSD II deze nieuwe betaaldiensten onder meer EU-breed onderworpen aan dezelfde vergunningvoorwaarden en worden zij onder toezicht gebracht van nationale toezichthouders. Daarmee wordt een gelijk speelveld gecreëerd voor de nieuwe diensten en worden consumenten in de EU op gelijke wijze beschermd. De consument kan zelf bepalen of hij gebruik maakt van deze diensten en, zo ja, van welke aanbieder.

42) De leden van de PvdD-fractie vragen verder of de regering de mening deelt dat het wenselijker en mogelijk is dat banken zelf innoveren, met behoud van bescherming van financiële gegevens? Zo nee, waarom niet? Deelt de regering voorts de mening dat dit belang groter is dan het beoogde doel van PSD II, namelijk innovatie als verdienmodel? Zo nee, waarom niet?

De regering verwelkomt innovatie in de financiële sector, mits de stabiliteit en integriteit van financiële markten en instituties gewaarborgd blijven. Zoals eerder genoemd creëert het wetsvoorstel ter implementatie van PSD II ruimte voor innovatieve nieuwe betaaldiensten en is bij de totstandkoming van PSD II gezocht naar een manier om innovatie van de betaaldienstverlening te stimuleren binnen de kaders van eisen die gelden op het gebied van veiligheid van het gebruik van betaaldiensten en consumentenbescherming. Deze innovatie vindt de regering belangrijk, omdat dit leidt tot vernieuwing en meer keuzemogelijkheden voor consumenten. Het is zeer goed mogelijk dat banken zelf zullen innoveren; deels doen zij dat al. Innovatie door derde partijen en potentiële toetreding van derde partijen houdt de banken evenwel scherp. Naar verwachting zullen banken onder druk van concurrentie zowel zelf innoveren op het gebied van betaaldiensten, als innovatie omarmen door samenwerkingsverbanden aan te gaan met (niet-bancaire) fintech-spelers, banken en betaalinstellingen. Dit is in lijn met het regeerakkoord waarin met een vergunning in lichtere vorm wordt ingezet op toetreding van innovatieve partijen met inachtneming van voldoende bescherming van klanten. PSD II creëert mogelijkheden voor nieuwe, derde partijen en introduceert tegelijkertijd strenge veiligheidsnormen voor de bescherming van financiële gegevens. Zowel bestaande instellingen als nieuwe toetreders zullen blijvend moeten voldoen aan deze normen.

3. Vergunningverlening

43) De leden van de VVD-fractie lezen in de implementatiewet dat in het kader van veilig betalingsverkeer meer voorwaarden aan vergunningverlening worden gesteld dan voorheen. Hoe wordt getoetst of de genoemde

extra vergunningseisen daadwerkelijk veiligheid toevoegen en risico's beperken en niet slechts tot extra lasten en daarmee uiteindelijk minder aanbieders leiden?

In het kader van een veilig betalingsverkeer worden meer voorwaarden gesteld aan vergunningverlening dan voorheen. Betaalinstellingen moeten onder andere kunnen aantonen hoe wordt omgegaan met veiligheidsincidenten en klachten, het opslaan, monitoren, traceren en beperken van toegang tot gevoelige betaalgegevens, de bedrijfscontinuïteit, de wijze waarop statistieken worden bijgehouden van transacties en fraude, het veiligheidsbeleid inclusief risicoanalyse en hoe toezicht wordt gehouden op agenten en bijkantoren. Bij het maken van nieuwe regels is een afweging gemaakt tussen het voorkomen van extra lasten en het beschermen van betaaldienstgebruikers. Dat heeft geleid tot de regels in PSD II en tot daaruit voortvloeiende technische standaarden en richtsnoeren die op Europees niveau (door de EBA) zijn vastgesteld.

44) De leden van de VVD-fractie vragen verder hoe wordt omgegaan met nieuwe innovatieve experimenten. Moeten zij direct aan alle eisen voldoen voor markttoegang of kan er ook sprake zijn van een ingroeimodel?

Nieuwe partijen moeten voldoen aan alle eisen voor markttoegang. De toezichthouders kunnen deze evenwel proportioneel toepassen. Van belang hierbij zijn de in 2016 en 2017 door DNB en de AFM gelanceerde Innovationhub en het programma Maatwerk voor Innovatie (vaak Regulatory Sandbox genoemd). Binnen deze initiatieven is het doel om (nieuwe of bestaande) partijen met innovatieve concepten of producten een laagdrempelig portaal bij de toezichthouder aan te bieden en – wanneer bestaande regelgeving of de toepassing daarvan onnodig knellend zou zijn – te bezien of bepaalde innovaties mogelijk zijn met een toepassing van de regels op maat, voor zover de regelgeving daarvoor ruimte laat voor wat betreft uitleg of proportionele toepassing ervan. Tevens is in dit kader relevant dat voor bepaalde diensten vrijstelling van de vergunningplicht geldt, als de omvang van de activiteiten beperkt is (zie het reeds bestaande artikel 1a van de Vrijstellingsregeling Wft). Overigens moeten deze partijen wel als vrijgestelde geregistreerd worden in het register van DNB.

45) De leden van de CDA-fractie vragen of de extra voorwaarden zoals die worden gesteld aan betaalinstellingen, alleen gelden voor nieuwe betaalinstellingen of ook voor bestaande betaalinstellingen zoals banken.

PSD II introduceert een aantal extra verplichtingen, onder andere op het terrein van beveiliging van data en cliëntauthenticatie. Deze gelden zowel voor bestaande als nieuwe instellingen. Bestaande instellingen moeten ten genoegen van de toezichthouder aantonen dat zij voldoen aan de extra verplichtingen. Ze krijgen daar tot 13 juli 2018 de tijd voor. Indien het wetsvoorstel ter implementatie van PSD II later dan deze datum in werking treedt, dienen bestaande instellingen direct na inwerkingtreding van het wetsvoorstel aan deze extra verplichtingen te voldoen.

46) De leden van de CDA-fractie vragen verder welk deel van de werkzaamheden van een betaalinstelling in de EU-lidstaat van vestiging moet plaatsvinden. Gaat het bijvoorbeeld om een bepaald deel van de medewerkers dat ergens gevestigd moet zijn, gaat het om een deel van de omzet die moet worden behaald of gaat het om een aantal transacties dat in het vestigingsland gedaan moet worden? Daarbij vragen deze leden hoe wordt voorkomen dat een betaalinstelling slechts op het moment van vergunningverlening voldoet aan de gestelde eisen en vervolgens

activiteiten verplaatst naar een ander land. Hoe en hoe vaak vindt monitoring plaats?
De leden van de SP-fractie menen dat de volgende uitspraak uit de memorie van toelichting onhoudbaar is: «Naast de vergunningsvoorwaarden stelt PSD II dat ten minste een deel van de werkzaamheden van een betaalinstelling in de lidstaat van vestiging moet plaatsvinden.» Deze leden constateren dat het eenieder vrij staat om op het internet tot zaken te komen met elke geïnteresseerde. Zij vinden het idee dat Europese of Nederlandse wetgeving in staat zou zijn om haar regels wereldwijd toe te passen een illusie. De leden van de SP-fractie vragen de regering of zij deze mening deelt. Ook vragen deze leden om een toelichting.

Uitgangspunt in het financiële toezicht is dat het hoofdkantoor van een (vergunningplichtige) financiële onderneming zich bevindt in de lidstaat waar de onderneming haar zetel heeft. Dat is voor Nederland in de Wet op het financieel toezicht vastgelegd in artikel 3:15 (het door DNB bestreken prudentiële domein) en de artikelen 4:40 en 4:84 (het door de AFM bestreken gedragsdomein). Voor onder andere banken en betaalinstellingen is dat geregeld door middel van het vereiste dat tenminste twee personen die het dagelijks beleid van de onderneming bepalen hun werkzaamheden vanuit Nederland verrichten. PSD II voegt daaraan toe dat de onderneming tenminste een deel van zijn bedrijf zal uitoefenen in Nederland. De regering is van mening dat dit materieel reeds is gewaarborgd in de aangehaalde bepalingen. Bij de vergunningverlening wordt onderzocht of aan deze voorwaarden wordt voldaan. Als blijkt dat de werkzaamheden van de instelling na het verkrijgen van de vergunning verdwijnen uit Nederland, kan DNB maatregelen treffen indien niet meer aan de vergunningvereisten wordt voldaan. DNB houdt geen prudentieel toezicht op de activiteiten van een betaalinstelling met dienstverlening vanuit een ander EU-land. De bevoegde autoriteit van dat andere EU-land houdt vanzelfsprekend wel prudentieel toezicht.

Als DNB signalen krijgt dat het toezicht in andere EU-landen anders, of minder goed is, dan bespreekt DNB dat met die buitenlandse toezichthouders. Mochten zij er samen niet uitkomen dan kan DNB de ontstane situatie bespreken met de European Banking Authority (EBA). De EBA kan vervolgens dit onderwerp in breder verband bespreken en eventueel hierover guidance bieden aan de sector.

Ik deel de mening van de leden van de SP-fractie dat het in beginsel eenieder vrij staat om via internet tot zaken te komen met ongeacht welke partij. Dat geldt ook voor de keuze van betaaldienstverlener. Deze kan zowel binnen als buiten de EU/EER gevestigd zijn. Als een betaaldienstverlener echter betaaldiensten aanbiedt in de EU/EER dan is PSD II van toepassing en gelden daarmee ook de daarin gestelde vergunningvereisten, welke voor Nederland zijn geïmplementeerd in de Wft. De instelling vraagt de vergunning aan in het land binnen de EU/EER waar (ten minste) een deel van de werkzaamheden wordt verricht. De instelling dient in dit land haar zetel en hoofdkantoor te hebben (plaats van vestiging van een rechtspersoon behorende tot de instelling, bijvoorbeeld een dochter.) Indien de lidstaat van vestiging een andere lidstaat is dan Nederland, kan de instelling diensten verlenen in Nederland op basis van de door de andere lidstaat verleende vergunning (Europees paspoort). Dit kan grensoverschrijdend, door middel van het verrichten van diensten naar Nederland, door middel van een in Nederland gelegen bijkantoor of via een Nederlandse agent. De toezichthouder in de lidstaat waar de vergunning is verleend, houdt toezicht op de instelling voor de diensten die in Nederland worden verricht. Indien een vergunninghoudende betaaldienstverlener uit een andere lidstaat in Nederland zijn diensten wil aanbieden (bijvoorbeeld via een agent of bijkantoor), dient deze instelling

een aantal gegevens, waaronder gegevens over welke betaaldiensten de instelling voornemens is te gaan verrichten, over te leggen aan de bevoegde autoriteit van de lidstaat van herkomst. De bevoegde autoriteit van de lidstaat van herkomst legt deze gegevens vervolgens ter beoordeling voor aan de bevoegde autoriteit van de lidstaat van ontvangst, in dit geval De Nederlandsche Bank. Indien DNB tot een ongunstige beoordeling komt, kan de lidstaat van herkomst niet overgaan tot inschrijving van de agent of het bijkantoor in het register. Zonder deze inschrijving kan de instelling haar diensten niet in Nederland aanbieden.

Indien sprake is van aanbieden van betaaldiensten op de Nederlandse markt zonder vergunning, is dit een overtreding van de Wft en kan DNB overgaan tot het treffen van handhavingsmaatregelen, waaronder het opleggen van boetes.

47) De leden van de SP-fractie vragen de regering hoe een ondernemer in China eerst een vergunning in de EU moet verkrijgen alvorens zij tot zaken kan komen met Europese burgers. Ziet de regering ook het risico dat als die vergunning verleend wordt in een land met lage standaarden, het toezicht extreem moeilijk wordt en daarmee de mogelijkheid voor burgers om hun recht te halen en bijvoorbeeld hun data terug te krijgen wordt belemmerd? Deze leden vragen de regering hoe de toezichthouder betalingen aan de eerder genoemde ondernemer wil tegenhouden indien er geen vergunning is verstrekt. Wordt de consument dan vervolgd? De voorgenoemde leden menen dat het in kwestie zijnde Chinese bedrijf moeilijk voor de rechter gedaagd kan worden als deze niet in overtreding is van de Chinese wet- en regelgeving. Deelt de regering deze opvatting?

Voor het aanbieden van betaaldiensten in de EU/EER is een vergunning vereist. Dit geldt ook voor een Chinese onderneming die met betaaldienstverlening actief wil worden in de EU/EER. De instelling kan de vergunning aanvragen in het EU/EER-land waar (ten minste) een deel van de werkzaamheden worden verricht. De instelling dient in dit land een zetel en hoofdkantoor te hebben (plaats van vestiging van een rechtspersoon behorende tot de instelling, bijvoorbeeld een dochter). Indien dit een andere lidstaat is dan Nederland, kan de instelling diensten verlenen in Nederland op basis van het Europese paspoort. Dit kan grensoverschrijdend (bijvoorbeeld via internet), door middel van een bijkantoor in Nederland of via een Nederlandse agent. De toezichthouder in de lidstaat waar de vergunning is verleend, houdt toezicht op de instelling voor de diensten die in Nederland worden verricht. Dit is de zogenoemde «home» toezichthouder. Een eventuele procedure over niet nakoming of een onrechtmatige daad door de instelling kan door de consument worden aangespannen bij de rechter in de lidstaat (binnen de EU/EER) waar de vergunning is verleend.

Als een partij op de Nederlandse markt actief is zonder dat deze over de juiste vergunning beschikt, kan DNB overgaan tot het nemen van handhavingsmaatregelen, waaronder het opleggen van boetes.

48) De leden van de SP-fractie hebben er moeite mee dat er veel verschil kan ontstaan in de vergunningverlening in verschillende EU-lidstaten, terwijl een vergunning wel toegang geeft tot burgers in álle EU-lidstaten. Hoe wordt voorkomen dat alle aanbieders trekken naar een bepaalde EU-lidstaat zonder noemenswaardige toelatingscriteria en/of toezicht op de aanbieders, teneinde in de hele Unie gebruik te kunnen maken van betaalgegevens van burgers?

Voor de beantwoording van deze vraag wordt verwezen naar de beantwoording van vraag 12.

4. Regels over niet toegestane en onbedoelde overboekingen

Eigen risico

49) De leden van de VVD-fractie lezen in de implementatiewet dat het eigen risico wordt verlaagd. Waarom wordt in de richtlijn gekozen voor de verlaging van het eigen risico? Waarom was het oude eigen risico inadequaat en waarom wordt er specifiek naar 50 euro verlaagd? Welke landen maken wel gebruik van de lidstaatoptie om het eigen risico te verlagen? Waarom kiezen deze landen daar wel voor en tot welk bedrag verlagen zij het eigen risico? Hoe wordt omgegaan met de situatie waarbij een transnationale overboeking een land raakt met twee verschillende eigen risico's?

50) De leden van de CDA-fractie vragen naar het ongebruikt laten van de lidstaatoptie om het eigen risico bij misbruik van een betaalinstrument, te verlagen naar nul euro. Deze leden begrijpen dat het verstandig is om een stimulans in te bouwen voor de consument om zorgvuldig te blijven handelen en een vorm van eigen risico daarbij behulpzaam kan zijn. Maar de leden van de CDA-fractie vragen of deze stimulans niet al zit ingebakken in de wet, wanneer bij frauduleus handelen, grove nalatigheid of het schenden van één of meer verplichtingen ex artikel 69 van PSD II het volledige risico – en dus het verlies – al bij de betaler/consument wordt neergelegd. Deze leden menen dat bij grove nalatigheid het redelijk is om de verliezen de consument te doen toekomen, maar achten een behoorlijke bescherming van de consument wenselijk wanneer het gaat om zaken die de consument minder zijn aan te rekenen, zeker als het gaat om consumenten die minder vaardig zijn met technologische ontwikkelingen zoals de doelgroep ouderen.

51) De leden van de GroenLinks-fractie lezen in de implementatiewet dat in het geval van misbruik het eigen risico van de betaler wordt verlaagd naar 50 euro. Waarom wordt het eigen risico niet geheel afgeschaft? Deze optie heeft Nederland namelijk wel.

Verschillende fracties hebben gevraagd naar het eigen risico, de verlaging naar 50 euro en de vraag waarom Nederland geen gebruik maakt van de lidstaatoptie om het eigen risico op 0 te zetten.

Het doel van een eigen risico bij verlies van een betaalinstrument, zoals een pinpas, is een passende prikkel om snel het verlies te melden. Onder PSD I was dit bedrag maximaal 150 euro. PSD II voorziet in een verlaging van het eigen risico van 150 naar 50 euro bij verlies van een betaalinstrument. Volgens de Europese Commissie was de aanleiding voor deze verlaging dat deze drempel in de praktijk vaak als een soort boete wordt ervaren. Daar komt bij dat de consument ook zonder het bedrag van 150 euro al prikkels heeft om het verlies van het betaalinstrument te melden, al is het alleen maar om weer toegang te krijgen tot de betaalrekening. Dit zijn voor de Commissie overwegingen geweest om in het voorstel het bedrag van 150 euro te verlagen naar 50 euro. Daarbij is volgens de Commissie specifiek voor 50 euro gekozen, omdat dit het gemiddelde bedrag benadert van kaarttransacties in de Europese Unie.[8] Dit bedrag is ook in de uiteindelijke richtlijn gekomen. Voor zover mij bekend maken Denemarken, Estland, Portugal, Zweden, Verenigd Koninkrijk en Noorwegen gebruik van de lidstaatoptie om dit bedrag verder te verlagen.

[8] Dit gemiddelde bedraagt 52 euro. Zie IA, p. 266.

Nederland heeft niet voor een nog lager eigen risico of afschaffing van het eigen risico gekozen, omdat een kleine financiële prikkel passend is om bij verlies van een betaalinstrument snel melding te doen van dit verlies. In de consultatie heeft deze keuze niet tot opmerkingen geleid.

In het geval van een transnationale overboeking geldt dat partijen kunnen kiezen welk recht van toepassing is. Hebben zij niet gekozen, dan geldt op grond van artikel 4 lid 1 onder b van Verordening Rome I[9] dat het recht, en het eigen risico dat in dat recht is opgenomen, van toepassing is van het land waar de betaaldienstverlener zijn gewone verblijfplaats heeft. Dit zal in de praktijk vaak het land van vestiging van de betaaldienstverlener zijn.

Overige

52) De leden van de VVD-fractie vragen in relatie tot dit onderdeel van de memorie van toelichting waarom is gekozen voor een inspanningsverplichting en niet voor een resultaatsverplichting of een plicht tot compensatie.

53) De leden van de VVD-fractie constateren dat het beschreven voorbeeld een casus schetst waarbij de primaire fout bij de consument ligt, die foutief heeft overgeboekt. Hoe verloopt dit voorbeeld als de betalingsinstantie per abuis verkeerd overboekt, in plaats van de consument? Komt ook dan de uiteindelijke verantwoordelijkheid voor verhaal te liggen bij de consument? Is dit evenwichtig?

Er geldt een inspanningsverplichting voor betaaldienstverleners om informatie te verstrekken over de ontvanger van geldmiddelen in het geval een betaler abusievelijk een «verkeerd» rekeningnummer heeft gebruikt om geld naar over te maken (artikel 7:542 lid 3 BW). Denk aan het geval dat een betaler bij een overmaking per ongeluk een verkeerd nummer invoert waardoor het ingevoerde rekeningnummer niet strookt met het door de betaler beoogde rekeningnummer. Het risico dat de geldmiddelen niet meer terug te halen zijn, ligt dan bij de betaler. Hij heeft immers de fout gemaakt door de verkeerde unieke identificator, zoals een rekeningnummer, in te vullen.

In het geval de fout bij de betaaldienstverlener ligt, geldt vanzelfsprekend dat de betrokken betaaldienstverlener de betaler moet compenseren (artikelen 7:543–544 BW). In dat geval is sprake van een resultaatsverplichting. Verloopt een transactie via een betaalinitiatiedienstverlener en treedt daar een fout op, dan is bovendien bepaald dat de betaler ook de rekeninghoudende betaaldienstverlener (vaak de bank) kan aanspreken om gecompenseerd te worden. Dit maakt het voor de betaler eenvoudiger: hij hoeft niet meer uit te zoeken wie precies in de transactie de fout heeft gemaakt. Spreekt de betaler de rekeninghoudende betaaldienstverlener aan, dan heeft deze laatste regres op de betaalinitiatiedienstverlener, als duidelijk is dat die laatste de fout heeft gemaakt (artikel 7:545a BW).

54) De leden van de CDA-fractie vragen naar de uitbreiding van de zorgplicht naar micro-ondernemingen, waar de regering nu niet voor kiest. Deze leden begrijpen deze houding gezien de consultatiereacties. Wel vragen deze leden naar de positie van zzp'ers, en dan met name zzp'ers die ook in loondienst werkzaam zijn of diegene die echt een zeer klein bedrijf hebben. Welk criterium wordt in deze gevallen gehanteerd voor wanneer wel of niet een zorgplicht van toepassing is? Is het mogelijk dat iemand bij gebruik van een particuliere rekening wel met een

[9] Verordening (EG) nr. 593/2008 van 17 juni 2008 inzake het recht dat van toepassing is op verbintenissen uit overeenkomst (Rome I).

zorgplicht tegemoet wordt getreden, maar als diezelfde persoon gebruik maakt van een zakelijke rekening de zorgplicht niet geldt? Welk regime is er van toepassing als iemand zakelijk gebruik maakt van een betaaldienst waarbij wordt gevraagd om het delen van rekeninggegevens, maar dit doet met een particuliere rekening?

De leden van de CDA-fractie merken terecht op dat de richtlijn een onderscheid maakt tussen particulieren (consumenten) en degenen die een betaaldienst gebruiken in het kader van het beroep en bedrijf (artikel 7:514, onderdeel l, BW). Bij een zelfstandige zonder personeel (zzp-er) zal het in de praktijk meestal zo zijn dat deze onder het regime van de zakelijk gebruiker valt, als hij gebruik maakt van de betaalrekening in het kader van zijn beroeps- en bedrijfsactiviteiten. De wet geeft ruimte om aanvullende bescherming of faciliteiten te bieden, voor zover dit voor de betaaldienstgebruiker gunstiger is. Deze ruimte kan de betaaldienstverlener gebruiken om zich te onderscheiden van zijn concurrenten, door bijvoorbeeld producten aan te bieden voor zzp-ers met dezelfde bescherming als die consumenten hebben. Zo zou een betaaldienstverlener een laag eigen risico kunnen hanteren voor zzp-ers, bij verlies van een betaalinstrument. Het staat een betaaldienstverlener vrij om voor betaaldienstgebruikers die geen consument zijn andere voorwaarden aan te bieden, waaronder een hoger of lager eigen risico bij verlies van een betaalinstrument (artikel 61 jo. 74 PSD II).

Op grond van de wet is niet het type rekening doorslaggevend, maar de hoedanigheid van de betaler. Met andere woorden: gebruikt de betaler de betaalrekening voor zijn privéuitgaven of om zijn bedrijf draaiende te houden?
In de praktijk maken rekeninghoudende betaaldienstverleners onderscheid tussen consumenten en zakelijk gebruikers door het aanbieden van verschillende betaalpakketten, met elk hun eigen algemene voorwaarden en tarieven. Het komt voor dat ondernemers met een klein bedrijf gebruik maken van een particuliere rekening. Komt een bank hierachter, dan kan dat reden zijn om bijvoorbeeld de klant te vragen om voor zijn bedrijfsactiviteiten alsnog een zakelijke rekening te openen.

55) Betaaldienstverleners moeten bij een niet-toegestane overboeking onmiddellijk en uiterlijk de volgende werkdag het bedrag terugboeken. De leden van de D66-fractie vragen welke consequenties eraan zijn verbonden wanneer dit de betaaldienstverlener niet lukt? Wat gebeurt er wanneer de dienstverlener intussen failliet is gegaan?

Op grond van artikel 7:528 BW is de betaaldienstverlener verplicht om het bedrag dat is gemoeid met een niet-toegestane transactie terug te boeken. Gebeurt dit niet, dan zal de dienstverlener op grond van het Burgerlijk Wetboek in beginsel aansprakelijk zijn voor de schade die de betaler lijdt als gevolg van het niet-voldoen aan de wettelijke verplichting (6:74 BW). Dit betekent concreet dat bijvoorbeeld eventuele misgelopen rente moet worden vergoed. In het zeer onwaarschijnlijke geval dat een betaaldienstverlener op die bewuste dag failliet gaat, loopt de betaler het risico dat de betaaldienstverlener in gebreke blijft. Toezicht op de financiële soliditeit van de betaaldienstverlener en toezicht op het bestaan en de werking van adequate maatregelen gericht op de bescherming van betaaldienstgebruikers (onder meer de regels inzake vermogensscheiding, verzekering of bankgarantie) kunnen falende betaaldienstverleners en de daaruit voortvloeiende kosten of verliezen voor betaaldienstgebruikers niet voorkomen, maar het risico daarop wel zoveel mogelijk beperken.

56) De leden van de SP-fractie constateren dat elke bank al regels voor niet-toegestane overboekingen heeft. Deze leden menen dat dit de reden is waarom PayPal en I-deal bijvoorbeeld zo populair zijn. De leden van de SP-fractie menen dat het bescherming biedt aan zowel consument als bedrijf en de praktijk wijst uit dat dit werkt. Deze leden vragen de regering waarom er nog meer regelgeving nodig is voor een proces dat goed verloopt.

De leden van de SP-fractie merken terecht op dat banken en andere betaaldienstverleners al de nodige eigen regels hebben over niet-toegestane overboekingen. In zoverre zijn de nieuwe regels over niet-toegestane transacties een verankering van goede handelspraktijken in de wet. Dit komt de consument ten goede, aangezien hij er op kan vertrouwen dat hij binnen de hele Europese Unie goed is beschermd wanneer er sprake is van een niet-toegestane overboeking. Hij is dan niet afhankelijk van de algemene voorwaarden van de betaaldienstverlener. Voor betaaldienstverleners heeft dit het voordeel dat ze binnen de Europese Unie gelijkluidende algemene voorwaarden kunnen gebruiken.

5. Betaaldienstagenten

57) De leden van de SP-fractie constateren dat wat er in de memorie van toelichting wordt gesteld hierover al in werking is getreden. Deze leden stellen dat financiële organisaties al een wettelijke plicht hebben om melding te maken van verdachte transacties. Zij vragen de regering wat PSD II toevoegt ten aanzien van bestaande nationale, Europese en internationale wet- en regelgeving.

Betaaldienstverleners zijn op grond van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) verplicht om ongebruikelijke transacties te melden bij de Financiële inlichtingen eenheid Nederland (FIU-Nederland). Die verplichting vloeit voort uit de Europese anti-witwasrichtlijnen, meest recent de vierde anti-witwasrichtlijn[10]. Omdat de vierde anti-witwasrichtlijn geen onderscheid maakt tussen de verschillende betaaldiensten die betaaldienstverleners kunnen aanbieden, zal deze verplichting ook gelden voor partijen die de betaaldiensten aanbieden die met PSD II worden geïntroduceerd: betaalinitiatiediensten en rekeninginformatiediensten. Voor betaaldienstverleners heeft dit het voordeel dat ze binnen de Europese Unie gelijkluidende algemene voorwaarden kunnen gebruiken.

6. Toegang tot betalingssystemen en betaalrekeningen

58) De leden van de PVV-fractie merken allereerst op, dat de Europese Commissie de door de financiële nieuwkomers gewenste techniek om toegang te krijgen tot de informatie over rekeningen van bankklanten heeft verworpen. Deze leden willen weten welke techniek de financiële nieuwkomers hebben voorgesteld en waarom de Europese Commissie deze techniek heeft verworpen.

Van een voorstel van financiële nieuwkomers voor technische standaarden of een bepaalde techniek is geen sprake geweest en evenmin van het verwerpen van een dergelijk voorstel door de Europese

[10] Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie (PbEU 2015, L 141).

Commissie. Op 13 maart 2018 heeft de Europese Commissie de technische standaarden over sterke cliëntauthenticatie gepubliceerd.[11]

In deze technische standaarden is geregeld hoe derde partijen toegang tot de betaalrekening kunnen krijgen. Er zijn nog twee vormen mogelijk. De eerste vorm is toegang via de interface die de betaaldienstgebruiker gebruikt. Derde partijen maken dan gebruik van methoden waarbij zij direct inloggen op de omgeving die de betaaldienstgebruiker gebruikt (*consumer interface*). De derde partij dient zich hierbij te identificeren. De tweede vorm is via een *dedicated interface* (via *Application Programming Interfaces*, zie vraag 59), waarbij rekeninghoudende betaaldienstverleners een speciale digitale omgeving bouwen waarop derde partijen zich kunnen aansluiten. Het betreft een aparte interface, speciaal om derde partijen toegang te verlenen. De technische standaarden verbieden vanaf september 2019 toegang via de omgeving die de klant gebruikt zonder identificatie (dit wordt ook wel *screen scraping* genoemd).

De definitieve tekst van de technische standaarden bepaalt dat er ten minste één interface moet zijn waarmee de derde partij toegang kan krijgen. Idealiter gebeurt dit middels een *dedicated interface*. Deze interface moet dezelfde mogelijkheden en mate van beschikbaarheid hebben als de interface die de betaaldienstgebruiker gebruikt (*consumer interface*). Indien een rekeninghoudende betaaldienstverlener een *dedicated interface* aanbiedt, worden derde partijen geacht deze methode te gebruiken. In het geval dat een rekeninghoudende betaaldienstverlener geen *dedicated interface* aanbiedt, of in het geval dat deze interface van onvoldoende kwaliteit is, mogen derde partijen gebruik maken van methoden waarbij zij direct inloggen op de omgeving die de klant gebruikt. Deze laatste methode is met strenge voorwaarden omkleed, om tegemoet te komen aan bezwaren op het gebied van privacy en gegevensbescherming. Zo moet de derde partij zich identificeren, zodat de bank het onderscheid kan maken tussen de eigen klant en de derde partij.

59) Voorts willen de leden van de PVV-fractie weten welke techniek om toegang te krijgen tot de informatie over rekeningen van bankklanten de banken hebben voorgesteld en of het klopt dat deze techniek de norm wordt. Kan de regering toelichten hoe een zogeheten application programming interface (API) precies werkt en op welke wijze banken de controle zullen houden ten aanzien van de informatie over rekeningen van hun klanten?

De techniek die nu in de technische standaarden wordt gereguleerd, is voorgesteld door de Europese Bankautoriteit (EBA), in nauw overleg met de Europese Centrale Bank (ECB), en overgenomen door de Europese Commissie (EC). Zoals genoemd in de beantwoording van vraag 58 kan er op twee manieren toegang verleend worden. Hetzij via de methode waarbij derde partijen de interface voor de betaaldienstgebruiker gebruiken en waarbij de derde partij zich moet identificeren (*consumer interface*), hetzij via een zogenaamde *dedicated interface.* Rekeninghoudende betaaldienstverleners bepalen zelf de manier waarop zij deze toegang aan derde partijen verlenen.

De techniek voor het verkrijgen van toegang tot de betaalrekening via de *dedicated interface* is door gebruik te maken van een API (A*pplication Programming Interface*). Een API maakt, kort gezegd, communicatie en

[11] Gedelegeerde verordening (EU) 2018/389 van de Commissie van 27 november 2017 tot aanvulling van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad wat betreft technische reguleringsnormen voor sterke cliëntauthenticatie en gemeenschappelijke en veilige open communicatiestandaarden (PbEU 2018, L69)

het uitwisselen van informatie mogelijk tussen verschillende (software) systemen. De API zorgt ervoor dat de juiste response (antwoord) wordt teruggestuurd naar degene die het verzoek om informatie (data) heeft gedaan. Welke verzoeken om informatie worden ondersteund door de API, is door de bank zelf te bepalen. Ook is het mogelijk om bepaalde verzoeken om informatie af te schermen voor specifieke gebruikers. Zo kan door middel van authenticatie dezelfde API worden gebruikt voor verschillende doeleinden. Welke rekeninginformatie van de klanten als «response» wordt verstuurd door de API, is dus afhankelijk van het verzoek om informatie dat is gedaan.

60) Tevens willen de leden van de PVV-fractie weten wat de voor- en nadelen van de API zijn en wat de gevolgen hiervan zijn voor de financiële nieuwkomers. Wat zijn verder de gevolgen voor de consumenten? Voorts willen de leden van de PVV-fractie weten of de nieuwe techniek definitief is. Zo nee, wanneer zal hier meer duidelijkheid over komen en hoe zal de Tweede Kamer hiervan op de hoogte worden gehouden?

Eén van de technieken voor het verkrijgen van toegang tot de betaalrekening is, zoals uiteengezet bij de beantwoording van vraag 59, het gebruik van een API (*Application Programming Interface*). De grootbanken in Nederland hebben aangekondigd dat zij een *dedicated interface* zullen aanbieden. Het gebruik van een *dedicated interface* heeft voor zowel de consument, de rekeninghoudende betaaldienstverlener als de derde partijen bepaalde voordelen, onder meer omdat deze manier het meest veilig wordt geacht: de hoeveelheid informatie die de *dedicated interface* verstrekt wordt bepaald door het verzoek om informatie. Zo wordt enkel de informatie verstrekt die nodig is voor het verlenen van de betreffende betaaldienst en waarvoor opdracht/toestemming gegeven is. Daarnaast hoeven derde partijen bij het gebruik van een *dedicated interface* minder maatregelen te nemen voor het verwerken van gevoelige gegevens, minder informatie op te slaan en minder informatie te verwerken. Voor consumenten biedt deze manier de zekerheid dat derde partijen alleen toegang krijgen tot de gegevens waarvoor de klant opdracht of toestemming heeft gegeven.

Als de derde partij toegang krijgt via de interface die de betaaldienstgebruiker gebruikt (*consumer interface*), beschikt de derde partij in beginsel over dezelfde gegevens als waarover de betaaldienstgebruiker beschikt. Hierdoor bestaat weliswaar niet het risico dat te weinig gegevens worden verstrekt aan een derde partij waardoor deze niet in staat is de gevraagde betaaldienst te verlenen, maar krijgt de derde partij wel toegang tot meer gegevens dan nodig voor het verlenen van de gevraagde betaaldienst. Omdat de derde partij zich wel moet kunnen identificeren, kan er in geval van misbruik worden vastgesteld welke partij hiervoor verantwoordelijk is.

De Europese Commissie heeft op 13 maart 2018 de definitieve tekst van de technische standaarden over sterke cliëntauthenticatie gepubliceerd.

61) De leden van de CDA-fractie vragen naar de bewegingsruimte die bijvoorbeeld banken hebben om betaaldienstverleners toegang te geven tot betaalrekeningen. Deze leden begrijpen dat de ene betaaldienstverlener dezelfde toegang zou moeten hebben als een andere betaaldienstverlener, maar zij vragen of degene die uiteindelijk toestemming geeft voor het delen van rekeninginformatie zelf wel een onderscheid mag maken in wat er gedeeld wordt met de ene betaaldienstverlener en met de andere betaaldienstverlener. Verder vragen deze leden of deze passage ook kan inhouden dat banken zelf een keuze hebben in op welke wijze en welke informatie zij delen met betaaldienstverleners, als zij er maar voor

zorgen dat elke betaaldienstverlener op dezelfde manier wordt behandeld. Deze leden vragen of het op deze manier kan dat banken een zeer beperkt aantal gegevens verstrekken.

PSD II geeft de rekeninghouder het recht om gebruik te maken van nieuwe betaaldienstverleners die diensten verlenen waarbij toegang nodig is tot de betaalrekening van de rekeninghouder, mits de rekeninghouder hiervoor toestemming geeft. In dat geval zijn banken verplicht toegang te verlenen. PSD II schrijft voor dat een bank betaalopdrachten die verstrekt zijn via een betaaldienstverlener niet anders behandelt dan opdrachten die de betaler rechtstreeks verstrekt. Evenzo bepaalt PSD II dat een bank verzoeken om informatie van een rekeninginformatiedienstverlener niet discrimineert, anders dan om objectieve redenen. Daarvan kan sprake zijn bij ongeautoriseerde toegang (zonder juiste toestemming van de betaaldienstgebruiker) of frauduleuze toegang (door iemand die zich voordoet als de betaaldienstgebruiker) tot de betaalrekening. De vraag welke informatie een bank deelt met een betaaldienstverlener is afhankelijk van de techniek bij de onderlinge communicatie. Als een bank een *dedicated interface* gebruikt, kan zij – zoals bij het antwoord op vraag 60 uiteengezet is – de aard en hoeveelheid beheersen van de informatie waartoe een derde partij toegang krijgt. Daarbij zijn zowel de bank als de derde partij gehouden aan het PSD II-vereiste van dataminimalisatie, alsmede aan de Algemene Verordening Gegevensbescherming. Daarmee is gewaarborgd dat alleen toegang wordt verleend tot die gegevens die nodig zijn om de betaaldienst te verlenen.

62) De leden van de CDA-fractie maken zich zorgen over de mogelijkheid voor «screen scraping» die met de implementatie van onderhavig wetsvoorstel gemoeid zou zijn. Deze leden begrijpen dat toegang tot gegevens in principe via een API zal gebeuren, maar indien dit (nog) niet werkt, er een terugvaloptie beschikbaar moet zijn in de vorm van «screen scraping», waarbij de consument zijn inloggegevens verstrekt aan een derde partij. Deze leden zien hierbij grote gevaren op de loer liggen, waarbij onwetende consumenten aan criminelen gegevens verstrekken. Daarbij is deze manier van gegevens verstrekken in strijd met wat altijd aan consumenten is verteld, namelijk om nooit inloggegevens te verstrekken aan wie dan ook. Deelt de regering deze zorgen en wat gaat zij doen om aan deze zorgen tegemoet te komen. Kan de regering duiden hoe de lagere regelgeving vanuit de Europese Commissie, via technische reguleringsnormen die openbaar zijn geworden op 27 november 2017, exact hiervoor uitpakt.

De regering deelt de zorgen van het CDA wat betreft de risico's die samenhangen met «screen scraping». In een toelichting d.d. 27 november 2017 bij haar voorstel voor de technische standaarden over sterke cliëntauthenticatie en veilige communicatie geeft de Europese Commissie aan dat *screenscraping*, een methode waarbij een derde partij zonder identificatie op geautomatiseerde wijze inlogt op de digitale omgeving bij de rekeninghoudende betaaldienstverlener en gegevens afleest vanuit de interface van de betaaldienstgebruiker zonder identificatie, verboden wordt.[12]

Zoals eerder aangegeven, regelen de technische standaarden twee manieren waarop derde partijen toegang kunnen krijgen tot een betaalrekening, namelijk middels een methode waarbij de derde partij direct inlogt op de interface die de betaaldienstgebruiker gebruikt, en waarbij de derde partij zich moet identificeren (*consumer interface*) of middels een

[12] In de technische standaarden zelf volgt dit uit de artikelen 27 en 28, waarin identificatie als eis wordt gesteld.

dedicated interface. De rekeninghoudende betaaldienstverlener bepaalt welke methode wordt gebruikt.

Van s*creen scraping* is sprake als een derde partij direct inlogt op de interface van de betaaldienstgebruiker en zich daarbij niet identificeert. Die methode is in ieder geval niet toegestaan.

De terugvaloptie is (pas) van toepassing indien een rekeninghoudende betaaldienstverlener een *dedicated interface* aanbiedt, maar deze niet aan alle eisen voldoet. In het geval een *dedicated interface* niet voldoet, dient de rekeninghoudende betaaldienstverlener een tweede systeem klaar te hebben staan waarbij, onder strikte voorwaarden, de derde partij toegang wordt verleend via de *consumer interface*. Pincodes hoeven daarbij nooit te worden afgegeven aan derde partijen. Wel kan het zo zijn dat tancodes/verificatiecodes/responsecodes worden gevraagd door de derde partij. Deze codes worden per specifieke transactie gegenereerd. Dit betekent dat als het bedrag of de begunstigde verandert, er een nieuwe code wordt gegenereerd. Daarmee wordt het risico op misbruik verkleind. Indien de betaaldienstgebruiker het niet vertrouwt, kan hij ervoor kiezen om van de desbetreffende betaaldienstverlener die deze methode hanteert, geen gebruik te maken. Vaak zal men ook nog op andere manieren of met andere betaalmethodes kunnen betalen. Artikel 97, derde lid, PSD II schrijft bovendien voor dat betaaldienstverleners (dus ook betaalinitiatie- en rekeninginformatiedienstverleners) beveiligingsmaatregelen treffen die de vertrouwelijkheid en integriteit van persoonlijke beveiligingsgegevens beschermen. Een voorbeeld van dergelijke beveiligingsmaatregelen is encryptie, waarbij de persoonlijke beveiligingsgegevens (zoals inloggegevens) op een onleesbare manier worden ingevoerd bij de derde partij. De persoonlijke beveiligingsgegevens hoeven dus niet zichtbaar (openlijk) te worden gedeeld met de derde partij. Daarnaast worden de risico's nog verder beperkt doordat een bank de betaalinitiatie- of rekeninginformatiedienstverlener zal identificeren, en dus zal moeten vaststellen of de derde partij onder toezicht staat. Hiermee wordt voorkomen dat criminele partijen toegang krijgen.

In Nederland stimuleert DNB het ontwikkelen en gebruik van een *dedicated interface*. De technische standaarden bepalen dat rekeninghoudende betaaldienstverleners een vrijstelling kunnen krijgen van bovenstaande terugvaloptie indien zij ex post kunnen aantonen dat hun *dedicated interface* aan alle eisen voldoet. In geval van een verleende vrijstelling hoeft de rekeninghoudende betaaldienstverlener geen tweede systeem voorhanden te hebben dat toegang via de *consumer interface* mogelijk maakt. Deze vrijstelling wordt afgegeven door de nationale toezichthouder (dit is in Nederland de Nederlandsche Bank) na consultatie van de Europese Bankautoriteit (EBA).

63) De leden van de SP-fractie vragen de regering hoe zij misbruik van deze regeling, waarbij de gegevens vanaf een computerbeeldscherm worden uitgelezen en gebruikt voor invoer in een ander, achterliggend programma, oftewel screen scraping, wil tegengaan.

Van s*creen scraping* is, zoals gezegd, sprake als een derde partij direct inlogt op de interface van de betaaldienstgebruiker en zich daarbij niet identificeert.

De technische standaarden verbieden deze vorm van toegang tot de betaalrekening. Het gebruik van een *dedicated interface* voor derde partijen wordt zoveel mogelijk gestimuleerd. Voor een nadere toelichting verwijs ik naar het antwoord op vraag 62.

64) De leden van de SP-fractie vragen de regering of zij inzicht heeft hoeveel misbruik er gemaakt kan worden van de in dit onderdeel van de memorie van toelichting genoemde faciliteit. Deze leden constateren dat gegevens die worden geëxporteerd naar een niet-EU/EER land geen juridische bescherming meer genieten en deze leden stellen dat het onmogelijk is om als burger je gelijk te halen. De voorgenoemde leden constateren voorts dat, zoals gesteld in het rondetafelgesprek van 15 november 2017, tussentijds toestemming intrekken niet mogelijk is. Zij vragen de regering dit eerst te onderzoeken voordat zij dit gedeelte van PSD II in werking laat treden.

Zoals met alle diensten, is het niet uitgesloten dat er – ondanks alle voorafgaande onderzoeken in het kader van de vergunningverlening – partijen met een vergunning zullen zijn die betaaldiensten zullen aanbieden met als doel het verrichten van frauduleuze betalingen of het misbruik maken van gegevens. Om misbruik tegen te gaan kan een bank een rekeninginformatiedienstverlener of een betaalinitiatiedienstverlener de toegang tot een betaalrekening ontzeggen om objectieve en op voldoende aanwijzingen gebaseerde redenen in verband met niet-toegestane of frauduleuze toegang tot de betaalrekening door een dergelijke dienstverlener, waaronder de niet-toegestane of frauduleuze initiëring van een betalingstransactie (artikel 523, vijfde lid, Boek 7 BW). De bank dient een dergelijk incident onmiddellijk te melden bij DNB. DNB kan na beoordeling van de zaak zo nodig passende maatregelen nemen. Bovendien kan in gevallen van strafbare feiten, bijvoorbeeld bij het plegen van valsheid in geschrifte (artikel 225 Sr), over worden gegaan tot strafvervolging door het openbaar ministerie.

Als een betaaldienstgebruiker opdracht geeft aan een betaaldienstverlener voor het verlenen van een bepaalde betaaldienst en de betaaldienstverlener toestemming geeft voor het verkrijgen van toegang tot zijn betaalrekening voor dat doel, verwerkt de betaaldienstverlener persoonsgegevens. Op deze verwerkingen is de AVG van toepassing. In gevolge de AVG mag een betaaldienstverlener persoonsgegevens alleen verstrekken aan een derde of gebruiken voor een ander doel dan waarvoor ze zijn verzameld als daarvoor een juridische grondslag bestaat. Daarvan kan bijvoorbeeld sprake zijn als de betaaldienstgebruiker hiervoor toestemming heeft verleend of als dit noodzakelijk is voor de uitvoering van een overeenkomst. De AVG geeft waarborgen voor verwerking van persoonsgegevens buiten de Unie. Ik ga hier in het kader van de beantwoording van vraag 67 nader op in. De rechtsgrondslag voor het verkrijgen van toegang tot persoonsgegevens voor het verlenen van betaaldiensten is veelal het uitvoeren van een overeenkomst, namelijk die tussen een betaaldienstgebruiker en een betaaldienstverlener. Als een betaaldienstgebruiker niet meer wenst dat een betaaldienstverlener toegang heeft tot zijn betaalrekening, kan hij de overeenkomst met de betaaldienstverlener opzeggen. Ook is het mogelijk om tussentijds toestemming te wijzigen of in te trekken. De betaaldienstverlener moet de betaaldienstgebruiker voorafgaand aan het sluiten van de overeenkomst duidelijk informeren over de procedure hiervoor.

Daarnaast zijn er technische waarborgen die de toegang van derde partijen tot de betaalrekening beperken. Ik verwijs hiervoor naar het antwoord op vraag 65.

65) De leden van de SP-fractie zouden graag zien dat Nederland regelt dat mensen per keer toestemming verlenen voor het uitwisselen van betaalgegevens en dat zij daarbij ook grenzen kunnen aangeven. Zodat zij bijvoorbeeld hun pingedrag of waar zij precies aankopen doen, kunnen afschermen. Deze informatie is namelijk goud waard maar kan ook leiden

tot problemen. Het schendt bijvoorbeeld de privacy als een hypotheekverstrekker inzicht heeft in hoeveel geld iemand uitgeeft aan een hobby.

In de eerste plaats moet onderscheid gemaakt worden tussen uitdrukkelijke toestemming van de betaaldienstgebruiker voor het verlenen van de betaaldienst en daarmee voor het verlenen van toegang tot de betaalrekening aan de betaaldienstverlener (artikelen 66(2) en 67 (2)(a) van PSD II) en uitdrukkelijke toestemming van de betaaldienstgebruiker voor toegang tot persoonsgegevens die noodzakelijk zijn voor het verlenen van betaaldiensten (artikel 94(2) PSD II).

Als een betaaldienstgebruiker gebruik wil maken van een betaalinitiatiedienst of rekeninginformatiedienst dient hij daartoe een overeenkomst te sluiten met een betaalinitiatie- of rekeninginformatiedienstverlener. In of bij deze overeenkomst dient de betreffende betaaldienstverlener de betaaldienstgebruiker om uitdrukkelijke toestemming te vragen voor de toegang tot persoonsgegevens die nodig zijn om de betreffende betaaldienst te verlenen (artikel 94(2) PSD II). Als de overeenkomst is gesloten en die uitdrukkelijke toestemming is verleend dient een betaaldienstgebruiker in geval van een betaalinitiatiedienst in beginsel voor het initiëren van elke betalingstransactie afzonderlijk uitdrukkelijk toestemming te verlenen aan de betaalinitiatiedienstverlener (artikel 66(2) PSD II). Dit is in feite een opdracht tot het initiëren van de betreffende betalingstransactie. Nadat de betaaldienstgebruiker zich via sterke cliëntauthenticatie heeft geïdentificeerd jegens de betaaldienstverlener, krijgt deze laatste toegang tot de betaalrekening en kan de opdracht worden uitgevoerd. Voor gebruik van een rekeninginformatiedienst is de uitdrukkelijke toestemming (artikel 67(2)(a) PSD II) van de betaaldienstgebruiker tot negentig dagen geldig. Als meer dan negentig dagen zijn verstreken sinds de laatste keer dat de betaaldienstgebruiker toestemming gaf aan de rekeninginformatiedienstverlener voor het verkrijgen van toegang tot zijn betaalrekening, wordt de betaaldienstgebruiker opnieuw om toestemming gevraagd. Geeft de gebruiker de toestemming niet, dan heeft de betaaldienstverlener vanaf dat moment niet langer toegang tot de betaalrekening.

De afscherming van gegevens (door een bank) kan in de praktijk plaatsvinden via een speciaal elektronisch portaal (de Application Programming Interface (API)), ofwel de *dedicated interface*. Als een derde partij via de reguliere consumenteninterface toegang zou krijgen tot de betaalrekening, krijgt deze in beginsel dezelfde informatie te zien als de rekeninghouder, hetgeen meer is dan nodig zal zijn voor het verlenen van de gevraagde betaaldienst. Zo krijgt een derde partij daardoor bijvoorbeeld niet alleen betaalrekeningen, maar ook andere rekeningen te zien.

Verder is tijdens het Maatschappelijk Overleg Betalingsverkeer () van november 2017 gesproken over consumentenbeschermende maatregelen, zoals de mogelijkheid voor consumenten om het verlenen van toegang aan rekeninginformatiedienstverleners bij voorbaat uit te schakelen bij hun bank. Dit heeft er inmiddels in geresulteerd dat het MOB heeft aangegeven graag te zien dat banken consumenten in mobiel bankieren apps en bij internetbankieren een overzicht bieden van de dienstverleners waaraan toestemming is verleend voor rekeninginformatiediensten.

De rechtsgrondslag voor het verkrijgen van toegang tot de betaalrekening, en daarmee tot persoonsgegevens, is veelal het uitvoeren van een overeenkomst, namelijk de overeenkomst voor het verlenen van de betreffende betaaldienst. In deze overeenkomst moet duidelijk zijn aangegeven voor welk doel (welke betaaldienst) en tot welke persoonsgegevens precies toegang wordt gevraagd en waarvoor dus toestemming

van de betaaldienstgebruiker nodig is. Bij verwerking van gegevens buiten deze doelen zal volgens de Algemene verordening gegevensbescherming wel sprake moeten zijn van verenigbare doelen (zie artikel 6, vierde lid, AVG voor een indicatie wanneer daar sprake van is). Als deze nieuwe doelen niet verenigbaar zijn met het oorspronkelijke doel van de verwerking, dan is toestemming noodzakelijk (of een wettelijke bepaling die tot de verwerking noopt, zie artikel 6, vierde lid, AVG). Deze vorm van toestemming betreft een rechtsgrondslag voor verwerking van persoonsgegevens op grond van de AVG en moet onderscheiden worden van de hiervoor genoemde vormen van toestemming ingevolge PSD II.

66) De leden van de PvdD-fractie constateren dat banken een belangrijke functie hebben in onze samenleving. Zij dienen de financiële middelen van burgers en ondernemingen op deugdelijke wijze te beschermen en te beheren, en daarbij dus uiterste zorg te dragen voor hun privacy. Betaalgegevens van mensen behoren immers tot de meest persoonlijke informatie die zij bezitten. Maar ook het al kwetsbare bancaire stelsel wordt met de komst van PSD II slachtoffer van de economisering van informatie en raakt het contact met haar klanten kwijt. De leden van de PvdD-fractie vragen of de regering uitgebreid in kan gaan op dit punt en voorts op de veranderende positie van banken door de toenemende invloed van (giga-) techbedrijven?

Het doel van PSD II is om de EU-markt voor elektronische betalingen verder te helpen ontwikkelen, waardoor consumenten, handelaren en andere marktpartijen volledig de voordelen kunnen genieten van de Europese interne markt, met name waar het gaat om handel via internet. Hierbij kan gedacht worden aan meer betaalgemak, met name bij internetaankopen in andere EU-landen, meer keuzemogelijkheid in en transparantie van betaaldiensten, meer rechtszekerheid en op termijn zou dit ook moeten leiden tot lagere kosten voor het gebruik van betaaldiensten. Dit kan alleen bewerkstelligd worden als meer partijen toegang kunnen krijgen tot de betaalmarkt, er meer innovatie van betaaldiensten plaatsvindt en er een gelijk speelveld gecreëerd wordt voor zowel bestaande als nieuwe, innovatieve partijen op de betaalmarkt. Alle partijen die betaaldiensten willen aanbieden op de Europese markt moeten voldoen aan dezelfde strenge regels, moeten in het bezit zijn van een vergunning om hun diensten te mogen aanbieden en staan onder permanent toezicht. Mogelijk zullen niet alleen kleine FinTech-bedrijven toegang vragen tot de Europese betaalmarkt, maar zullen ook grote technologiebedrijven (BigTech bedrijven) een vergunning aanvragen voor het verlenen van bancaire dan wel betaaldiensten, voor zover zij deze nog niet hebben. De opkomst van zowel grote als kleine technologiebedrijven binnen de financiële sector zal de rol van traditionele banken naar verwachting op termijn fundamenteel veranderen. Hoe snel deze verandering zal plaatsvinden is op voorhand niet te voorspellen. Traditionele banken zullen strategische keuzes moeten maken om te kunnen concurreren dan wel samen te werken met innovatieve FinTech-bedrijven. Technologisch-innovatieve bedrijven zorgen daarmee voor vernieuwing in de financiële sector wat kan leiden tot meer keuzemogelijkheden voor consumenten en lagere prijzen.

67) De leden van de PvdD-fractie zien dat, onder het mom van innovatie en vermarkting als kennelijk noodzakelijk verdienmodel, bovengenoemde kerntaken van banken op de tweede plaats komen te staan. Hiermee verliezen banken hun belangrijkste taak om gegevens te (kunnen) beschermen tegen de toenemende informatie-oorlog en worden mogelijk grote bedrijven als Google binnenkort nóg meer eigenaar van ónze gegevens. Erkent de regering dat er geen garanties zijn dat dergelijke bedrijven de financiële gegevens van burgers net zo goed (moeten)

beschermen als banken? Zo nee, waarom niet? Deelt de regering de mening dat dit juist een taak is die enkel aan banken moet worden toevertrouwd? Zo nee, waarom niet? Deelt de regering de mening dat het zeer onwenselijk is dat giga-techbedrijven als Google zich in toenemende mate een informatiemonopolie weten toe te eigenen? Zo nee, waarom niet?

Zowel bestaande als nieuwe partijen die betaaldiensten aanbieden op de Europese betaalmarkt, of dat nu banken zijn, FinTech-start-ups of grote technologiebedrijven, moeten zich niet alleen aan PSD II houden, maar ook aan de Europese gegevensbeschermingsregelgeving. Vanaf 25 mei 2018 is dat de Algemene verordening gegevensbescherming (AVG). Deze verordening geeft strikte regels voor de verwerking van persoonsgegevens waaraan zowel banken als andere betaaldienstverleners zich zullen moeten houden. In Nederland zal de Autoriteit Persoonsgegevens op de naleving van deze verordening toezien. De AVG bevat in hoofdstuk V ook de nodige waarborgen voor verwerking van gegevens buiten de grenzen van de Europese Unie/EER (zgn. «derde landen»). Doorgifte aan derde landen mag in het bijzonder niet leiden tot ondermijning van het door de verordening gewaarborgde beschermingsniveau (artikel 44 AVG). Persoonsgegevens mogen in een derde land worden verwerkt indien er een «adequaatheidsbesluit» is van de Europese Commissie waarin – kort gezegd – is beoordeeld dat het derde land persoonsgegevens voldoende beschermt. In deze beoordeling wordt onder meer gekeken naar de staat van de rechtstaat van het betrokken land, het aanwezige toezicht en de deelname van het derde land aan internationale verdragen, met name op het gebied van gegevensbescherming (artikel 45 AVG). Verder is verwerking in een derde land mogelijk wanneer er voldoende waarborgen zijn in de zin van artikel 46 AVG. Hieraan kan worden voldaan door bindende bedrijfsvoorschriften, het gebruik van door de Europese Commissie ontworpen modelcontracten en, na toestemming van de toezichthouder, het gebruik van bepaalde contractsbepalingen om voldoende bescherming van persoonsgegevens te verzekeren. Voor specifieke situaties is een uitzondering mogelijk, onder meer vanwege gewichtige redenen of wanneer de betrokkene instemt na te zijn voorgelicht over eventuele risico's van doorgifte aan het derde land (artikel 49 AVG). Wanneer het bedrijf actief is in de Europese Unie of zijn diensten aanbiedt zal de nationale toezichthouder op de hiervoor genoemde regels kunnen toezien, ongeacht of de verwerking in de Unie al dan niet plaatsvindt (artikel 3, eerste en tweede lid, AVG). Daarmee is de bescherming van persoonsgegevens voldoende geborgd, ook indien grote bedrijven in derde landen deze persoonsgegevens verwerken.

PSD II stelt daarnaast als aanvullende voorwaarde dat een betaaldienstverlener uitdrukkelijk toestemming nodig heeft van de betaaldienstgebruiker om toegang te krijgen tot persoonsgegevens voor het verlenen van betaaldiensten. Deze eis geldt bovenop de eisen die de AVG stelt aan verwerking van persoonsgegevens. De nieuwe regelgeving laat overigens de bestaande mededingingsregels in stand, waaronder het verbod om misbruik te maken van een economische machtspositie (artikel 24 Mededingingswet).

7. Vergoeding voor het gebruik van betaalinstrumenten

68) 69) 70) 73) 74) 75) De leden van de fracties van de PVV en GroenLinks vragen naar de voor- en nadelen van het gedeeltelijk verbod op surcharging ten op zichte van een algeheel verbod op surcharging en willen weten waarom de regering niet voor een algeheel verbod op surcharging heeft gekozen. De leden van de fracties van de VVD, D66 en GroenLinks vragen naar de effecten van het gedeeltelijk verbod op

surcharging in PSD II op het gelijke speelveld, op concurrentie en daarmee de lange termijn innovatie in de sector, en voorts welke regels ten aanzien van surcharging zullen gelden voor toekomstige toetreders tot de betaalmarkt.

Een verbod op surcharging richt zich op het verbieden van het door winkeliers in rekening brengen van kosten voor betaalkaarttransacties bij de consument. Door het verbieden van die doorberekening is het voor de consument bij aanvang van de transactie duidelijk wat de totale prijs van een dienst of product wordt. Hij wordt niet meer in een laat stadium geconfronteerd met bijkomende kosten voor het gebruik van een bepaald betaalmiddel. Denk aan het geval dat een vliegticket wordt besteld en vlak voor de definitieve boeking nog een extra toeslag in rekening wordt gebracht voor het gebruik van een betaalmiddel, waardoor de definitieve prijs hoger wordt. Na implementatie van PSD II zal deze praktijk in verreweg de meeste gevallen tot het verleden behoren.

PSD II verbiedt specifiek het doorberekenen van kosten voor het gebruik van betaalmiddelen waarvan de tarieven zijn geplafonneerd door de Verordening inzake afwikkelingsvergoedingen (betalingen onder de MIF-verordening), zoals debet- en de meeste creditcards, alsook het doorberekenen van kosten bij Europese overschrijvingen en Europese automatische incasso's (betalingen onder de SEPA-verordening). Voor het gebruik van overige betaalmiddelen, waarvan de tarieven niet zijn geplafonneerd, mogen winkeliers wel een vergoeding vragen. Dit betreft de vaak duurdere creditcards die doorgaans extra service bieden aan hun klanten in de vorm van welkomstcadeautjes, verzekeringen, spaarprogramma's e.d., die eventueel extra kosten kunnen opleveren. PSD II bevat evenwel een lidstaatoptie om ook te verbieden dat kosten voor het gebruik van die betaalinstrumenten worden doorberekend. Daar wordt geen gebruik van gemaakt, zoals hierna aan de hand van drie argumenten wordt besproken.

Met het verbod op surcharging wordt onderscheid gemaakt tussen debitcards en creditcards uitgegeven door zogeheten vierpartijenschema's (vallend onder het verplicht gestelde verbod) en creditcards uitgegeven door driepartijen-schema's (niet vallend onder het verplicht gestelde verbod). Voor deze laatste groep is het verplicht gestelde gedeeltelijke verbod op surcharging in beginsel niet van toepassing.[13] Aangezien creditcards gebaseerd op driepartijenschema's in Nederland maar zeer beperkt gebruikt worden, is het verbod in feite van toepassing op vrijwel alle kaarttransacties in Nederland. Het verbod geldt zowel voor bestaande aanbieders als voor nieuwe toetreders.

Voor iDEAL-betalingen geldt dat winkeliers niet apart kosten in rekening kunnen brengen voor de onderliggende overschrijving, maar wel voor de kosten van de iDEAL-dienstverlening.

---

[13] Een transactie voor de aankoop van een product met een betaling via een creditcard kent naast een betaler (consument) en een ontvanger (winkelier) doorgaans zowel een betaaldienstverlener voor de betaler (kaartuitgever) als een betaaldienstverlener voor de ontvanger (kaartacceptant). Dit is een «vierpartijenschema». Hiernaast bestaan driepartijenschema's, waar niet twee verschillende betaal-dienstverleners bij de transactie betrokken zijn (één namens de consument en één namens de winkelier), maar waar de kaartuitgever en de kaartacceptant één en dezelfde betaaldienstverlener is («pure» driepartijenschema's). Tot slot bestaan driepartijenschema's «plus», waarvoor geldt dat een andere betaaldienstaanbieder een licentie voor de acceptatie van op kaarten gebaseerde transacties of de uitgifte van op kaarten gebaseerde betaalinstrumenten verleent, of dat dergelijke betaal-instrumenten via een agent of samen met een co-brandingpartner worden uitgegeven: deze worden als vierpartijenschema's beschouwd en vallen ook het verplicht gestelde gedeeltelijke verbod op surcharging in PSD II waarvan de kosten niet mogen worden doorberekend aan de consument.

Er is door de leden van de fracties van de PVV en GroenLinks gevraagd naar de voor- en nadelen van een algeheel verbod op surcharging. In het wetsvoorstel is gekozen voor het door PSD II verplicht gestelde gedeeltelijke verbod op surcharging en niet voor de lidstaatoptie van uitbreiding naar een algeheel verbod. Ten eerste ligt het voor de hand dat winkeliers als gevolg van het verbod op surcharging de kosten van gebruik van betaalkaarten zullen doorberekenen in de prijzen van hun producten en diensten. Bij een volledig verbod betekent dit echter dat ook de kosten van de relatief dure betaalkaarten worden doorberekend in de productprijzen, waardoor ook consumenten die kiezen voor een goedkope betaalkaart meebetalen aan de kosten van het gebruik van dure betaalkaarten. Hierdoor zal er geen prikkel meer zijn voor consumenten om te kiezen voor goedkope en efficiënte betaalkaarten, hetgeen de regering eveneens niet wenselijk vindt. De hogere prijzen voor iedereen als voor de hand liggend gevolg van een verbod op surcharging zijn tijdens de behandeling van het wetsvoorstel verbod toeslag gebruik betaalmiddelen bij consumenten aan de orde geweest, en werden door verschillende leden van uw Kamer als onwenselijk beschouwd.[14] Het lid De Vries (VVD) gaf hierover aan: «*Dure opties, zoals American Express en de zakelijke kaarten van MasterCard en Visa, worden nu ook onder dit verbod geschaard. Waarom kiest de initiatiefnemer daarvoor? Dan zorg je toch uiteindelijk voor een grotere kostenstijging?*» en «*De consument die nu gebruikmaakt van een goedkoop betaalmiddel, betaalt straks uiteindelijk mee aan het gebruik van een duurder betaalmiddel door een andere consument*». Het lid Merkies (SP) zei: «*Gaan betalers van een debetkaart, dus van een gewone pinpas die wij allemaal kennen, dan ongevraagd meebetalen aan de hogere kosten die gepaard gaan met creditcardbetalingen? Dat lijkt mij een zeer ongewenste situatie. Het zou zonde zijn, want we hebben een bijzonder efficiënt betalingsverkeer in Nederland...*» Het lid Dijkgraaf (SGP) tot slot gaf aan: «*Hoe verhoudt zich dat verder tot het aanmoedigen van het efficiëntste betaalmiddel? Dat is wat de Kamer eigenlijk wil. We moeten prikkels in prijzen inbouwen, zodat mensen gebruik gaan maken van het goedkoopste systeem.*»

Bij het inzetten van de lidstaatoptie moet volgens PSD II rekening worden gehouden met de belangen van meer concurrentie en het gebruik van efficiënte betaalmiddelen. Ten tweede kan een algeheel verbod tot gevolg hebben dat winkeliers ervoor kiezen om bepaalde dure betaalinstrumenten niet meer aan te bieden, terwijl daar nog wel vraag naar bestaat. Dit zou de innovatie in betaalmiddelen en de keuzemogelijkheden van consumenten kunnen begrenzen, en zodoende concurrentiebeperkend kunnen werken. Ook hierover zijn tijdens de behandeling van genoemd wetsvoorstel door verschillende leden van uw Kamer zorgen geuit. Zo vroeg het lid Van Dijck (PVV): «*Leidt een verbod op surcharging niet tot minder keuzemogelijkheden voor de klant, doordat ondernemers dure betaalmiddelen gaan mijden?*» en het lid De Vries (VVD) gaf aan: «*Hoe komt de initiatiefnemer tot de stelling dat de consument een ruimere keus in betaalmiddelen krijgt? Volgens de VVD is het risico reëel aanwezig dat de keuzemogelijkheden voor de betaalmethode op internet of in winkels juist minder worden, omdat ondernemers de duurdere betaalmethode niet meer zullen aanbieden.*» Ook de regering vindt concurrentie en innovatie op het gebied van betaalmiddelen belangrijk. Concurrentie in betaalmiddelen en -aanbieders kan leiden tot betere diensten voor gebruikers, doordat betalen sneller, veiliger of juist gebruiksvriendelijker

[14] Handelingen II 2015/16, nr 82, item 3. Behandeling van het voorstel van wet van het lid Van Vliet tot wijziging van Boek 6 en Boek 7 van het Burgerlijk Wetboek en van de Overgangswet nieuw Burgerlijk Wetboek in verband met het invoeren van een verbod op het vragen van een toeslag voor het gebruik van betaalmiddelen bij consumenten (Wet verbod toeslag gebruik betaalmiddelen bij consumenten) (34 291).

gebeurt. Bovendien kan meer concurrentie ook tot prijsverlagingen en innovatie leiden, ten gunste van winkelier en consument. De regering vindt de mogelijke consequentie dat als gevolg van het verbod bepaalde dure betaalinstrumenten niet meer worden aangeboden dan ook niet wenselijk.

Ten derde is in Nederland reeds sprake van een relatief goedkoop en efficiënt betaallandschap. Online betalingstransacties vinden veelal plaats met behulp van iDEAL[15], en niet, zoals in veel andere lidstaten, met behulp van een creditcard. iDEAL maakt online betalen bij een webwinkel mogelijk via een overschrijving en is daardoor een relatief goedkope manier van betalen. Het gebruik van iDEAL kost – ongeacht de transactiesom – een vast bedrag per transactie, waardoor consumenten en winkeliers weten waar ze aan toe zijn. Bij creditcards wordt een percentage van de waarde van de transactie in rekening gebracht, waardoor winkelier en consument minder grip hebben op de kosten. Daarbij geldt dat in Nederland relatief weinig met creditcard wordt betaald en het aandeel «dure» creditcards, dat buiten het in PSD II verplicht gestelde verbod op surcharging valt, zeer beperkt is.[16] Door dit relatief kleine aandeel creditcardbetalingen zal de keuze voor een gedeeltelijk dan wel algeheel verbod op surcharging in de praktijk voor zowel consument als winkelier waarschijnlijk op de korte termijn niet veel verschil maken. Echter, op lange termijn kan een algeheel verbod op surcharging leiden tot een vergroting van het aanbod van duurdere creditcards, omdat de kosten hiervan voor consumenten niet meer direct zichtbaar c.q. merkbaar zijn; consumenten hoeven immers geen aparte toeslag te betalen. Dit kan er verder toe leiden dat het aandeel creditcardtransacties zal toenemen, en mogelijkerwijs ook het aantal consumenten dat hierdoor schulden aangaat en door die schulden mogelijk in de problemen kan komen. Dit is een situatie die Nederland nu niet kent en die de regering ook niet wenselijk vindt. Met het gedeeltelijk verbod op surcharging wordt zo goed mogelijk aangesloten bij het bestaande (goedkope en efficiënte) betaallandschap en -cultuur in Nederland. Ook de schuldenproblematiek is tijdens de behandeling van genoemd wetsvoorstel besproken. Zo gaf het lid Nijboer (PvdA) aan: «*Als wij [creditcards] even duur maken voor de consument, namelijk gratis, dreigt dan niet dat consumenten veel meer creditcards gaan gebruiken? Leidt dat niet tot veel hogere maatschappelijke kosten?»* en «*Moet je het gebruik van een creditcard wel willen stimuleren, terwijl de pinkaart een heel mooi betaalmiddel is? Die is goedkoop, efficiënt en leidt niet tot onredelijke schulden. Is dit geen groot risico dat samenhangt met dit voorstel?»* Tot slot gaf ook het lid Ronnes (CDA) aan bezorgd te zijn over het risico dat creditcards meer gebruikt gaan worden als betaalmiddel, waardoor er meer op afbetaling wordt gekocht, met opbouw van schulden tot gevolg.

70) De leden van de PVV-fractie vragen welke EU-lidstaten voor een algeheel verbod op surcharging hebben gekozen.

Informatie over de wijze waarop iedere EU-lidstaat het verbod op surcharging wil vormgeven is niet vrij beschikbaar. Het is bij de regering bekend dat een aantal lidstaten op dit moment een algeheel verbod op surcharging heeft voorgesteld. Het gaat daarbij om Kroatië, Zweden,

---

[15] https://www.ideal.nl/actueel/mobiele-ideal-betaling-is-doorslaand-succes/; https://www.ideal.nl/actueel/meer-dan-een-miljard-betalingen-met-ideal/; https://www.ideal.nl/ontvangen/kerncijfers/ideal-betalingen/.

[16] Het marktaandeel creditcards uitgegeven door driepartijenschema's op de Nederlandse creditcard-markt is heel beperkt (grove inschatting ≈ 2%). Van een deel hiervan zijn de tarieven geplafonneerd, deze vallen daarmee onder het verplicht gestelde verbod op surcharging; voor een ander deel geldt dit niet.

Italië, Slowakije, Litouwen, Griekenland, het Verenigd Koninkrijk en Oostenrijk. Van de lidstaten Duitsland, Polen en Denemarken is bij de regering bekend dat zij een gedeeltelijk verbod hebben ingevoerd respectievelijk voornemens zijn om in te voeren.

74) De leden van de GroenLinks-fractie vragen in welke gevallen de consument per transactie extra moet betalen voor het gebruik van een creditcard en hoe hoog de regering verwacht dat de toeslagen zullen zijn.

Het marktaandeel creditcards uitgegeven door driepartijenschema's op de Nederlandse creditcardmarkt is heel beperkt (naar inschatting ongeveer 2%).[17] De kosten die winkeliers voor het accepteren van creditcards aan consumenten doorberekenen, verschillen per overeenkomst en deze overeenkomsten zijn niet openbaar. Volgens een internetbron ligt de algemene vergoeding voor het accepteren van American Express betalingen (dat creditcards uitgeeft gebaseerd op driepartijenschema's) rond de 3%.[18]

72) De leden van de CDA-fractie vragen aandacht voor de praktische uitwerking bijvoorbeeld hoe een winkelier vooraf weet of een bepaalde creditcard wel of niet onder het verbod op surcharging valt, of het altijd duidelijk is of een creditcard behoort tot een vierpartijenstelsel of een driepartijenstelsel, en handhaving van het verbod praktisch werkt. 73) De leden van de D66-fractie vragen of het voldoende duidelijk blijft voor de consument wanneer er wel en wanneer er geen sprake is van surcharging. 72) Tot slot vragen de leden van de CDA-fractie of het, gezien de vermeende praktische onduidelijkheden, niet beter zou zijn om alle surcharging te verbieden.

Van een aantal creditcards is vooraf duidelijk voor winkeliers dat zij niet onder het verbod op surcharging vallen. Het gaat hierbij om bekende creditcards van driepartijenstelsels, zoals Diners Club en bepaalde kaarten van American Express. Er kan onduidelijkheid zijn onder winkeliers bij dure creditcardtypen die niet onder het surcharging verbod vallen, maar die wel uitgegeven zijn door vierpartijenstelsels, en bij creditcardtypen uitgegeven door driepartijenschema's die samenwerken met licentie-houders, agenten en co-brandingpartners. Het gaat hierbij o.a. om commerciële B2B creditcards (kaarten die alleen gebruikt worden voor zakelijke transacties die direct in rekening worden gebracht bij een bedrijf). Goede informatievoorziening door banken, kaartmaatschappijen, werkgevers (bij commerciële creditcards) en winkeliers is daarom van belang. In de praktijk vallen de meeste Nederlandse (kaart)transacties die vallen onder de MIF- en SEPA-verordeningen in het huidige wetsvoorstel onder het surcharging verbod, namelijk een deel van de kosten van betalingen via iDEAL[19], het PIN systeem (debitcards) en het overgrote deel van de creditcardtransacties (waaronder alle creditcards uitgegeven door vierpartijenschema's. Het kan echter niet uitgesloten worden dat het voor consumenten die gebruik maken van creditcards in het begin onduidelijk is of hun betaalkaart onder het surcharging verbod valt of niet. Hierbij is informatievoorziening van belang. Toonbankinstellingen kunnen dit duidelijk vermelden in de winkel, bijvoorbeeld bij de kassa, en op hun website (toonbankinstellingen en webwinkels).

---

[17] Alleen voor de «pure» driepartijenschema's zouden consumenten in geval van een gedeeltelijk verbod nog extra voor de betaling worden belast. Het aandeel van de «pure» driepartijen-schema's en dat van de driepartijenschema's «plus» binnen die 2%, is niet bekend.

[18] https://nl.mobiletransaction.org/accepteert-american-express/.

[19] Voor iDEAL-betalingen geldt dat winkeliers niet apart kosten in rekening kunnen brengen voor de onderliggende overschrijving, maar wel voor de kosten van de iDEAL-dienstverlening.

Een algeheel verbod zou als voordeel hebben dat het consumenten en winkeliers zekerheid biedt dat voor geen enkele kaartbetaling en overschrijving een toeslag in rekening mag worden gebracht. Naar verwachting speelt dit voordeel echter vooral op de korte termijn, bij inwerkingtreding van PSD II, en weegt het niet op tegen de nadelen van een algeheel verbod (zoals beschreven in het antwoord op de vragen 68, 69, 70, 73, 74 en 75).

68) 71) De leden van de VVD- en de PVV-fracties vragen hoe wordt voorkomen dat een gedeeltelijk of geheel verbod op het vragen van een vergoeding (surcharging) gelegenheid biedt om de transactiekosten door te bereken in consumenten prijzen?

Na inwerkingtreding van het gedeeltelijk verbod op surcharging mogen winkeliers de vergoedingen voor het gebruik van betaalinstrumenten niet meer doorberekenen aan de consument. Het ligt in de lijn der verwachting dat winkeliers deze kosten doorberekenen in de prijzen van hun producten of diensten. Het verbod is met name ingegeven met het oog op de duidelijke informatie over de volledige prijs van een dienst of product en bevordert ook het gebruik van efficiënte betaalinstrumenten.

De implicaties voor de Nederlandse markt van het (gedeeltelijk) verbod op surcharging zijn naar verwachting afwezig tot zeer beperkt. Dit komt doordat Nederlandse consumenten weinig gebruik maken van creditcards, doordat weinig winkeliers hun klanten kosten in rekening brengen voor creditcard-gebruik en doordat veel online transacties worden voldaan via iDEAL; een relatief goedkope manier van betalen waarvoor geldt dat een deel van de kosten van een overschrijving ook onder het verbod op surcharging valt. In 2016 zijn er in Nederland in totaal 53 miljoen creditcardbetalingen gedaan, waarvan 23 miljoen online betalingen en 30 miljoen aan de toonbank. Het aandeel creditcardbetalingen op het totale aantal (online) betalingen in 2016 is beperkt, namelijk 13% (Jaarverslag Currence 2016); de acceptatiegraad van creditcardbetalingen onder webwinkeliers is laag, namelijk 21% (Boom Marktverkenningen i.o.v. Currence, 2017). Een minderheid van de creditcard accepterende webwinkeliers (25%) maakt (soms) gebruik van de mogelijkheid om creditcardbetalingen te surchargen. Volgens DNB gaat er van e-commerce als geheel juist een dempende werking uit op consumentenprijzen vanwege toenemende (prijs)concurrentie en lagere kosten van webwinkels ten opzichte van toonbankinstellingen.[20] Het aandeel betalingen met creditcard op het totale aantal toonbankbetalingen is ook erg laag, in 2016 namelijk minder dan 0,5% (cijfers DNB en Betaalvereniging Nederland).[21] Het is daarom zeer onwaarschijnlijk dat er van het verbod een noemenswaardige invloed zal uitgaan op de consumentenprijzen aan de toonbank.

71) De leden van de PVV-fractie willen weten of het klopt dat winkeliers als gevolg van PSD II hogere transactiekosten moeten betalen aan de financiële nieuwkomers.

Detailhandel Nederland en de Gezamenlijke Toonbankinstellingen hebben aangegeven te vrezen dat PSD II voor kaartacceptanten (winkeliers) eenzijdig nadelig uitpakt door het verbod op surcharging. Zij stellen dat daardoor naar verwachting andere kosten zullen stijgen en deze als gevolg van het verbod niet meer aan de consument mogen worden doorberekend. Zij stellen verder dat onder PSD II nieuwe betaalinitiatieven

[20] https://www.dnb.nl/nieuws/nieuwsoverzicht-en-archief/dnbulletin-2017/dnb352876.jsp.
[21] https://statistiek.dnb.nl/downloads/index.aspx#/details/retailbetalingsverkeer-kwartaal/dataset/9aa3c704–8e00–40b2-b075-b17e2a63de30.

zullen ontstaan die duurder zijn voor een winkelier. Het gevolg hiervan zou volgens hen kunnen zijn dat deze hogere kosten worden doorberekend in consumentenprijzen.

Het is niet op voorhand vast te stellen of financiële nieuwkomers winkeliers eventuele hogere kosten in rekening brengen dan de huidige betaaldienst-aanbieders, dan wel een deel van de kosten in rekening willen brengen bij banken. De hoogte van de kosten voor het gebruik van betaalmiddelen staat nog niet vast, aanbieders en acceptanten spreken deze in onderhandeling af. Bovendien zal er naar verwachting als gevolg van PSD II meer concurrentie optreden wat een prijsdrukkend effect kan hebben. Het is vervolgens aan de winkeliers om al dan niet op individuele basis te beslissen of zij deze betaalmogelijkheden willen accepteren of niet. Hierbij maken zij een afweging tussen de hoogte van de kosten van de betaalmethode en de kwaliteit van de geleverde dienst in relatie tot de (extra) opbrengsten die het aanbieden van deze betaalmethode oplevert. Vanuit de vrijheid om betaalmogelijkheden al dan niet te accepteren wordt ook een disciplinerende werking verwacht om kosten te beperken. Marktwerking zal uiteindelijk de hoogte van de kosten bepalen alsmede welke financiële nieuwkomers toe zullen treden tot de markt.

76) De leden van de SP-fractie vragen of het de bedoeling van de regering is om de regellast voor ondernemers in Nederland te vergroten naar zij de indruk hebben dat het gedeeltelijk verbod alleen van toepassing is op in de EU opererende bedrijven.

Blijkens het wetsvoorstel zijn de regels van PSD II, waaronder het gedeeltelijk verbod op surcharging, van toepassing op alle betaaldiensten die in Nederland worden aangeboden. De regeldruk voor ondernemers in Nederland en ondernemers daarbuiten, die in Nederland diensten aanbieden, is daarmee gelijk.

8. Betalingstransacties waarbij het transactiebedrag niet vooraf bekend is

77) 78) en 79)
De leden van de fracties van de VVD en CDA vragen naar de wijze waarop de implementatie van deze bepaling inzake «Betalingstransacties waarbij het transactiebedrag niet vooraf bekend is» plaats zal vinden, of dat bijvoorbeeld tanken bij een onbemand tankstation alleen nog kan, indien vooraf toestemming wordt gegeven over het maximumbedrag dat van de betaalrekening mag worden afgeschreven, of hiermee de huidige gang van zaken dat er een in theorie onbeperkt bedrag kan worden afgeschreven verdwijnt, en zo ja of de regering erkent dat dit ook een nadeel voor de consument kan betekenen, omdat zoals in het geval van het onbemande tankstation men niet altijd vooraf exact weet hoe groot het benodigde bedrag is dat afgeschreven moet worden, en of er met consumentenorganisaties gesproken is over deze maatregelen en zo ja, wat hun opvattingen waren over deze maatregel. Voorts vraagt de fractie van de SP of de regering met voorbeelden te komen waarbij consumenten niet bij bestelling op de hoogte zijn van de extra kosten voor het gebruik van deze faciliteiten en in hoeverre de klachten heeft ontvangen dat hiervan sprake is, met name in Nederland. Tot slot vraagt de VVD-fractie of de huidige verkooppunten, zoals hotels en benzinestations, al geschikt gemaakt zijn om het geblokkeerde bedrag weer te geven dan wel welke tijd en welke kosten gemoeid zijn met de omschakeling.

In bepaalde gevallen kan een klant met een betaalkaart een betaalopdracht geven zonder dat op dat moment al exact duidelijk is om welk bedrag het gaat. Een voorbeeld hiervan is een betalingstransactie bij een

automatisch (onbemand) tankstation, waarbij het verschuldigde bedrag achteraf wordt bepaald en afgeschreven, alsmede betalingtransacties bij dienstverleners, zoals hotels of autoverhuurders, waarbij een bedrag wordt gereserveerd voor potentiële lasten (zoals het gebruik van de minibar in een hotel of de schade aan een huurauto). PSD II regelt de kaartbetalingen in zulke situaties. De bank van de betaler blokkeert een bedrag op de rekening van de betaler, als een soort borg. Dit mag alleen als de betaler toestemming heeft gegeven voor het exacte te blokkeren bedrag. Als het product of de dienst definitief geleverd is, is het exact verschuldigde bedrag bekend bij de leverancier, de betaler en de banken. Dit bedrag wordt afgerekend en het geblokkeerde bedrag vrijgegeven. Voor zover bekend hebben de Nederlandse toezichthouders hierover de afgelopen jaren geen klachten ontvangen.

Om aan genoemde bepaling in PSD II te voldoen is er door de branches die deze wijze van betalen aanbieden voor gekozen om consumenten hierover te informeren via een sticker in plaats van aanpassing van software. Hierover heeft overleg plaatsgevonden tussen de betreffende branches en de Consumentenbond. Op een duidelijk zichtbare sticker wordt de consument geïnformeerd over het feit dat pre-autorisatie plaatsvindt en over het maximale bedrag van de reservering. Dit bedrag van maximaal EUR 150 is in de branche afgesproken. Het voordeel hiervan voor de consument is dat hij op die manier weet welk bedrag op zijn kaart is geblokkeerd. Hij kan hiermee rekening houden in zijn betaalgedrag. De kosten van het informeren via een sticker beperken zich tot het maken van enkele duizenden stickers en distributie daarvan en zijn eenmalig. Momenteel is de branche in overleg met de Betaalvereniging en de Stichting Bevorderen Efficiënt Betalen over de uitvoering hiervan.

9. Sterke cliëntauthenticatie

80) De leden van de VVD-fractie vragen of de introductie van een sterke cliëntauthenticatie enige verandering teweegbrengt in het Nederlandse betalingsverkeer. De authenticatie bij banken voldoet immers al aan de eis van twee factoren.

Partijen die in Nederland actief zijn in het betalingsverkeer beschikken over goede en veilige methodes voor authenticatie. PSD II zal op dit gebied daarom geen grote impact hebben voor de partijen die al actief zijn in Nederland. Wel biedt PSD II een aantal extra waarborgen voor de veiligheid. Voorbeelden hiervan zijn gegeven bij de beantwoording van vraag 16. Bij grensoverschrijdende betalingen vindt mogelijk wel verandering plaats als gevolg van PSD II. Bij online aankopen bij webwinkels in andere lidstaten dient dan, afgezien van enkele uitzonderingen, sterke cliëntauthenticatie te worden toegepast. Dat is nu nog niet altijd het geval. Dit komt ten goede aan het algemene veiligheidsniveau van het betalingsverkeer in Europa.

81) De leden van de D66-fractie vragen of bij elke betaling een sterke cliëntauthenticatie moet worden gegeven. Is er een tijdsperiode waarna een gebruiker weer opnieuw deze sterke cliëntauthenticatie moet afgeven? In het geval dat een rekening door meerdere personen wordt gebruikt, zowel bij een zakelijke als privé account, is dan toestemming en authenticatie van één gebruiker voldoende voor een dienstverlener om toegang te krijgen tot de persoons- en betaalgegevens van alle accounthouders van die rekening?

De technische standaarden over sterke cliëntauthenticatie, waarin onder meer de eisen rondom sterke cliëntauthenticatie zijn opgenomen, bepalen dat bij elke betalingstransactie sterke cliëntauthenticatie moet worden toegepast, maar dat er een aantal uitzonderingen is.

Voor contactloze betalingen geldt een uitzondering als het individuele bedrag van de betaling niet meer dan 50 euro is en het cumulatieve bedrag van eerdere betalingen sinds de laatste keer dat er sterke cliëntauthenticatie plaatsvond niet meer is dan 150 euro, of het aantal keren dat er een contactloze betaling zonder sterke cliëntauthenticatie plaatsvond niet meer dan vijf is.

Voor kleine betalingen in het algemeen geldt er ook een uitzondering als het individuele bedrag van de betaling niet meer is dan 30 euro en het cumulatieve bedrag van eerdere betalingen sinds de laatste keer dat er sterke cliëntauthenticatie plaatsvond niet meer is dan 100 euro, of het aantal keren dat er een betaling zonder sterke cliëntauthenticatie plaatsvond niet meer dan vijf is.

Voor onbeheerde terminals voor het betalen van parkeergeld of tolgeld geldt eveneens een uitzondering. Sterke cliëntauthenticatie is daarnaast niet noodzakelijk als de klant een transactie doet naar iemand op een eigen lijst met vertrouwde partijen. Voor terugkerende betalingen, zoals een automatische incasso, hoeft slechts bij de eerste betaling sterke cliëntauthenticatie te worden toegepast. Ten slotte is sterke cliëntauthenticatie niet noodzakelijk als er een transactie wordt gedaan naar een rekening van dezelfde (rechts)persoon bij dezelfde rekeninghoudende betaaldienstverlener.

Als er geen sprake is van een uitzondering dan dient sterke cliëntauthenticatie te worden toegepast. Op deze manier geeft een betaaldienstgebruiker toestemming aan de betaalinitiatiedienstverlener voor de toegang tot zijn betaalrekening. Deze toegang heeft de betaalinitiatiedienstverlener nodig om de betaling te initiëren. Deze toestemming is eenmalig en geldt alleen voor deze specifieke transactie. Bij een volgende transactie (hiervan is ook sprake als het bedrag en/of de begunstigde wijzigt) dient opnieuw toestemming te worden verleend, waarbij sterke cliëntauthenticatie plaatsvindt.

Ook de rekeninginformatiedienstverlener heeft voor zijn dienstverlening toegang tot de betaalrekening nodig. Ook in dat geval dient hiervoor eerst sterke cliëntauthenticatie plaats te vinden. De toestemming voor het verlenen van deze betaaldienst en daarmee voor toegang tot de betaalrekening kan worden gegeven voor maximaal 90 dagen. Hierna dient opnieuw sterke cliëntauthenticatie plaats te vinden. Gedurende deze 90 dagen kan de rekeninginformatiedienstverlener toegang krijgen tot de betaalrekening *zonder* afgifte van sterke cliëntauthenticatie als de betaaldienstgebruiker hier actief om vraagt of maximaal vier keer per 24 uur, tenzij de betaaldienstgebruiker toestemming heeft gegeven voor een hogere frequentie. De rekeninginformatiedienstverlener heeft toestemming nodig voor elke afzonderlijke rekening waartoe hij toegang krijgt. Als een betaalrekening meerdere rekeninghouders heeft, moeten alle rekeninghouders toestemming geven.

Zie voor de toegang tot de gegevens van de betaalrekening ook de beantwoording van vraag 82.

82) Ook hier vragen de leden van de SP-fractie de regering welke extra voorzieningen verplicht worden gesteld ten opzichte van bestaande wet- en regelgeving. Is het mogelijk, zo vragen zij, dat mensen onbedoeld of

onbewust toestemming verlenen voor het uitwisselen van gegevens? Is de regering bereid te regelen dat bij het uitwisselen van gegevens de burger altijd nog een keer toestemming moet geven als de gegevens van de bank naar een derde partij gaan?

Een derde partij kan onder strikte voorwaarden toegang krijgen tot de betaalrekening van de rekeninghouder bij de bank. Voor het verkrijgen van toegang tot de betaalrekening is toestemming nodig van de betaaldienstgebruiker voor het verlenen van de betreffende betaaldienst. Deze verleent hij door zich te identificeren met behulp van sterke cliëntauthenticatie. Dit kan niet ongemerkt, onbedoeld of onbewust plaatsvinden. Sterke cliëntauthenticatie vereist namelijk dat de identiteit van de betaaldienstgebruiker wordt gecontroleerd. Deze controle vindt plaats door een combinatie van iets dat de betaaldienstgebruiker *weet* (wachtwoord, pincode), iets dat hij *bezit* (bankpas, random reader, geregistreerde mobiele telefoon), of een unieke persoonlijke *eigenschap* van de betaaldienstgebruiker (vingerafdruk, stem, irisscan). Als de identiteit van de betaaldienstgebruiker juist is vastgesteld, wordt een specifieke code (tancode, verificatiecode, of response code) gegenereerd. Met het gebruik van die code wordt toegang gegeven tot de betaalrekening en kan de betaling worden geïnitieerd. De regels met betrekking tot sterke cliëntauthenticatie zijn uitgewerkt in technische reguleringsnormen op grond van PSD II.

Naast toestemming voor het verlenen van de betaaldienst en daarmee voor toegang tot de betaalrekening, bepaalt PSD II dat een betaaldienstverlener ook uitdrukkelijke toestemming van de rekeninghouder nodig heeft voor het verwerken van de persoonsgegevens van de rekeninghouder die nodig zijn voor het verlenen van de gevraagde betaaldienst. Dit vereiste van uitdrukkelijke toestemming is een aanvullende eis, opgenomen in artikel 94(2) van PSD II, die geldt bovenop de in de AVG gestelde eisen aan verwerking van persoonsgegevens (zie ook beantwoording van vraag 94 tot en met 97). Hiervoor dient de betaaldienstverlener de betaaldienstgebruiker afzonderlijk om toestemming te vragen. In geval van een al bestaande overeenkomst is dit nieuwe vereiste ook van toepassing en dan dient hierom naar aanleiding van PSD II te worden gevraagd. De uitdrukkelijke toestemming zou in een digitale omgeving bijvoorbeeld kunnen worden gevraagd in de vorm van een apart venster (bijvoorbeeld een pop-up of een aan te vinken checkbox in een dialoog), waarin de betaaldienstgebruiker kan aangeven toestemming te verlenen. Wordt deze toestemming niet verleend, dan kunnen hier geen negatieve consequenties aan verbonden zijn, anders dan dat de betaaldienst niet kan worden verleend. De precieze invulling van het PSD II vereiste in de praktijk zal door DNB en de Autoriteit Persoonsgegevens gezamenlijk worden vormgegeven. Daarbij kan waar mogelijk worden aangesloten bij de eisen die de AVG stelt ten aanzien van het verlenen van toestemming.

PSD II bepaalt dat betaalinitiatie- en rekeninginformatiedienstverleners alleen gegevens mogen verwerken die nodig zijn voor het verlenen van de gevraagde betaalinitiatie- of rekeninginformatiedienst. Verwerking van gegevens voor andere doeleinden wordt niet gereguleerd door PSD II, maar door de algemene gegevensbeschermingsregels, in het bijzonder de Algemene Verordening Gegevensbescherming (AVG). Op grond van deze regels is voor een dergelijke verwerking aanvullende (extra) toestemming nodig, bovenop de toestemming die de betaaldienstgebruiker heeft gegeven om de gegevens te gebruiken voor het verlenen van betaaldiensten. Ook andere waarborgen uit de AVG zijn op deze verwerking van toepassing.

10. Bescherming van persoonsgegevens

Toestemmingsverlening

83) De leden van de VVD-fractie vragen of de «uitdrukkelijke toestemming» nader kan worden omschreven. Hoe wordt voorkomen dat mensen uitdrukkelijk toestemming verlenen zonder zich daadwerkelijk van de inhoud vergewist te hebben van hetgeen waarvoor zij toestemming verlenen? Kan de regering een concreet voorbeeld geven hoe men toestemming verleent via bijvoorbeeld een app of een computer?

Om aan de eisen van PSD II en de AVG te voldoen, zal de betaaldienstverlener de betaaldienstgebruiker vooraf moeten informeren over het doel waarvoor de gegevens worden verwerkt en welke gegevens voor die verwerking nodig zijn. Het is vervolgens aan de betaaldienstgebruiker om al dan niet toestemming te geven voor het verlenen van de betaaldienst en daarmee voor toegang tot de betaalrekening en tot zijn gegevens. Voor de wijze waarop toestemming wordt gegeven verwijs ik naar de beantwoording van vraag 82.

84) De leden van de CDA-fractie vragen naar de «uitdrukkelijke toestemming» die een betaaldienstgebruiker moet geven voor het delen van zijn betaalgegevens. Deze leden vragen of een eenmalige goedkeuring door de gebruiker het mogelijk maakt dat zijn gegevens tot in lengte van dagen worden gedeeld. Deze leden vragen verder hoe in de praktijk aan de gebruiker duidelijk wordt gemaakt wat het gevolg is van zijn keuze om toestemming te geven zijn gegevens te delen. Hierop doorvragend, willen deze leden weten of een eenmaal gegeven toestemming voor altijd geldig is, of dat de toestemming van tijd tot tijd vernieuwd en dus herbevestigd moet worden. Verder vragen deze leden hoe een gebruiker zijn toestemming weer kan intrekken. Wat gebeurt er met de gegevens die eerder zijn verstrekt nadat een gebruiker zijn toestemming voor het gebruik van de gegevens heeft ingetrokken?

Toegang tot de betaalrekening wordt steeds door de betreffende betaaldienstgebruiker per specifieke transactie of reeks van transacties gegeven. Dit gaat gepaard met gebruik van sterke cliëntauthenticatie. Zie ook de beantwoording van vraag 81 en 82. De uitdrukkelijke toestemming aan rekeninginformatiedienstverleners voor het verlenen van de rekeninginformatiedienst, en daarmee voor toegang tot de betaalrekening, geldt niet voor onbepaalde tijd. Deze toestemming kan worden gegeven voor maximaal 90 dagen. Hierna moet opnieuw toestemming worden gegeven (zie eveneens de beantwoording van vraag 81).

Naast toestemming voor het verlenen van de betaaldienst en daarmee voor toegang tot de betaalrekening, bepaalt artikel 94(2) PSD II dat een betaaldienstverlener ook uitdrukkelijke toestemming van de rekeninghouder nodig heeft voor het verwerken van de persoonsgegevens van de rekeninghouder die nodig zijn voor het verlenen van de gevraagde betaaldienst. Op de verwerking van persoonsgegevens zijn ook de eisen van de AVG van toepassing. Intrekken van toestemming voor het verwerken van persoonsgegevens kan in het geval van betaaldienstverlening in ieder geval door beëindiging door de betaaldienstgebruiker van de overeenkomst met de betaaldienstverlener. Bij de beantwoording van de vragen 94 tot en met 97 ga ik hier verder op in.

85) De leden van de CDA-fractie vragen naar een nadere uitwerking van het begrip «uitdrukkelijk toestemming geven» door de consument. Zij vragen de regering een aantal praktische voorbeelden te geven hoe uitdrukkelijk toestemming geven voor de gebruiker uiteindelijk zal werken.

Deze leden vragen hierbij voorts naar een vergelijking met het huidige gebruik dat voortkomt uit de zogenaamde «cookiewet», waarbij gebruikers met één muisklik toestemming geven voor het plaatsen van tracking cookies. Gaat het delen van rekeninggegevens straks op een vergelijkbare manier? Indien dit het geval is, deelt de regering de mening van de leden van de CDA-fractie dat dit een veel te licht regime zou zijn?

De toestemming voor het verwerken van persoonsgegevens voor het verlenen van betaaldiensten moet uitdrukkelijk worden gegeven (artikel 94(2) PSD II). De manier waarop uitdrukkelijke toestemming wordt gegeven voor het verlenen van de betaaldienst en daarmee voor toegang tot de betaalrekening alsmede de wijze waarop uitdrukkelijke toestemming wordt gegeven voor het verwerken van gegevens voor het verlenen van de gevraagde betaaldienst, is beschreven in de beantwoording van vraag 82. Deze wijzen van verlening van toestemming bieden de nodige waarborgen om zoveel mogelijk te voorkomen dat toestemming lichtvaardig wordt gegeven.

Of de door een betaaldienstverlener voorziene procedures en maatregelen betreffende de toestemming voor het verlenen van de betaaldienst en de toegang tot de betaalrekening voldoen aan de daarvoor geldende vereisten, wordt door DNB getoetst bij de vergunningaanvraag. Als een vergunning is verleend, komt de manier waarop door een betaaldienstverlener vorm is gegeven aan de uitdrukkelijke toestemming voor het verlenen van de betaaldienst en toegang tot de betaalrekening onder doorlopend toezicht van DNB te staan en komt de manier waarop vorm is gegeven aan de uitdrukkelijke toestemming voor het verwerken van persoonsgegevens voor het verlenen van de betaaldienst onder doorlopend toezicht van de AP te staan. Laatstgenoemde bevoegdheid van de AP om toezicht te houden staat naast de bevoegdheid van de AP om toezicht te houden op de naleving van de AVG door betaaldienstverleners. Bij overtreding van de eisen van PSD II of de AVG kan DNB dan wel de AP handhavend optreden.

Het stellen van zwaardere eisen aan de wijze waarop toestemming wordt verleend is niet toegestaan, omdat PSD II maximumharmonisatie bevat. Bovendien is het stellen van zwaardere eisen niet wenselijk, omdat dit zorgt voor een ongelijk speelveld tussen de lidstaten en daarmee indruist tegen het achterliggende doel van PSD II, namelijk het bevorderen van een gelijk speelveld voor betaaldienstverleners op de interne markt. Daarnaast is het stellen van zwaardere eisen op voorhand ook niet nodig. Het ligt meer voor de hand om de nieuwe regels van PSD II en het toezicht op de naleving daarvan eerst een kans te geven en de ontwikkelingen te blijven monitoren.

86) De leden van de fractie van Groenlinks vragen hoe «uitdrukkelijke toestemming» er in de praktijk uit gaat zien. Hoe gaat de regering ervoor zorgen dat het voor alle burgers duidelijk is waar zij ja of nee tegen zeggen? Voorts vragen deze leden in hoeverre van burgers verwacht kan worden dat zij zich voldoende realiseren waarvoor zij precies toestemming geven. Hoe gaat de regering bijdragen aan de bewustwording van consumenten?

Op de vraag hoe beide vormen van «uitdrukkelijke toestemming» er in de praktijk uit gaan zien, wordt verwezen naar de beantwoording van vraag 82. Aan de bewustwording van consumenten waar het gaat om het verlenen van toestemming wordt op verschillende manieren bijgedragen. Allereerst zal de Europese Commissie komen met een pamflet over de rechten van consumenten. DNB zal op verzoek van en namens het Maatschappelijk Overleg Betalingsverkeer (MOB) voorlichting aan het

publiek verzorgen via haar website www.dnb.nl/psd2 en zal in het najaar van 2018 starten met een voorlichtingscampagne voor consumenten en bedrijven om de bewustwording over de veranderingen in het betalingsverkeer als gevolg van PSD II te vergroten. Het MOB heeft inmiddels aangegeven graag te zien als banken consumenten in mibiel bankieren apps en bij internetbankieren een overzicht bieden van de dienstverleners waaraan toestemming is verleend voor rekeninginformatiediensten.

87) Verder constateren de leden van de fractie van Groenlinks dat zodra de betaaldienstgebruiker zijn toestemming intrekt, een rekeninginformatiedienstverlener niet langer toegang mag hebben tot de informatie van diens betaalrekening. Hoe gaat dit worden gecontroleerd? Hoe kan een betaaldienstgebruiker zeker weten dat alle informatie daadwerkelijk onbereikbaar is geworden en niet ergens blijft opgeslagen?

Op grond van de AVG geldt dat gegevens niet langer bewaard mogen worden dan nodig (artikel 5 (1) (e) AVG) en moet de verwerkingsverantwoordelijke de gebruiker informeren over de duur van opslag van gegevens (artikel 13 (2) (a) AVG). Na het verstrijken van die termijn moeten de gegevens worden gewist. De betrokkene kan hier zo nodig expliciet om vragen (artikel 17 AVG). Voor wat betreft de controle hierop wordt verwezen naar de beantwoording van vraag 85. Indien DNB tijdens het uitoefenen van doorlopend toezicht of bij de vergunningverlening signalen ontvangt dat de AVG wordt overtreden, kan DNB deze doorgeven aan de AP. Er is dus voortdurende controle of de verwerking van gegevens op een rechtmatige manier plaatsvindt.

88) De leden van de SP-fractie vragen de regering waarom er geen waarborgen voor kwetsbare groepen zijn opgenomen in PSD II. Ook vragen deze leden waarom de wijze waarop een burger toestemming geeft niet wordt beschreven. De leden van de SP-fractie vragen de regering waarom er geen mechanisme bestaat om de toestemming in te trekken.

Voor de wijze waarop toestemming wordt gegeven verwijs ik naar de beantwoording van vraag 82. Zowel toestemming voor het verlenen van een betaaldienst – en daarmee voor toegang tot de betaalrekening – als toestemming voor toegang tot persoonsgegevens die nodig zijn voor het verlenen van betaaldiensten kunnen in elk geval worden ingetrokken als de betaaldienstgebruiker de overeenkomst die hij heeft gesloten met de betaaldienstverlener beëindigt (opzegt). Het intrekken van toestemming vindt plaats tussen de betaaldienstverlener en de betaaldienstgebruiker. De betaaldienstverlener moet de betaaldienstgebruiker voorafgaand aan het sluiten van de overeenkomst duidelijk informeren over de manier waarop de toestemming kan worden ingetrokken.

Het MOB heeft aangegeven graag te zien als banken consumenten in mobiel bankieren apps en bij internetbankieren een overzicht bieden van de dienstverleners waaraan toestemming is verleend voor rekeninginformatiediensten.

89) De voorgenoemde leden van de SP-fractie vragen de regering waarom niet expliciet geregeld is dat de consument eigenaar is van zijn eigen data. De leden van de SP-fractie vragen de regering wat zij gaat doen, nu blijkt dat de toezichthouder niet kan garanderen dat hij het werk kan verrichten dat op hem afkomt. Is de regering bereid om meer waarborgen in te bouwen teneinde de toestemming om gegevens te verstrekken per keer en niet voor een bepaalde periode te laten lopen? De leden van de SP-fractie vragen de regering voorts of zij bereid is expliciet te regelen

waarvoor precies toestemming wordt gegeven. Is de regering bereid tot deze aanscherpingen?

Het Ministerie van Financiën is ter voorbereiding op de invoering van PSD II met de vier toezichthouders (DNB, AFM, ACM en AP) in overleg om hun samenwerking te bevorderen en het toezicht op de naleving van PSD II op elkaar af te stemmen. Dankzij het doorlopende prudentieel toezicht dat DNB uitoefent, het doorlopend toezicht van de AP op naleving van het uitdrukkelijke toestemmingsvereiste en de mogelijkheid om signalen door te geven aan de AP, worden de mogelijkheden om toezicht te houden zo optimaal mogelijk benut.

PSD II bevat maximumharmonisatie waardoor een gelijk speelveld wordt gecreëerd voor betaaldienstverleners en op het gebied van consumentenbescherming. Extra eisen of aanscherpingen zijn om die reden niet mogelijk en ook niet wenselijk. Deze zouden indruisen tegen het achterliggende doel van PSD II, namelijk het bevorderen van de interne markt en creëren van een gelijk speelveld.

90) De leden van de SP-fractie constateren dat toezichthouders als de AFM en DNB, maar ook brancheorganisaties allen waarschuwen of vrezen voor een toename van cybercriminaliteit. Deze leden hebben goed geluisterd naar TROS Radar, waar werd gemeld: «Ondanks dat de PSD II op 13 januari 2018 in werking treedt, zijn een aantal essentiële zaken nog niet geregeld. Het Ministerie van Financiën liet Radar weten: «De regels met betrekking tot het verlenen van toegang tot de betaalrekening en de toestemming hiervoor van de consument zijn nog niet vastgesteld. Het verlenen van toegang tot de betaalrekening gaat via uitdrukkelijke toestemming van de consument en de betaalinitiatie- of rekeninginformatiedienstverlener, niet tussen de consument en de bank.»
De leden van de SP-fractie vragen de regering of zij van mening is dat veiligheid van burgers altijd voorop moet staan. Deze leden vragen de regering bij positieve beantwoording of zij bereid is eerst het Ministerie van Financiën en toezichthouders de tijd te geven zich klaar te maken voor PSD II alvorens deze inwerking treedt.

De regering onderschrijft dat veiligheid van burgers voorop moet staan. PSD II voorziet in voldoende waarborgen voor een veilig en betrouwbaar betalingsverkeer. In Nederland is de implementatie van PSD II vertraagd. Verder uitstel van de inwerkingtreding van PSD II is onwenselijk. Een te late implementatie zorgt voor een ongelijk speelveld ten opzichte van andere lidstaten die wel tijdig implementeren. De nieuwe betaaldiensten kunnen bovendien nu ongereguleerd worden verleend. Indien de implementatiewet in werking treedt, moeten verleners van deze betaaldiensten beschikken over een daarvoor afgegeven vergunning en komen zij onder doorlopend toezicht te staan. Snelle invoering van de implementatiewet is in het belang van zowel betaaldienstverleners als betaaldienstgebruikers. Voor de volledigheid merk ik nog op dat de Europese Commissie een inbreukprocedure kan starten die eventueel kan resulteren in een boete vanwege niet tijdige implementatie. Inmiddels is reeds een ingebrekestelling van de Europese Commissie ontvangen in verband met de niet tijdige implementatie van PSD II.

91) De leden van de SP-fractie zouden graag zien dat Nederland regelt dat mensen per keer toestemming verlenen voor het uitwisselen van betaalgegevens en dat zij daarbij ook grenzen kunnen aangeven. Zodat zij bijvoorbeeld hun pingedrag of waar zij precies aankopen doen, kunnen afschermen. Deze informatie is namelijk goud waard maar kan ook leiden tot problemen. Het schendt de privacy als een hypotheekverstrekker inzicht heeft in hoeveel geld iemand uitgeeft aan een hobby bijvoorbeeld.

Het is niet nodig dat een financiële instelling weet dat iemand zwanger is omdat hij of zij boodschappen doet bij een babywinkel op internet. Zo zijn er nog vele duizenden voorbeelden te geven van gegevens die niet behoren te worden blootgesteld door deze richtlijn. Erkent de regering dat?

Bescherming tegen onrechtmatige gegevensverwerking is reeds op diverse plekken geregeld. Zowel in PSD II als in de AVG zijn strikte doelbeperkingen vastgelegd. Dit betekent dat de gegevens niet mogen worden verwerkt voor andere doeleinden dan waarvoor de toestemming is gegeven. Het regelgevend kader van PSD II en de AVG biedt volgens de regering voldoende waarborgen om de situaties die de SP noemt, te voorkomen. Zie hiervoor de beantwoording van de vragen 94 tot en met 97.

92) De leden van de SP-fractie willen ook graag dat gegarandeerd wordt dat gegevens terug te halen zijn en dat ze verwijderd worden uit databases waarin zij terecht zijn gekomen. Kan de regering uiteenzetten hoe deze garantie gestand gedaan wordt?

Zoals eerder aangegeven, mogen op grond van de AVG gegevens niet langer bewaard worden dan nodig voor het doel waarvoor ze worden verwerkt (artikel 5 (1) (e) AVG). Op grond van de AVG moet de verwerker van gegevens de gebruiker informeren over de duur van opslag van gegevens (artikel 13 (2) (a) AVG). Na het verstrijken van deze termijn moeten de gegevens worden gewist. De betrokkene kan hier expliciet om vragen (artikel 17 AVG). De AP houdt toezicht op de naleving van deze bepalingen en kan bij overtreding hoge boetes opleggen.

93) Externe partijen van klein formaat, maar ook bedrijven zoals Google krijgen binnenkort dus – na «toestemming» van burgers – toegang tot hun financiële transacties. De leden van de PvdD-fractie vragen of de regering de zorg deelt dat burgers veelal niet écht akkoord gaan met algemene voorwaarden. Denk daarbij aan het akkoord gaan met de algemene voorwaarden zonder zich te laten informeren over de consequenties daarvan (met andere woorden: de algemene voorwaarden niet lezen). Is de regering bereid banken te verplichten burgers elk kwartaal expliciet op dit punt om toestemming te vragen? Zo nee, waarom niet? Op welke andere wijzen gaat de regering samen met banken zorgen dat burgers geïnformeerd worden over de gevolgen van het akkoord gaan met het delen van informatie met externe partijen en wat is de rol van deze externe partijen daarin? Hoe gaat de regering voorkomen dat situaties ontstaan waarbij een burger toestemming geeft financiële transacties te delen met externe bedrijven, terwijl daardoor ook transacties met een derde zichtbaar kunnen worden die geen toestemming heeft gegeven?[22]

Voor wat betreft het geven van toestemming voor het verlenen van een betaaldienst wordt in de eerste plaats verwezen naar de beantwoording van vraag 81 en 82. Voordat een betaaldienstverlener toegang tot een betaalrekening kan krijgen, moet de betaaldienstgebruiker zich eerst identificeren door gebruik te maken van sterke cliëntauthenticatie. Vervolgens kan de betaaldienstgebruiker opdracht geven tot het verlenen van de betaaldienst. Dit vindt plaats door middel van dynamic linking, waarmee inloggegevens worden gegenereerd. De betreffende betaaldienstverlener gebruikt deze inloggegevens om de betaling te initiëren. De wijze waarop derhalve toestemming wordt gegeven voor het verlenen van

[22] Voorbeeld: X doet een financiële transactie aan Y. Y geeft toestemming om zijn/haar financiële transacties te delen met externe bedrijven, maar X niet. Kan een extern bedrijf voorgenoemde transactie alsnog inzien?

toegang tot de betaalrekening kan niet ongemerkt, onbedoeld of onbewust plaatsvinden. De toestemming voor toegang tot de betaalrekening bij betaalinitiatiediensten geldt per transactie. Bij rekeninginformatiediensten kan deze voor maximaal 90 dagen worden gegeven. Daarna moet opnieuw toestemming worden gevraagd. Als geen nieuwe toestemming wordt gegeven moeten de gegevens van de betaaldienstgebruiker worden gewist. De betrokkene kan hier zo nodig expliciet om vragen (artikel 17 AVG). Banken en andere betaaldienstverleners zijn dus reeds, op grond van de technische standaarden voor sterke cliëntauthenticatie verplicht om elk kwartaal expliciet toestemming te vragen.

Ten aanzien van het informeren van burgers via het MOB wordt verwezen naar de beantwoording van vraag 86.

Voor de rol van externe (derde) partijen wordt verwezen naar de beantwoording van vraag 82. Bij het aangaan van de overeenkomst moet de betaaldienstgebruiker worden geïnformeerd over de verwerking van persoonsgegevens. Als toestemming wordt gevraagd aan de betaaldienstgebruiker om toegang tot meer gegevens dan noodzakelijk voor de uitvoering van de overeenkomst tussen partijen, mag deze bredere toestemming niet voorwaardelijk zijn om de overeenkomst (voor het verlenen van de betaaldienst) te kunnen afsluiten. Het verzoek om toestemming mag ook geen deel uitmaken van de algemene voorwaarden en moet begrijpelijk zijn opgesteld.

Indien de rekeninginformatiedienstverlener, na uitdrukkelijke toestemming, toegang krijgt tot de betaalrekening en de rekeninggegevens, kan het zo zijn dat hij ook toegang krijgt tot persoonsgegevens van anderen dan de betaaldienstgebruiker (te weten gegevens van hen aan wie de betaaldienstgebruiker geld heeft overgemaakt of van wie hij geld heeft ontvangen). In zijn algemeenheid geldt dat als de betaaldienstverlener toegang krijgt tot persoonsgegevens, hij zich dient te houden aan de AVG. Een rekeninginformatiedienstverlener kan de (persoons)gegevens van derden nodig hebben voor het verlenen van een door een betaaldienstgebruiker gevraagde rekeninginformatiedienst, om bijvoorbeeld in beeld te brengen hoeveel geldmiddelen de gebruiker aan derden heeft overgemaakt. Ingevolge PSD II heeft een betaaldienstgebruiker jegens banken het recht om van een rekeninginformatiedienst gebruik te kunnen maken. Om dat recht daadwerkelijk uit te kunnen oefenen, vloeit daaruit een wettelijk vastgelegde verplichting voort voor banken om aan derde partijen die rekeninginformatiediensten verlenen toegang tot de betaalrekening te verlenen. Verwerking van gegevens van derden is toegestaan voor zover dat noodzakelijk is voor het verlenen van de gevraagde rekeninginformatiedienst. PSD II ziet alleen op toegang tot betaalrekeningen en in verband daarmee tot persoonsgegevens, ten behoeve van het verlenen van betaaldiensten aan de betaaldienstgebruiker die daarom vraagt. De AVG verbiedt dat persoonsgegevens voor niet-verenigbare doelen worden verwerkt. Persoonsgegevens van derden kunnen daarom niet aan andere partijen (zoals commerciële bedrijven) worden doorgegeven of voor andere bedrijfsactiviteiten dan de gevraagde rekeninginformatiedienst voor die specifieke gebruiker worden gebruikt, zonder dat deze derde zelf daar toestemming voor heeft gegeven. Op grond van de AVG is dit ook niet toegestaan als de betaaldienstgebruiker zelf wel toestemming heeft verleend om zijn gegevens te delen met een andere partij. Dit kan wellicht worden verduidelijkt aan de hand van het volgende voorbeeld. Een betaaldienstgebruiker heeft opdracht gegeven aan een betaaldienstverlener om hem een rekeninginformatiedienst te verlenen voor het maken van een online huishoudboekje, waarin onder meer inzichtelijk is hoeveel geld hij per maand overmaakt aan zijn dochter voor haar studie. Voorafgaand aan deze opdracht heeft hij uitdrukkelijk

toestemming gegeven aan de betreffende betaaldienstverlener voor toegang tot zijn persoonsgegevens die nodig zijn voor het verlenen van deze specifieke betaaldienst. Als de betaaldienstverlener zijn persoonsgegevens ook wil gebruiken om hem een zorgverzekering op maat aan te bieden, mag dat alleen als de betaaldienstgebruiker daarvoor toestemming heeft gegeven. Deze kan voor dat doel alleen toestemming geven voor zover het gaat om gebruik van zijn eigen persoonsgegevens. Voor het gebruik van de persoonsgegevens van zijn dochter kan alleen zijn dochter toestemming geven. Als zij dat niet doet, mogen haar persoonsgegevens – waartoe de betaaldienstverlener wel toegang had voor het verlenen van de rekeninginformatiedienst – niet gebruikt worden voor het aanbieden van een zorgverzekering.

Verhouding tot de Algemene Verordening Gegevensbescherming

94) De leden van de PVV-fractie vragen of de regering nader kan ingaan op de Algemene Verordening Gegevensbescherming (AVG) en of het op basis hiervan duidelijk zal zijn welke data banken mogen delen.

95) De leden van de Groenlinks-fractie vragen wat er gebeurt in geval van strijdigheid tussen de bepalingen van PSD II en de AVG. Waar wordt voorrang aan gegeven in geval van tegenstrijdigheid?

96) Voorts vragen de leden van de GroenLinks-fractie welke informatie met betrekking tot de AVG de regering nog niet ter beschikking had bij het opstellen van deze memorie van toelichting, die relevant is voor het wetgevingsproces. Wanneer verwacht de regering deze informatie te ontvangen en te delen met de Kamer? Zal dit plaatsvinden gedurende de behandeling van het wetsvoorstel?

97) De leden van de SP-fractie vinden dat wat er in de memorie van toelichting wordt gesteld onjuist is. Deze leden menen dat er nog niet gekeken is welk effect PSD II heeft op de AVG. Graag vragen deze leden de regering te onderzoeken hoe de PSD II past binnen de kaders van de AVG. Met name vragen deze leden de regering dit, wanneer persoonsgegevens buiten de EU/EER terechtkomen. Zij stellen dat dan geen toezichthouder nog juridische gronden heeft om toezicht te houden. De leden van de SP-fractie vragen de regering welke bescherming dan geldt voor consumenten.

De fracties van PVV, GroenLinks, en SP hebben aandacht gevraagd voor de verhouding tussen de Algemene Verordening Gegevensbescherming en de Richtlijn PSD II op het gebied van bescherming van persoonsgegevens bij het verlenen van betaaldiensten. Naar aanleiding hiervan verduidelijk ik graag dat de verwerking van persoonsgegevens voor het verlenen van betaaldiensten moet voldoen aan de eisen van de AVG én van PSD II.

Op grond van de AVG moet worden voldaan aan de beginselen van gegevensverwerking, die in artikel 5 AVG zijn neergelegd en die in de AVG nader zijn uitgewerkt en geconcretiseerd. Zo moeten persoonsgegevens onder meer worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is, moeten deze voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt. De verwerking moet toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt, juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden

verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren. Voor een nadere toelichting op de eisen die voortvloeien uit de AVG wordt verwezen naar de AVG zelf en naar de memorie van toelichting bij de Uitvoeringswet AVG[23].

Op één punt geeft PSD II aanvullende gegevensbescherming ten opzichte van de AVG. In artikel 94 (2) PSD II is bepaald dat bij de verwerking van gegevens in het kader van het verlenen van een betaaldienst uitdrukkelijke toestemming nodig is van de betaaldienstgebruiker als extra voorwaarde voordat diens gegevens mogen worden verwerkt. Deze eis komt bovenop de eisen die de AVG stelt, waaronder de eis dat er een grondslag moet zijn voor gegevensverwerkingen in het algemeen (zie artikel 6, eerste lid, AVG). Concreet houdt dit in dat de grondslag voor de gegevensverwerking voor het verlenen van betaaldiensten (veelal) de overeenkomst zal zijn (onderdeel b van genoemd artikel 6, eerste lid, AVG) en dat daarenboven voor die gegevensverwerking ook nog deze additionele toestemmingsvoorwaarde geldt. Op dit onderdeel geeft PSD II een bijzondere regel die, vanwege het bijzondere, sectorspecifieke karakter, bovenop het regime van de AVG geldt. Aangezien de voorwaarde van uitdrukkelijke toestemming zal gelden bovenop de voorwaarden die de AVG stelt, wordt de betaaldienstgebruiker beter beschermd dan wanneer enkel de AVG van toepassing zou zijn. Op de samenloop tussen de verschillende voorwaarden kom ik verderop in de nota naar aanleiding van het verslag terug, bij bespreking van het advies van de AP.

De AVG zelf kent overigens ook een toestemmingsvereiste, namelijk als grondslag voor gegevensverwerking (artikel 6, eerste lid, onderdeel a, AVG). Zoals gezegd zal de grondslag voor verwerking van persoonsgegevens voor het verlenen van betaaldiensten veelal de overeenkomst zijn. Alleen als sprake is van gegevensverwerking door betaaldienstverleners voor andere, niet-verenigbare, doelen dan het verlenen van de gevraagde betaaldienst, zoals het aanbieden van een andere dienst of product, kan het verlenen van (aanvullende) toestemming in de zin van de AVG mogelijk dienen als grondslag voor verwerking van gegevens. In een dergelijk geval is er dan dus sprake van een cumulatie van toestemmingsvereisten. In de praktijk volstaat dan het eenmalig vragen van toestemming waarbij dan wel toegelicht wordt dat de toestemming beide doelen dient.

Naar aanleiding van de vragen van de leden van de SP-fractie of persoonsgegevens buiten de EU kunnen worden gebracht, geef ik aan dat dit niet zomaar kan. De AVG geeft namelijk strikte voorwaarden waaronder gegevens in derde landen mogen worden verwerkt. Ik ben hier bij de beantwoording van vraag 67 nader op ingegaan.

Datalekken

98) De leden van de CDA-fractie benadrukken de grote persoonlijke en financiële gevolgen wanneer privacygevoelige informatie op straat komt te liggen. In dit kader vragen deze leden welke rechten een gebruiker heeft wanneer zijn gegevens onbedoeld openbaar worden gemaakt, bijvoorbeeld na een hack. Is er recht op een schadevergoeding?

99) De leden van de GroenLinks-fractie vragen welke maatregelen kunnen worden getroffen in het geval van een datalek.

---

[23] Kamerstukken II 2017/18, 34 851, nr. 3.

De leden van de fracties van de CDA en GroenLinks vragen naar de gevolgen van een datalek. Dit zijn kwesties die in de AVG zijn geregeld. Zoals gezegd is de AVG ook van toepassing op de verwerking van persoonsgegevens voor het verlenen van betaaldiensten. Zo bepaalt artikel 33 AVG dat de verwerkingsverantwoordelijke melding maakt van een inbreuk op het recht op bescherming van persoonsgegevens aan de toezichthoudende autoriteit (in Nederland: de AP). Voor financiële ondernemingen geldt in voorkomende gevallen een meldplicht aan DNB of de AFM. Financiële ondernemingen, waaronder betaaldienstverleners, zijn uitgezonderd van de verplichting van artikel 34 AVG (artikel 42 UAVG), als gevolg waarvan zij niet verplicht zijn elk datalek ook te melden aan de betrokken klanten, met het oog op voorkoming van onnodige paniek. De zorgplicht van de financiële onderneming brengt echter mee dat zij, als dat mogelijk is, haar klanten informeert. Dit doet zij nu al bij incidenten onder de Wet op het financieel toezicht en dat zal niet anders zijn ten aanzien van datalekken onder dit wetsvoorstel. Daarnaast geldt dat ingevolge PSD II DNB in kennis moet worden gesteld van elk groot beveiligingsincident. Indien dit incident gevolgen kan hebben voor de financiële belangen van de betaaldienstgebruikers moeten ook de betaaldienstgebruikers onverwijld in kennis worden gesteld van het incident en moet aan hen worden meegedeeld hoe zij de mogelijk schadelijke gevolgen van het incident kunnen beperken.

Artikel 82 (1) van de AVG bepaalt dat eenieder die materiële of immateriële schade heeft geleden ten gevolge van een inbreuk op deze verordening, het recht heeft om van de verwerkingsverantwoordelijke of de verwerker schadevergoeding te ontvangen voor de geleden schade. In Nederland staat hiertoe een schadevergoedingsactie open op grond van onrechtmatige daad (artikel 6:162 BW).

100) De nieuwe wet- en regelgeving zal ertoe leiden dat externe bedrijven die niet gehouden zijn aan de dwingende regelgeving voor de bancaire sector, toch financiële transacties kunnen inzien en gebruiken. De leden van de PvdD-fractie vragen of de regering de mening deelt dat dit grote risico's met zich mee brengt? Zo nee, waarom niet? Denk aan de verantwoordelijkheid en aansprakelijkheid van externe bedrijven indien problemen ontstaan met het gebruik van de verkregen financiële gegevens, maar dus ook dat die risico's wezenlijk zijn.

Naar aanleiding van deze vragen, merkt de regering op dat elk bedrijf dat betaaldiensten verleent waarbij gegevens worden verwerkt zich aan de regels van de AVG en PSD II zal moeten houden. Hier is bij de beantwoording van de vragen 94 tot en met 97 op ingegaan. Bovendien zal elk bedrijf dat betaaldiensten verleent een vergunning moeten hebben, waarbij DNB zal toetsen of een bedrijf voldoet aan de voorwaarden. Welke voorwaarden dit zijn hangt af van de soort betaaldiensten die het bedrijf wil verlenen en waarvoor een vergunning is aangevraagd. Verder zijn deze bedrijven onderworpen aan doorlopend toezicht van DNB, AFM en de AP. De AP zal er bovendien op toezien of de wijze waarop de gegevens worden verwerkt voldoet aan de AVG. Hierdoor zijn de risico's zoveel mogelijk beperkt.

Koppelverkoop

101) De leden van de CDA-fractie vragen naar de mogelijkheden voor het koppelen van bepaalde consumentenvoordelen aan het toestemming geven voor het delen van persoonsgegevens. Zij doelen hierbij bijvoorbeeld op een aanbieder van betaaldiensten die korting aanbiedt op bepaalde producten, indien de gebruiker bereid is om zijn betaalgegevens te delen om wat voor reden dan ook. Deze leden zouden het zeer

bezwaarlijk vinden als dergelijke koppelverkoop toegestaan zou zijn, omdat het de drempel verlaagt voor het delen van persoonlijke gegevens, terwijl gebruikers niet altijd de gevolgen goed kunnen doorgronden. Biedt de richtlijn mogelijkheden om deze vorm van koppelen c.q. delen van gegevens en korting op producten te verbieden? Zo nee, wat vindt de regering hiervan? Zo nee, zijn er mogelijkheden om dit in nationale wetgeving wel separaat te regelen? Zo ja, is dit dan ook geregeld?

102) De leden van de D66-fractie constateren dat sommige dienstverleners ook andere diensten aanbieden waar cliënten gebruik van maken. Kan de regering aangeven of het niet verlenen van toestemming voor het ene product van een dienstverlener gevolgen kan hebben voor de toegang tot een ander product? Concreter: zou bijvoorbeeld Google toegang tot Gmail kunnen verhinderen wanneer een cliënt geen toestemming geeft voor het delen van persoonsgegevens? Wanneer een cliënt wel toestemming geeft, worden de gegevens dan apart bewaard van de data uit andere diensten of staat het de aanbieder vrij om data te koppelen?

103) De leden van de GroenLinks-fractie vragen in hoeverre partijen de consument mogen overhalen akkoord te gaan door (gratis) online diensten aan te bieden, kortingen of andere voordelen in het vooruitzicht te stellen. Zijn consumenten zich altijd bewust dat zij in die gevallen, in plaats van met geld, met hun persoonlijke data betalen?

Naar aanleiding van de vragen van de fracties van het CDA, D66 en GroenLinks, verduidelijk ik graag dat bescherming van persoonsgegevens is geregeld in de AVG. Dit houdt in dat er onder meer een grondslag voor verwerking moet zijn; voor het verlenen van betaaldiensten zal dit veelal de overeenkomst zijn (artikel 6 (1) (b) AVG). In dat geval zal de daarmee rechtmatige gegevensverwerking noodzakelijk moeten zijn voor de uitvoering van de overeenkomst. Deze grondslag moet strikt worden uitgelegd. Indien een bank bijvoorbeeld de betaalgegevens van een betrokkene wil gebruiken voor marketingdoeleinden, dan is dit niet noodzakelijk voor de uitvoering van de overeenkomst. De overeenkomst kan dan niet als rechtsgrondslag dienen voor de gegevensverwerking voor marketingdoeleinden. Daarvoor zal apart toestemming moeten worden gevraagd (rechtsgrondslag is dan toestemming, art 6(1) (a) AVG). De betrokkene moet in een dergelijk geval zijn toestemming vrijelijk kunnen geven en ook weigeren. Als daar geen sprake van is dan is er niet voldaan aan de eisen die de AVG stelt aan toestemming (artikel 7 AVG). In hoeverre het koppelen van bepaalde voordelen aan het geven van toestemming door consumenten voor het gebruiken van zijn gegevens toelaatbaar is, zal aan de hand van deze voorwaarde van de AVG beoordeeld moeten worden. Het is aan de AP, en uiteindelijk aan de rechter, om hierover te oordelen, aangezien het de nadere invulling en interpretatie van een Europese norm betreft.

In het door de leden van de D66-fractie genoemde geval van een dienstverlener die meerdere soorten diensten aanbiedt waarbij gegevens worden verwerkt, vereist de AVG dat per dienst wordt beoordeeld of en in hoeverre verwerking van persoonsgegevens noodzakelijk is ter uitvoering van de overeenkomst. Een dienstverleningsovereenkomst mag niet zomaar worden geweigerd indien een betrokkene weigert een andere, gekoppelde, overeenkomst te sluiten. Er is dan namelijk geen vrijelijk aangegane overeenkomst. Verder is het koppelen van persoonsgegevens die bij het verlenen van verschillende diensten zijn verwerkt, ook een verwerking die aan de eisen van de AVG moet voldoen. Zo mag deze verdere verwerking alleen als deze verenigbaar is met het oorspronkelijke doel waarvoor de persoonsgegevens zijn verkregen. Is deze verdere verwerking niet verenigbaar, dan is aanvullende toestemming nodig van

de betrokkene of is verdere verwerking mogelijk als er een wettelijke plicht rust op de verwerkingsverantwoordelijke. In beide gevallen moet de betrokkene geïnformeerd worden over de verdere verwerking (artikel 13 (3) AVG). Ter verduidelijking verwijs ik hierbij naar het hiervoor gegeven voorbeeld over het aanbieden van een zorgverzekering, waarbij gebruik gemaakt wordt van persoonsgegevens die zijn verkregen voor het verlenen van een rekeninginformatiedienst.

De leden van de fractie van GroenLinks vragen naar verlening van gratis online betaaldiensten in ruil voor persoonsgegevens. Ook hiervoor zal een voldoende grondslag voor verwerking moeten zijn, zoals overeenkomst of toestemming. Verder is het van belang dat de betrokkene weet wat er met zijn gegevens gebeurt (artikel 13 AVG). Meer algemeen is het de vraag in hoeverre mag worden «betaald» met het verstrekken van persoonsgegevens in ruil voor het verlenen van betaaldiensten. De Europese Gegevensbeschermingstoezichthouder (EDPS) heeft zich in het verleden hierover kritisch uitgelaten. Het is uiteindelijk aan de AP en de rechter om te beoordelen onder welke voorwaarden dat eventueel mogelijk is.

Overige

104) De leden van de PVV-fractie willen weten welke maatregelen er getroffen zullen worden om de privacy van de consumenten onder PSD II te waarborgen.
De leden van de PVV-fractie willen verder weten op welke wijze banken en financiële nieuwkomers consumenten zullen informeren over PSD II en over de gevolgen die het met zich meebrengt.

Zoals hiervoor bij de beantwoording van de vragen 94 tot en met 97 aangegeven, moet de verwerking van gegevens plaatsvinden in overeenstemming met de eisen die de AVG en PSD II stellen. Op naleving van deze eisen zal de Autoriteit Persoonsgegevens toezien. Verder werken betaaldienstverleners, waaronder banken, aan maatregelen om te zorgen dat ook in de praktijk aan deze eisen zal worden voldaan.

Banken en derde partijen informeren hun klanten over PSD II via (de wijziging van) hun algemene voorwaarden alsook via hun websites en die van de Betaalvereniging Nederland. Op verzoek van het Maatschappelijk Overleg Betalingsverkeer (MOB) heeft DNB onlangs een aantal veelgestelde vragen en antwoorden over PSD II op haar website gepubliceerd. Zie https://www.dnb.nl/betalingsverkeer/psd2/index.jsp. Daarnaast start DNB, op verzoek van het MOB, in het najaar van 2018 met een voorlichtingscampagne voor consumenten en bedrijven om de bewustwording over de veranderingen in het betalingsverkeer als gevolg van PSD II te vergroten. Verder zou het MOB graag zien dat banken consumenten in mobiel bankieren apps en bij internetbankieren een overzicht bieden van de dienstverleners waaraan toestemming is verleend.

105) De leden van de D66-fractie zijn van mening dat een correcte omgang met persoonsgegevens een groot goed is. Zij hebben hierover nog enkele vragen. Overweging 89 van de richtlijn noemt de beginselen noodzaak, evenredigheid, doelbegrenzing en een niet-buitensporige gegevensbewaarperiode. Kan de regering per term aangeven wanneer er sprake is van deze beginselen? Kan hiervan worden afgeweken door hetzij de dienstverlener, hetzij de cliënt? Kan een cliënt via een dashboard controle uitoefenen op welke gegevens hij of zij wil delen en voor welke periode? Kan de regering aangeven hoe deze beginselen afwijken van de voorwaarden die aan banken worden gesteld voor de bescherming van persoonsgegevens? Kan de regering ook aangeven in hoeverre de richtlijn

afwijkt van de regels die nu voor banken gelden op gebied van het delen van persoonsgegevens ter voorkomen en opsporing van betalingsfraude?

Overweging 89 verwijst naar een aantal beginselen van verwerking van persoonsgegevens. Deze beginselen komen overeen met de beginselen die in artikel 5 van de AVG zijn opgenomen en die de basis vormen voor het wettelijk kader van gegevensverwerking. Toegespitst op PSD II en betaaldiensten, betekent dit dat er een grondslag moet zijn voor de verwerking van gegevens voor het verlenen van betaaldiensten. Dat zal in dit geval meestal een onderliggende overeenkomst zijn. Verder moet het noodzakelijk zijn om de gegevens van de betrokkene te verwerken voor het verlenen van de gevraagde betaaldienst en moet de verwerking van gegevens evenredig zijn. Dat wil zeggen dat niet meer gegevens mogen worden verwerkt dan noodzakelijk voor het verlenen van de gevraagde betaaldienst. Voor een betaalinitiatiedienst bijvoorbeeld, zal het niet nodig zijn dat de betaalinitiatiedienstverlener toegang heeft tot alle transacties die de betaaldienstgebruiker in het verleden heeft verricht. Er zal wel informatie nodig zijn m.b.t. identificatiegegevens van de rekening (IBAN, naam) en het aanwezige saldo (is er voldoende saldo aanwezig op de rekening?) en nog te verwerken transacties. De verwerking van persoonsgegevens is daarnaast beperkt tot een doel; in dit geval de gevraagde betaaldienst. Zo mogen de gegevens die verwerkt worden om een betaling te initiëren niet zomaar gebruikt worden om de betaaldienstgebruiker reclamemateriaal te sturen. Volgens het beginsel van een niet-buitensporige gegevensbewaarperiode mogen gegevens niet langer worden bewaard dan nodig voor het betreffende doel. Bij een betaalinitiatiedienst zal het bijvoorbeeld niet nodig zijn om de gegevens lang te bewaren: slechts voor de uitvoering van de transactie plus de tijd waarbinnen de betaaldienstgebruiker een geïnitieerde transactie kan betwisten. Van deze eisen kan niet ten nadele van de klant worden afgeweken. PSD II wijkt niet af van de regels die nu gelden voor banken op het gebied van delen van persoonsgegevens ter voorkoming en opsporing van betalingsfraude.

106) De leden van de GroenLinks-fractie lezen dat de Afdeling aangeeft dat er geen specifieke grondslag is voor wat betreft bescherming van persoonsgegevens en dat zij adviseert te voorzien in een grondslag voor de implementatie van het vereiste «uitdrukkelijke toestemming» in lagere regelgeving. Hoe kijkt de regering hier tegen aan? De voorgenoemde leden vragen welk voordeel het heeft regels met betrekking tot (bescherming van) persoonsgegevens bij of krachtens algemene maatregel van bestuur vast te stellen, in plaats van bij wet. Wat zijn verder de voor- en nadelen van het opnemen van een voorhangbepaling?

Het advies van de Afdeling is op dit punt gevolgd. Er is naar aanleiding van het advies van de Afdeling in het wetsvoorstel een bepaling opgenomen, waardoor de Wft in artikel 3:17 zal voorzien in een specifieke delegatiegrondslag ter implementatie van artikel 94 (2) van de richtlijn. De algemene maatregel van bestuur die gebaseerd wordt op deze bepaling van de wet, voorziet in implementatie van artikel 94 (2) van de richtlijn. Deze wijze van implementatie biedt het voordeel dat, binnen de ruimte die de richtlijn biedt, op kortere termijn wijzigingen of specificaties kunnen worden aangebracht, hetgeen minder snel mogelijk is wanneer de bepaling in de wet wordt opgenomen. Bovendien heeft deze wijze van implementatie bij PSD II het voordeel dat de praktijk en de AP opnieuw over de gegevensbeschermingsbepalingen kon worden geconsulteerd. Indien zou worden voorzien in een voorhangbepaling, zou deze tijdwinst deels teniet worden gedaan, doordat de totstandkoming van de algemene maatregel van bestuur een aantal weken langer zal duren.

11. Nieuwe rol EBA

107) Hoe wordt de nauwe samenwerking tussen de Europese Bankautoriteit (EBA) en de ECB ingevuld, zo vragen de leden van de VVD-fractie. Hoe wordt voorkomen dat delen van het toezicht tussen wal en schip vallen? Kan hierbij ook ingegaan worden op het commentaar van de AFM, die stelt dat het toezicht over PSD II te zeer verspreid is over de verschillende nationale en internationale toezichthouders?

De EBA en de ECB zijn gezamenlijk voorzitter van het zogenoemde SecuRe Pay Forum. Dit is een samenwerkingsorgaan van «overseers» op betaalsystemen en -instrumenten en toezichthouders op betaaldienstverleners, dat tot doel heeft de veiligheid van het retailbetalingsverkeer in Europa te bevorderen. De technische reguleringsnormen en richtsnoeren die PSD II verlangt op het gebied van veiligheid zijn gezamenlijk ontwikkeld door het SecuRe Pay Forum en EBA. Met PSD II is het toezicht in Europese landen op betaaldienstverlening versterkt en geharmoniseerd. Grote lacunes in het toezicht zijn voorshands niet zichtbaar. Met het SecuRe Pay Forum en EBA wordt effectieve samenwerking gerealiseerd. De vier bij PSD II betrokken toezichthouders in Nederland – DNB, AFM, AP en ACM – zijn met elkaar in gesprek om hun samenwerking te intensiveren en op elkaar af te stemmen.

108) De leden van de PVV-fractie vragen welke nieuwe taken EBA erbij krijgt en in hoeverre er sprake is van een overdracht van soevereiniteit.

De hoofdtaak van EBA is het ontwerpen van technische reguleringsnormen (die door de Commissie worden vastgesteld) en het opstellen van richtsnoeren voor (het toezicht op) financiële instellingen. Deze rol had de EBA ook al onder PSD I. PSD II verleent EBA geen nieuwe taken en er is geen sprake van overdracht van soevereiniteit.

109) De leden van de SP-fractie menen dat het introduceren van een nieuwe toezichthouder beter moet worden geborgd in nationale wetgeving. Deze leden vinden dat het ontbreken van richtsnoeren en faciliteiten niet aan geloofwaardigheid doet winnen. De voorgenoemde leden hopen dat PSD II op korte termijn goed geïmplementeerd en beheerd gaat worden en vragen de regering of zij dat kan garanderen.

Voor de beantwoording van deze vraag wordt verwezen naar de beantwoording van vraag 107.

§4. De richtlijn in Europese context

110) Een van de doelstellingen van de richtlijn is concurrentie binnen de sector te bevorderen. De leden van de D66-fractie vragen de regering aan te geven hoe dit samenvalt met verordening (EU) nr. 260/2012, die de nummerportabiliteit bemoeilijkt?

De SEPA-verordening voorziet in de invoering van betalingsstandaarden, -voorschriften en -praktijken en een geïntegreerde verwerking van betalingen.[24] Met de invoering van de *single euro payments area* (SEPA) wordt één uniforme Europese betaalmarkt gecreëerd, waarin alle eurobetalingen in de EU zijn gestandaardiseerd en het girale betalingsverkeer meer uniform en transparant is geworden. De PSD II-richtlijn richt zich niet op betaalinfrastructuur maar op concurrentie op basis van

[24] VERORDENING (EU) Nr. 260/2012 VAN HET EUROPEES PARLEMENT EN DE RAAD van 14 maart 2012 tot vaststelling van technische en bedrijfsmatige vereisten voor overmakingen en automatische afschrijvingen in euro en tot wijziging van Verordening (EG) nr. 924/2009.

(nieuwe) betaaldiensten die gebruik maken van deze betaalinfrastructuur. Overigens zal met de invoering van PSD II naar verwachting een deel van het betalingsverkeer verschuiven van traditionele banken naar nieuwe Fintech marktpartijen. De bankrekening zal echter blijven bestaan als de plaats waar het geld van een klant daadwerkelijk is opgeslagen. De nieuwe betaaldiensten worden dan ook naast of bovenop de bankrekening gebruikt. Het nader onderzoek doen naar overstappen van bank met een bepaalde vorm van nummerbehoud (nummerportabiliteit) blijft dan relevant om concurrentieproblemen bij het overstappen van bank op te lossen.

111) De leden van de GroenLinks-fractie vragen wat er gebeurt als verschillende EU-lidstaten verschillende interpretaties van de AVG hanteren? Kunnen bedrijven landen tegen elkaar uit gaan spelen, waardoor er een race naar de bodem ontstaat op het gebied van privacy?

Om een consistente toepassing van de AVG in de Unie te bevorderen en te voorkomen dat bepalingen uit de AVG uiteenlopend worden geïnterpreteerd, bevat deze verordening een zogenaamd «coherentiemechanisme». Dit wordt toegelicht in de memorie van toelichting bij de Uitvoeringswet AVG (paragraaf 3.2 De hoofdlijnen van hoofdstuk VII van de verordening inzake samenwerking en coherentie in de praktijk). Zo dienen gegevensbeschermingstoezichthouders – als dit aangewezen is – samen te werken om in concrete gevallen te bepalen welke toezichthouder bevoegd is om op te treden. Verder dient zoveel mogelijk tot eenduidige uitleg van begrippen en regels te worden gekomen.[25] Hiertoe is in de AVG een Europees Comité voor gegevensbescherming in het leven geroepen (de opvolger van de huidige artikel 29 Werkgroep). Dit Comité bestaat uit de voorzitter van één toezichthoudende autoriteit per lidstaat en de Europese Toezichthouder voor gegevensbescherming, of hun respectievelijke vertegenwoordigers (artikel 68 lid 3 AVG). Het Comité kan zogenaamde soft law uitvaardigen die juridisch niet bindend is, maar waar, net zoals nu van de opinies van de huidige artikel 29 werkgroep, wel een zeker gezag uitgaat. Uiteindelijk is natuurlijk het laatste woord aan de (Europese) rechter ten aanzien van de vraag of in een concreet geval de juiste interpretatie is gegeven.

112) De leden van fractie van GroenLinks vragen verder hoe wordt voorkomen dat niet elke Europese toezichthouder de open normen in de richtlijn even streng uitlegt en even streng handhaaft op overtreding? Wat zou er mis kunnen gaan als er niet even streng wordt gehandhaafd?

Voor het antwoord op deze vraag wordt verwezen naar de beantwoording van vraag 12.

113) De genoemde leden van GroenLinks willen verder weten of het klopt dat er na 13 januari 2018 een situatie kan ontstaan waarin Nederlandse bedrijven nog geen vergunning kunnen krijgen, maar buitenlandse partijen die in eigen land een vergunning hebben gekregen, wel al toegang eisen tot de Nederlandse markt.

Ja, dat is mogelijk. Zowel vergunninghoudende als niet-vergunninghoudende partijen uit andere lidstaten kunnen, voordat de implementatiewet in werking treedt, in Nederland hun diensten aanbieden (er geldt immers nog geen vergunningsplicht). Totdat de implementatiewet in werking treedt hebben Nederlandse banken echter nog niet de wettelijke verplichting om aan deze partijen toegang te verlenen tot de betaalrekeningen van hun klanten.

---

[25] Zie *Kamerstukken II* 2017/18, 34 851, nr. 3.

114) De leden van de SP-fractie constateren dat op 1 augustus 2014 IBAN is geïntroduceerd (door SEPA) en men nu keihard bezig is dit ongedaan te maken, omdat het leidt tot tal van fouten door consumenten. Deze leden vragen de regering waartoe dit heeft geleid. De leden van de SP-fractie constateren dat tot nu toe de banken in Nederland niet controleren of een naam bij een rekeningnummer hoort. Dat pakt vaak vervelend uit bij verkeerde overboekingen, omdat het terughalen van verkeerd overgemaakt geld alleen kan als de rekeninghouder daaraan meewerkt. Deze leden vragen de regering de schade te becijferen die alleen al hiermee gepaard is gegaan. Zij vragen de regering een getal te noemen hoeveel schade consumenten en bedrijven zullen leiden door fouten met PSD II. Is het niet verstandig dit eerst goed te onderzoeken.

In de eerste plaats wil de regering het beeld wegnemen dat het IBAN de oorzaak is van onbedoelde overboekingen en dat men bezig zou zijn het IBAN ongedaan te maken. Ook vóór de IBAN-introductie maakten consumenten deze fouten, omdat in ca 2/3 van het betalingsverkeer nooit naam–nummercontrole plaatsvond. Alleen in het oude circuit van de voormalige Postbank vond die controle plaats, omdat de gironummers niet zelfcontrolerend waren. Aangezien het IBAN wel zelfcontrolerend is en het bovendien bij Europese Verordening is voorgeschreven als unieke identifier van de rekeninghouder en dus leidend is, heeft de ING voor de ex-gironummers deze interne controle losgelaten.[26]

Verder wordt opgemerkt dat er ook de nodige stappen zijn gezet om het aantal onbedoelde overboekingen te doen verminderen. Betaalvereniging Nederland heeft op 25 januari jl. met de Consumentenbond de uitkomsten van het onderzoek naar onverschuldigde betalingen besproken. In 2015 is de Betaalvereniging met de Consumentenbond overeengekomen om te onderzoeken hoe vaak consumenten in 2016 gebruik maakten van de Procedure Onverschuldigde Betaling (POB) en wat de redenen daarvoor waren. De POB is bedoeld om consumenten te helpen hun geld terug te krijgen als zij onbedoeld hebben overgeboekt naar een verkeerde begunstigde (een onverschuldigde betaling hebben gedaan). Uit het onderzoek is gebleken dat particuliere bankklanten in 2016 van februari t/m december 14.357 maal (gemiddeld 1.305 keer per maand) van de POB gebruik hebben gemaakt. Dit is een daling ten opzichte van 2014 en 2015, toen de POB gemiddeld 4.500, respectievelijk 1.500 keer per maand werd uitgevoerd.

In 2017 hebben banken tal van maatregelen genomen om de kans op fraude en vergissingen van klanten te verkleinen, met als belangrijkste de (geleidelijke) invoering van de IBAN-Naam Check. Hierbij krijgt de consument bij afwijkingen tussen de opgegeven en geregistreerde naam een waarschuwing. Deze blijft echter zelf verantwoordelijk voor wat hij daarmee doet. Onbedoelde overboekingen kunnen hier niet voor 100% mee worden voorkomen. Enige banken hebben het ingevoerd, andere banken zijn nog doende.

§5. Wijze van implementatie

115) De leden van de VVD-fractie hebben uiteenlopende vragen over de implementatie van de richtlijn. Waarom is hier gekozen voor een richtlijn als geëigend rechtsmiddel en niet een verordening, zeker daar artikel 107 van de richtlijn op veel plekken een volledige harmonisatie voorschrijft?

[26] Gevolg is zelfs dat hierdoor onbedoelde overboekingen die het gevolg waren van typefouten in de niet-zelfcontroleerbare gironummers worden voorkomen, omdat fouten in het IBAN door de zelfcontrole niet tot overboekingen kunnen leiden.

Het rechtsinstrument wordt bepaald door de grondslag in het Verdrag betreffende de werking van de Europese Unie. De grondslag van PSD II is artikel 114 Verdrag betreffende de werking van de EU (VWEU), namelijk harmonisatie van de interne markt, en dan specifiek de harmonisatie van het vrije verkeer van personen, diensten en kapitaal (artt. 45 tot en met 66 van het Werkingsverdrag EU). De Europese Commissie gaf in het impact assessment aan dat een actualisering van de bestaande regels van richtlijn PSD I de meest wenselijke optie was. Zij stelde daarom voor om het nieuwe instrument evenals PSD I de vorm te geven van een richtlijn. De instrumentkeuze van een richtlijn stelt Nederland in staat om de bepalingen binnen zijn eigen rechtsorde in te passen. Daarom vindt Nederland de door de Commissie gemaakte keuze goed verdedigbaar.

116) De leden van de VVD-fractie vragen op welke manier niet is gebleken dat er behoefte bestaat aan het gebruik maken van de lidstaatoptie, bijvoorbeeld ex artikel 2 (5), artikel 8 (3) en artikel 32 (4)? Welk onderzoek is hiernaar verricht? Welke landen maken wel gebruik van de verschillende lidstaatopties, voor zover bekend, en wat betekent dit voor het level playing field voor Nederlandse aanbieders en consumenten?

117) De leden van de D66-fractie constateren dat er een groot aantal opties zijn voor EU-lidstaten. De regering kiest ervoor van sommige opties wel gebruik te maken en van andere niet. Kan de regering aangeven in hoeverre Nederland hierbij afwijkt van de andere EU-lidstaten? Welke opties worden door andere EU-lidstaten gebruikt? Heeft dat effect op de uitwerking van de richtlijn in praktijk?

Tijdens de voorbereiding van het wetsvoorstel zijn zowel toezichthouders als andere stakeholders betrokken. Ook tijdens de openbare consultatie van het wetsvoorstel zijn partijen in de gelegenheid gesteld om aan te geven of al dan niet gebruik gemaakt zou moeten worden van lidstaatopties. Ten aanzien van een aantal lidstaatopties heeft een expliciete afweging plaatsgevonden naar aanleiding van overleg met belanghebbenden. Het gaat daarbij om de lidstaatopties in de artikelen 38, tweede lid, 61, derde lid, (beide over gelijkstellen micro-ondernemingen met consumenten) en 62, vijfde lid, (verbod vergoeding gebruik betaalinstrument) van PSD II.

Het beeld van het gebruik dat lidstaten – voor zover nu bekend – maken van de verschillende lidstaatopties is divers. Veel lidstaten hebben hun wetgeving ter implementatie van PSD II nog niet gereed. Ten aanzien van de lidstaten die hun wetgeving al wel gereed hebben is geen duidelijke lijn te destilleren. Wat het effect zal zijn van het al dan niet gebruik maken van de verschillende lidstaatopties is niet op voorhand te zeggen en zal derhalve in de praktijk moeten blijken.

§6. Gevolgen voor het bedrijfsleven

118) Welk overleg is er met het bedrijfsleven geweest om de verwachte kosten voor het bedrijfsleven, zowel incidenteel als structureel, te minimaliseren, zo vragen de leden van de VVD-fractie. Kan de regering iets zeggen over de verwachte omvang voor de betaalinitiatiedienstverleners en de verwachte omvang voor de rekeninginformatiedienstverleners? Hoe wordt voorkomen dat vooral kleinere aanbieders geconfronteerd zullen worden met disproportionele structurele en administratieve lasten en daarmee op termijn de markttoegang voorkomen wordt?

De eerste betaalinitiatie- en rekeninginformatiedienstverleners zullen waarschijnlijk in de loop van 2018 van start kunnen gaan. Pas in 2019 zal evenwel gestart worden met de jaarlijkse doorrekening van doorlopende

toezichtkosten. Immers de heffing 2018 voor de doorlopende toezichtkosten wordt gebaseerd op de omzet in 2017 en die was nihil voor deze diensten.

In 2019 wordt de nieuwe Wet bekostiging financieel toezicht 2019 van toepassing, evenals de daaruit voortvloeiende lagere regelgeving. Op grond van die nieuwe wet worden de werkelijke (begrote) kosten per sector in rekening gebracht. Hoe die doorbelasting over de verschillende partijen binnen de sector betaalinstellingen wordt verdeeld, zal in de ministeriële regeling 2019 worden bepaald. Hiervoor zal DNB in het voorjaar van 2019 voorstellen doen aan de Minister. Voor zover het gaat om vergunningaanvragen kan in 2018 al wel een heffing plaatsvinden. Dat betreft een vast bedrag per aanvraag.

119) Banken moeten toegang verlenen aan derde partijen. De leden van de D66-fractie vragen of het in praktijk nu ook al gebeurt, dat banken derde partijen toegang geven tot betaalgegevens wanneer de klant daar toestemming voor geeft? Het systeem van de bank en die van de derde dienstverlener moeten op elkaar aansluiten om betalingsgegevens uit te kunnen wisselen. Wiens verantwoordelijkheid is het dat deze koppeling werkt? Dragen de derde partijen financieel bij aan het in stand houden van de infrastructuur van de bank wanneer zij gebruik maken van de betaalgegevens van die bank? Is er sprake van een fee die de derde partij moet betalen aan de bank?

Toegang door derde partijen komt nu ook al voor, maar alleen op basis van een contract tussen de betreffende derde partij en de bank. Op grond van PSD II mag het aanbieden van betaalinitiatie- en rekeninginformatiediensten niet afhankelijk zijn van een contractuele relatie met de bank. De rekeninghoudende betaaldienstverlener, meestal een bank, is verantwoordelijk voor de koppeling (interface). De derde partijen zijn niet gehouden om een vergoeding te betalen voor het gebruik van de door de bank aangeboden interface. De rekeninghoudende betaaldienstverleners zullen dus de kosten moeten dragen voor het ontwikkelen en in stand houden van de interface.

120) De leden van de D66-fractie lezen in de implementatiewet dat de eenmalige inhoudelijke nalevingskosten naar schatting 58 miljoen euro bedragen en de structurele inhoudelijke nalevingskosten 8 miljoen euro. Hoe is tot deze bedragen gekomen? Wie zal deze kosten dragen? Hoe zijn deze kosten verdeeld tussen banken, betaaldienstverleners en andere partijen?

Op pagina 15 e.v. van de memorie van toelichting staat een nadere beschrijving van de kosten. De geschatte inhoudelijke nalevingskosten hebben met name betrekking op het voldoen aan de verplichting voor banken om toegang te verlenen aan derde partijen die de nieuwe diensten (betaalinitiatie- en rekeninginformatiediensten) willen aanbieden. Met name het gereed maken van een *dedicated interface* tussen de systemen van de banken en die van derde partijen brengt kosten met zich mee. Andere kosten hangen hiermee samen, zoals kosten om te voldoen aan de veiligheidseisen die PSD II stelt aan het verlenen van toegang en kosten met betrekking tot het toepassen van sterkte cliëntauthenticatie. Daarnaast brengt de uitbreiding van de reikwijdte kosten met zich mee. Een groot deel van de transparantie- en consumentenbeschermingseisen die zijn opgenomen in titel III en IV, zijn door deze uitbreiding op meer betalingstransacties van toepassing dan voorheen, namelijk op «one-leg-in» betalingstransacties (waarbij slechts één van de bij de betalingstransactie betrokken betaaldienstverlener zich in de Unie hoeft te bevinden) en op betalingstransacties in elke valuta (voorheen alleen

valuta van lidstaten). Overige kosten hebben betrekking op het voldoen aan de eisen rondom preautorisatie bij betalingstransacties waarbij het bedrag vooraf niet bekend is (zie artikel 75 van de richtlijn) en op het opnieuw distribueren van de als gevolg van PSD II gewijzigde contract- en productvoorwaarden onder bankklanten. Zoals blijkt uit de specificatie worden de kosten hiervoor zoveel mogelijk door de marktpartijen zelf gedragen.

121) De leden van de SP-fractie vragen de regering hoe zij gaat voorkomen dat de kosten op het conto van de consument terechtkomen. Deze leden vragen de regering welke gevolgen het gaat hebben op eventuele prijsstijgingen, dat moet worden voldaan aan zoveel nieuwe wet- en regelgeving vanuit de Europese Commissie, zoals PSD II, e-Privacy en de AVG.

De kosten van implementatie van PSD II zijn weergegeven in de memorie van toelichting bij het wetsvoorstel. Deze kosten kunnen door de financiële sector worden doorberekend in de prijzen van hun producten en diensten. Eén van de doelen van PSD II is echter vergroting van de concurrentie op de betaalmarkt door toetreding van nieuwe partijen mogelijk te maken. Op termijn zal dit juist verlaging van prijzen voor consumenten tot gevolg kunnen hebben. Voor de administratieve lasten en nalevingskosten van de AVG verwijs ik graag naar de memorie van toelichting bij de Uitvoeringswet AVG.[27] Bij de nog in onderhandeling zijnde Verordening e-privacy verwijs ik naar het aan uw Kamer gestuurde BNC-fiche van 17 februari 2017.[28]

§7. Financiële gevolgen voor de rijksbegroting

122) De leden van de Groenlinks-fractie vragen of de regering een uitsplitsing kan maken waar de structurele kosten van 8,4 miljoen euro neerslaan. Deze leden constateren dat grote onzekerheid bestaat rondom de schatting van de extra kosten voor toezichthouders. Wat gebeurt er als er toch meer capaciteit nodig blijkt te zijn?

Op pagina 15 e.v. van de memorie van toelichting staat een nadere beschrijving van de kosten. De voornaamste structurele kosten hebben betrekking op het onderhouden van de *dedicated interfaces* en de daarbij behorende verplichtingen, waaronder het voldoen aan de veiligheidseisen met betrekking tot het verlenen van toegang, zoals het toepassen van sterke cliëntauthenticatie. De *dedicated interface* moet een zeer hoge mate van beschikbaarheid hebben. Andere structurele kosten betreffen het uitvoeren van preautorisatie, waarbij een bedrag op de betaalrekening wordt gereserveerd voor een toekomstige uitgave van de kaarthouder en de betaler elke keer zijn toestemming moet geven over de hoogte van het te reserveren bedrag en waarbij de bank de reservering zo snel mogelijk weer dient te laten vervallen. Zie ook de beantwoording van vraag 120. Zoals blijkt uit de specificatie worden deze kosten zoveel mogelijk door de marktpartijen zelf gedragen.

De inschatting van de kosten van het toezicht is berekend op basis van de geraamde benodigde structurele toezichtcapaciteit. Mocht er meer capaciteit nodig zijn, dan zal er ofwel een aanvullend budget worden gevraagd, ofwel zal binnen de bestaande capaciteit de toezichtprioritering worden heroverwogen.

---

[27] Kamerstukken II 2017–18, 34 851, nr. 3, paragraaf 6.2.
[28] Kamerstukken II 2016–17, 22 112, nr. 2306.

§8. Uitvoering en handhaving

1. Toezichthouders

123) De leden van de CDA-fractie maken zich zorgen over het grote aantal toezichthouders dat betrokken is bij de handhaving van onderhavig wetsvoorstel. De regering verwijst in het licht hiervan naar afspraken die de Autoriteit Persoonsgegevens (AP) en DNB hier samen over moeten gaan maken. Deelt de regering de zorgen van de CDA-fractie dat het toezicht wel eens te versnipperd kan zijn, met een verlies van de toezicht-kwaliteit tot gevolg? Ziet de regering mogelijkheden het toezicht bij minder partijen te beleggen?

De regering begrijpt de zorgen. De handhaving is bewust toebedeeld aan de betrokken toezichthouders en volgt qua verdeling de toezichtmandaten. DNB houdt o.a. prudentieel toezicht op financiële ondernemingen, waaronder betaaldienstverleners. De AFM houdt o.a. gedragstoezicht op financiële markten. De ACM houdt toezicht op eerlijke concurrentie en consumentenbelangen. Daarnaast houdt de AP toezicht op de naleving van de Wbp (en vanaf 25 mei 2018 de AVG) bij de verwerking van persoonsgegevens ten behoeve van betaaldienstverlening. Daarnaast houdt de AP doorlopend toezicht op de naleving van het vereiste van uitdrukkelijke toestemming voor het verlenen van toegang tot persoonsgegevens voor betaaldienstverlening (artikel 94(2) PSD II). Tot slot houden DNB en de ACM toezicht op respectievelijk anti-witwasregelgeving en de Mededingingswet. Deze toezichthouders zijn elk op hun toebedeelde taken ingericht en bereiden zich momenteel voor op de implementatie van PSD II.
Het gegeven dat op één en dezelfde praktijksituatie meerdere toezichthouders op basis van verschillende wettelijke bepalingen toezicht houden leidt op voorhand niet tot een verlies van toezichtkwaliteit. Het huidige Twin Peaks model van gedrags- en prudentieel toezicht is zelfs juist om reden van vergroting van de toezichtkwaliteit in het verleden als zodanig ingericht. Het is wel zaak en zelfs verplicht op grond van artikel 26 van PSD II dat de betrokken toezichthouders bij het toezicht op de naleving van PSD II met elkaar samenwerken. Afspraken over samenwerken en mogelijkheden om informatie uit te wisselen zijn hierbij essentieel; niet alleen vanwege het vergroten van de toezichtkwaliteit, maar ook om administratieve lasten te beperken en «dubbele» handhaving of het uitblijven van handhaving te voorkomen.

124) De leden van de D66-fractie constateren dat het aantal partijen waar de toezichthouders toezicht op moeten houden zal toenemen en dat het speelveld complexer wordt. Is de regering van mening dat de toezicht-houders hiertoe voldoende geëquipeerd zijn, zowel in wettelijk mandaat als in middelen en mankracht?

De regering is van mening dat de wettelijke mandaten en de bevoegdheden van de toezichthouders op basis van de onderhavige wetgeving adequaat zijn. Om de bescherming van persoonsgegevens die nodig zijn voor het verlenen van betaaldiensten nog extra te borgen wordt middels een nota van wijziging voorgesteld het doorlopend toezicht op de naleving van de aanvullende PSD II-eis (betreffende uitdrukkelijke toestemming voor toegang tot persoonsgegevens (artikel 94(2) PSD II)) aan de AP toe te delen. Voor zover nodig hebben de toezichthouders extra middelen toebedeeld gekregen of capaciteit vrijgemaakt om de nieuwe toezichttaken uit te voeren (in het geval van de AFM). Voor een toelichting hierop per toezichthouder wordt verwezen naar het antwoord op vraag 126.

125) De leden van de GroenLinks-fractie merken op dat vanuit verschillende invalshoeken de AFM, DNB, de Autoriteit Consument en Markt (ACM) en de AP toezicht houden op de naleving van PSD II. Deze leden vragen hoe er voor wordt gezorgd dat deze samenwerking soepel verloopt? Wie is eindverantwoordelijk in het geval van een grijs gebied? Hoe schat de regering het risico in dat betrokken toezichthouders niet een heldere, afgestemde visie hebben en snel met elkaar zullen schakelen? Hoe kijkt de regering aan tegen een overkoepelende Betaalautoriteit?

Het is een gezamenlijke verantwoordelijkheid van regering en Staten-Generaal om te zorgen voor uitvoerbare en handhaafbare wetgeving. In de ontwerpfase van het wetsvoorstel is nauw overleg gevoerd met de verschillende toezichthouders. Met hun opmerkingen is rekening gehouden. De ACM heeft bovendien een formele uitvoerbaarheids- en handhaafbaarheidstoets (UHT) uitgevoerd die ik u ook heb toegezonden. Daarnaast is de wetgeving openbaar geconsulteerd. Na consultatie is opnieuw met de toezichthouders overlegd. Omdat de Minister van Financiën en de Minister voor Rechtsbescherming verantwoordelijkheid dragen voor het toezicht(kader) van de toezichthouders op de naleving van PSD II en de gegevensbeschermingsregelgeving, is het afgelopen jaar door de ministeries een aantal bijeenkomsten georganiseerd met de verschillende toezichthouders om de benodigde samenwerking tot stand te brengen. Tijdens deze bijeenkomsten zijn ook mogelijke grijze gebieden besproken en is waar mogelijk nadere uitleg verschaft over de wettekst en de richtlijn. De toezichthouders zelf hebben tevens een gezamenlijke taskforce ingesteld o.l.v. DNB die de daadwerkelijke samenwerking na implementatie voorbereidt. Alle toezichthouders hebben aangegeven hun zienswijzen op elkaar en met elkaar te willen afstemmen om mogelijke lacunes of overlap in het toezicht te voorkomen. Niet uitgesloten is dat na implementatie nog interpretatievragen opkomen die nu nog niet voorzien zijn. Dit is gebruikelijk bij nieuwe ingrijpende wetgeving. Ik heb er vertrouwen in dat zowel wetgever als toezichthouders onderling elkaar zullen blijven vinden en zie derhalve geen noodzaak voor een overkoepelende betaalautoriteit.

126) De leden van de GroenLinks-fractie vragen voorts hoe het zit met de capaciteit van alle toezichthouders? Zijn zij berekend op deze nieuwe wet? Hoeveel extra werk levert dit op per toezichthouder in fte? Worden zij hiervoor gecompenseerd?

De toezichthouders bereiden zich momenteel voor op de implementatie van PSD II. Op basis van de richtlijn en de concept-regelgeving hebben zij een inschatting gemaakt van de capaciteit die nodig is voor de taken die hieruit voortvloeien. De AFM verwacht de benodigde capaciteit vrij te kunnen maken vanuit de totale capaciteit voor het doorlopende toezicht. Het toezicht van de AFM op de naleving van PSD II heeft naar verwachting geen gevolgen voor de toezichtbegroting van de AFM. DNB breidt de capaciteit voor het toezicht op betaalinstellingen met 6 FTE uit, met name met het oog op het toezicht op de naleving van PSD II. Hierbij zijn veronderstellingen gehanteerd ten aanzien van de groei van de sector. De geschatte kosten van deze benodigde extra capaciteit ad 1,24 mln EUR worden doorberekend aan de sector. De ACM is reeds in 2017 gestart met de voorbereiding en breidt de capaciteit voor het toezicht op de naleving van PSD II uit met 1,75 FTE. De ACM wordt voor de geschatte kosten van deze benodigde extra capaciteit ad 194.500 EUR jaarlijks ten laste van de rijksbegroting gecompenseerd. De AP richt momenteel het toezicht op de naleving van PSD II in en breidt hiervoor haar capaciteit uit met 3 FTE. De AP wordt in ieder geval in eerste instantie voor de geschatte kosten van deze benodigde extra capaciteit ad 330.000 EUR jaarlijks ten laste van de rijksbegroting gecompenseerd. Om recht te doen aan het uitgangspunt

dat de kosten van toezicht aan onder toezicht gestelde instellingen worden doorberekend zal door beide ministeries in samenspraak met de AP worden onderzocht of deze en bepaalde andere kosten op termijn door de AP aan de onder toezicht staande instellingen doorberekend kunnen worden. Dit betreft niet de reguliere AVG toezichtkosten, maar (eventueel) specifieke, aan een of meerdere onder toezichtstaande instellingen toe te wijzen kosten.

127) De leden van de GroenLinks-fractie vragen voorts of de AP gebonden kan zijn aan een rechtsoordeel van DNB over de naleving van de AVG.

De AP houdt toezicht op de naleving van de nationale en Europese privacyregelgeving. Vanaf 25 mei 2018 is dat de AVG en de nationale wetgeving ter uitvoering van die verordening. Onderhavig wetsvoorstel voorziet in een bevoegdheid voor DNB en de AFM om vertrouwelijke gegevens of inlichtingen die zijn verkregen bij het uitoefenen van het toezicht op het verlenen van betaaldiensten, te verstrekken aan onder meer de Autoriteit Persoonsgegevens. Dit kan bijvoorbeeld aan de orde zijn als DNB het vermoeden heeft dat mogelijk sprake is van strijd met regelgeving op het gebied van gegevensbescherming. Aangezien de AP daarvoor de bevoegde toezichthouder is, is het aan de AP om daarover in voorkomende gevallen een oordeel te vellen en in een latere instantie aan de rechter.

128) De leden van de SP-fractie zijn verbluft door de volgende uitspraak uit de memorie van toelichting: «Naar verwachting levert dit een bijdrage aan de totstandkoming van één Europese markt voor financiële dienstverlening, waarvan zowel betaaldienstgebruikers als betaaldienstverleners profiteren.» Deze leden menen dat toezichthouders en banken unaniem zijn dat het toezicht een versnipperde bende gaat worden. De leden van de SP-fractie constateren dat burgers en bedrijven binnenkort geen raad meer weten waar een klacht te melden. De voorgenoemde leden vragen de regering duidelijk te maken welke toezichthouder aan te spreken is bij een klacht: de AP, de ACM of de AFM. Deze leden vragen de regering voor één aanspreekpunt te kiezen voor burgers, zodat zij niet ontmoedigd worden misbruik van hun gegevens aan te kaarten. Is de regering hiertoe bereid?

Als een burger een klacht heeft over een betaaldienst kan hij daarvoor in de eerste plaats terecht bij de betreffende betaaldienstverlener zelf. Deze moet de klacht te behandelen volgens de daarvoor geldende wettelijk verplichte interne klachtenprocedure.

Als een burger iets heeft gesignaleerd dat verband houdt met PSD II en dit aan een toezichthouder wil melden, moet het duidelijk zijn bij welke toezichthouder hij hiervoor terecht kan. Dit punt wordt meegenomen bij de afspraken die toezichthouders momenteel onderling maken over de operationele aspecten van het toezicht na implementatie van PSD II. Verder geldt een doorzendplicht voor de toezichthouders om verkeerd geadresseerde stukken door te zenden aan de juiste toezichthouder.

3. Uitwisseling vertrouwelijke gegevens en inlichtingen

129) De leden van de CDA-fractie vragen naar de complexiteit van het uitwisselen van gegevens tussen toezichthouders. Zij vragen of het uitwisselen van gegevens tussen toezichthouders op een veilige manier gebeurt, zeker omdat het gaat om vertrouwelijke informatie. Daarbij vragen deze leden of de toezichthoudende taken door de ACM wel op een efficiënte en effectieve manier kunnen worden toegepast, nu zij afhankelijk zijn van de gegevensaanlevering door derden. De leden van de

CDA-fractie vragen hier ook naar de tijd die mogelijk verloren gaat doordat gegevens niet rechtstreeks naar de ACM gaan maar via een andere toezichthouder. Dezelfde vragen hebben zij in relatie tot het delen van gegevens met de AP.

Het is voor een efficiënte samenwerking en een goede afstemming van het toezicht van de AFM, DNB, de ACM en de AP op de naleving van PSD II noodzakelijk dat zij vertrouwelijke informatie over het toezicht met elkaar kunnen delen. De AFM en DNB kunnen al vertrouwelijke informatie met elkaar delen. In het wetsvoorstel worden specifieke grondslagen gecreëerd voor de AFM en DNB om ook vertrouwelijke informatie, die zij hebben verkregen in het kader van het toezicht op de naleving van de PSD II, aan de ACM en de AP te verstrekken. Alle betrokken toezichthouders erkennen dat deze samenwerking van groot belang is voor de effectiviteit en de kwaliteit van het toezicht op PSD II. Zij zijn actief met elkaar in dialoog over de samenwerking na implementatie, waarbij ook gerichte aandacht bestaat voor het proces van uitwisseling van vertrouwelijke informatie, zowel voor de veiligheid van de gegevensuitwisseling als voor de effectiviteit en efficiëntie hiervan. De toezichthouders betrekken hierbij de best practice ervaringen met de gegevensuitwisseling tussen de AFM en DNB.

130) In de richtlijn is bepaald dat toezichthouders van de verschillende EU-lidstaten gezamenlijk toezicht houden op correcte naleving van de bepalingen omtrent uitwisseling van persoonsgegevens. De leden van de D66-fractie vragen of de regering kan aangeven welke stappen er ondernomen worden wanneer een dienstverlener die in een andere EU-lidstaat haar vergunning heeft verkregen niet correct omgaat met de persoonsgegevens van een Nederlandse cliënt? Zijn er volgens de regering voldoende waarborgen incorrecte omgang met persoonsgegevens te voorkomen? Is het voor de cliënt duidelijk wat hij of zij kan doen wanneer er onjuist c.q. onveilig is omgegaan met zijn of haar gegevens en wat kan deze cliënt daadwerkelijk doen?

Graag verduidelijk ik dat de wijze waarop gegevens worden verwerkt en uitgewisseld is geregeld in de Algemene Verordening Gegevensbescherming. In aanvulling hierop geeft PSD II aanvullende bescherming. Zo bepaalt artikel 94 (2) van PSD II dat de consument uitdrukkelijke toestemming moet geven voor de verwerking van persoonsgegevens die nodig zijn om de betaaldienst te verlenen. De Autoriteit Persoonsgegevens houdt na vergunningverlening doorlopend toezicht op de naleving van dit vereiste. De Autoriteit Persoonsgegevens is bovendien bevoegd om erop toe te zien dat de wijze van gegevensverwerking voldoet aan de eisen die de Algemene Verordening Gegevensbescherming stelt. De AP ziet er, met andere woorden, onder meer op toe dat er een deugdelijke grondslag is op grond waarvan gegevens worden verwerkt én dat is voldaan aan de eis van uitdrukkelijke toestemming van artikel 94(2).

Ik meen dat met het kader van de AVG en de aanvullende bescherming die PSD II biedt er voldoende wettelijke waarborgen zijn voor naleving van de regels omtrent gegevensuitwisseling. Ik heb er bovendien vertrouwen in dat de AP zowel het toestemmingsvereiste van artikel 94(2) als de eisen ten aanzien van gegevensverwerking onder de AVG effectief zal handhaven. Als een betaaldienstgebruiker een vermoeden heeft dat er sprake is van onveilige gegevensverwerking dan is er mogelijk sprake van overtreding van het principe van passende beveiliging van persoonsgegevens (artikel 5 lid 1 onder f van de AVG). De betaaldienstgebruiker kan hiertoe een klacht indienen bij de AP. Op grond van de AVG is de AP gehouden om op deze klacht te reageren (artikel 77 AVG).

§10. Advies Autoriteit Persoonsgegevens

131) De leden van de VVD-fractie vragen of de regering nader kan ingaan op het advies van de AP. Wat zijn de consequenties van deze wet voor de privacy en de bescherming van de persoonsgegevens? Houdt de AP ook na wijziging het advies om het wetsvoorstel aldus niet in te dienen staande of waren de wijzigingen in de wet afdoende voor een nieuw oordeel?

De Autoriteit Persoonsgegevens heeft destijds negatief geadviseerd, omdat volgens de Autoriteit de Algemene Verordening Gegevensbescherming voorrang heeft op de richtlijn PSD II en de Autoriteit Persoonsgegevens bovendien in de aan de AP voorgelegde conceptversie nog niet als toezichthouder was aangewezen op de bepaling van PSD II die bepaalt dat voor de verwerking van persoonsgegevens voor het verlenen van betaaldiensten «uitdrukkelijke toestemming» vereist is (artikel 94 (2) PSD II).

In de memorie van toelichting ben ik ingegaan op het advies van de Autoriteit Persoonsgegevens. In de toelichting heb ik onder meer aangegeven dat, anders dan de AP adviseert, de verhouding tussen de AVG en PSD II moet worden bepaald aan de hand van uitleg van beide instrumenten. Zoals blijkt uit de antwoorden die de Europese Commissie heeft gegeven, is PSD II ten opzichte van de AVG een bijzondere wet, die met de introductie van de extra toestemmingseis aanvullende bescherming beoogt te bieden wanneer bij het verlenen van betaaldiensten persoonsgegevens worden verwerkt. Voor het verwerken van persoonsgegevens ten behoeve van het verlenen van betaaldiensten moet zowel aan het toestemmingsvereiste van artikel 94(2) PSD II als aan de eisen uit de AVG worden voldaan. De genoemde eis van uitdrukkelijke toestemming uit PSD II is volgens de Commissie niet dezelfde als de toestemming als verwerkingsgrondslag in de zin van de AVG. Bij de toepassing van artikel 94 (2) PSD II moet volgens de Commissie om uitdrukkelijke toestemming worden gevraagd aan de gebruiker, op basis van informatie van de betaaldienstverlener over welke gegevens voor de uitvoering van de overeenkomst worden verwerkt. Er zijn verder geen vormvereisten gesteld. De grondslag voor verwerking van persoonsgegevens voor het verlenen van betaaldiensten is (veelal) de overeenkomst (artikel 6(1), onderdeel b, AVG). Het in artikel 94(2) PSD II gestelde vereiste van uitdrukkelijke toestemming vormt daarop een aanvullend vereiste en is dus niet aan te merken als grondslag voor de verwerking van de gegevens zelf (artikel 6, eerste lid, onderdeel a, AVG). Voor de vorm die dit vereiste in de praktijk kan hebben wordt verwezen naar de beantwoording van vraag 82.

Omdat dit toestemmingsvereiste een PSD II-vereiste is, was dit in het aan de AP voorgelegde concept vormgegeven als een prudentieel vereiste en is het toezicht daarop aan DNB toegedeeld. Aangezien dit toestemmingsvereiste echter in het verlengde ligt van de AVG en voor de invulling daarvan waar mogelijk kan worden aangesloten bij de eisen die de AVG stelt ten aanzien van het verlenen van toestemming, is het bij nader inzien wenselijk om het toezicht op dit vereiste toe te delen aan de AP. Daartoe wordt middels een nota van wijziging voorgesteld om de AP doorlopend toezicht te laten houden op de naleving van dit vereiste. Over de praktische uitvoering hiervan dienen samenwerkingsafspraken te worden gemaakt tussen DNB en de AP, zodat het toezicht van DNB en van de AP goed op elkaar is afgestemd. Naast de bescherming die artikel 94 (2) PSD II biedt, is zoals gezegd ook de AVG van toepassing. De Autoriteit Persoonsgegevens is en blijft bevoegd om op de naleving van de AVG toe te zien.

Ik deel het gevoelen van de AP dat het wenselijk is dat over de verhouding tussen de AVG en PSD II in Europees verband meer duidelijkheid komt. Ik erken dat het verwarrend werkt dat een term als «(uitdrukkelijke) toestemming» in PSD II en de AVG op verschillende wijze lijken te worden uitgelegd. De mogelijkheden om hier als lidstaat zelf duidelijkheid te scheppen zijn zeer beperkt, doordat de uitleg van zowel de richtlijn PSD II als de AVG is voorbehouden aan de toezichthouder, de rechter en uiteindelijk het Hof van Justitie. Ik zal binnen de mij ten dienste staande mogelijkheden aandacht blijven vragen voor meer coherentie en duidelijkheid, onder meer in zogenaamde implementatiewerkgroepen die met enige regelmaat door de Europese Commissie worden georganiseerd. Daarbij betrek ik ook de AP.

132) De leden van de fractie van het CDA vragen of de regering een reactie kan geven op alle punten die de AP naar voren brengt in haar brief van 27 november 2017 aan de Tweede Kamer met afschrift aan de Minister van Financiën.

Op de drie in de brief van de AP van 27 november 2017 genoemde onderwerpen ben ik reeds ingegaan bij de beantwoording van vraag 131.

133) De leden van de D66-fractie lezen dat de AP stelt onvoldoende wettelijke middelen te hebben gekregen voor toezicht op de vraag of aanbieders alleen na uitdrukkelijke toestemming toegang krijgen tot alleen de noodzakelijke persoonsgegevens. Kan de regering aangeven waarom deze bevoegdheid niet direct en wettelijk verankerd bij de AP is neergelegd?

Voor de beantwoording van deze vraag verwijs ik naar het antwoord op vraag 131.

134) De leden van de GroenLinks-fractie vragen in hoeverre de regering bij het plannen van de voorbereiding van de wetgeving rekening heeft gehouden met het vragen en verwerken van een advies van de AP.

In beginsel wordt over het ontwerp van een implementatieregeling geen advies gevraagd.[29] Een reden om hiervan af te wijken is slechts als het vragen van advies noodzakelijk is voor een zorgvuldige voorbereiding van de regeling. Dit kan bijvoorbeeld het geval zijn als de te implementeren bindende Europese regeling wezenlijke beleidskeuzen openlaat. Aangezien de bepaling in PSD II die betrekking heeft op de verwerking van persoonsgegevens een specifiek PSD II vereiste is en daarop geen lidstaatopties van toepassing zijn, is in eerste instantie in de planning van het wetsvoorstel geen rekening gehouden met het vragen van advies aan de AP.

135) De AP heeft in haar brief van 27 november 2017 aandacht gevraagd voor drie aspecten uit het wetsvoorstel die zij noodzakelijk acht ter bescherming van de persoonsgegevens en de persoonlijke levenssfeer van burgers, alsmede om rechtszekerheid te bieden. De leden van de PvdD-fractie vragen de regering uitgebreid te reageren op deze brief en daarbij aan te geven of zij bereid is de aanbevelingen over te nemen. Indien de regering de aanbevelingen niet wil overnemen, waarom niet?

Voor het antwoord op deze vraag verwijs ik naar het antwoord op vraag 131.

---

[29] Artikel 1:7, eerste lid, Algemene wet bestuursrecht en aanwijzing 342, tweede lid, Aanwijzingen voor de regelgeving.

Overig

136) De leden van de VVD-fractie hebben nog enkele andere vragen. Hoe wordt omgegaan met de nieuwe mogelijkheden die digitale transacties bieden om geld wit te wassen en welke maatregelen worden er, in deze implementatiewet of in andere wetten, genomen om dit risico op witwassen tegen te gaan?

Op grond van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) dienen banken, andere financiële ondernemingen en diverse aangewezen beroepsgroepen reeds onderzoek te verrichten naar hun cliënten en ongebruikelijke transacties te melden bij de Financiële inlichtingen eenheid Nederland (FIU-Nederland). Deze verplichtingen vloeien voort uit de Europese anti-witwasrichtlijnen[30]. Aangezien deze verplichtingen ook van toepassing zijn op betaaldienstverleners en daarmee ook op aanbieders van de in PSD II geïntroduceerde nieuwe betaaldiensten, hoeven deze verplichtingen niet nog afzonderlijk geregeld te worden in de wetgeving ter implementatie van PSD II. De toezichthouders bereiden zich momenteel voor op het toezicht op de naleving van genoemde verplichtingen.

137) De leden van de VVD-fractie vragen op welk moment de regering verwacht dat deze wet in werking kan treden? Hoe wordt omgegaan met de consequenties van de verwachte vertraagde invoering? Wat zijn de consequenties van deze vertraging voor de concurrentiepositie van Nederlandse dienstenaanbieders en de bescherming van consumenten? Kan hierbij ook ingegaan worden op de berichten van Pricewaterhouse-Coopers dat slechts 9% van de banken op dit moment is voorbereid op de inwerkingtreding van PSD II?

In de brief van 23 oktober 2017 aan de Tweede Kamer is vermeld dat de wetgeving ter implementatie van PSD II naar verwachting in het voorjaar van 2018 in werking kan treden. In deze brief is tevens ingegaan op de mogelijke consequenties van de vertraagde invoering. Inmiddels moet deze verwachting worden bijgesteld naar najaar 2018. Zoals in de brief van 9 april 2018 aan de Tweede Kamer is vermeld heeft met name de precieze verdeling van het toezicht tussen de AP en DNB op de verwerking van persoonsgegevens voor het verlenen van betaaldiensten de nodige afstemming en tijd gevergd.

Voor zover kan worden nagegaan is het bericht dat slechts 9% van de banken op dit moment is voorbereid op de inwerkingtreding van PSD II afkomstig uit een rapport van PWC en gebaseerd op een enquête, uitgevoerd in de eerste helft van 2017.[31] Daarin staat op p. 2 onder meer dat 9% van de Europese banken zich toen in de implementatiefase bevond. Banken in Nederland bereiden zich momenteel voor op de inwerkingtreding van de PSD II-wetgeving. Hoe ver individuele banken daarmee precies zijn is mij niet bekend. Ik heb tot nu toe geen signalen ontvangen dat banken niet tijdig klaar zouden zijn met de voorbereiding op PSD II.

---

[30] Meest recent richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie (PbEU 2015, L 141) (de vierde anti-witwasrichtlijn). De vierde anti-witwasrichtlijn wordt op dit moment in de Wwft geïmplementeerd (Kamerstukken II, 2017–2018, 34 808, nr. 2).

[31] https://www.pwc.nl/nl/themas/blogs/psd2-stimuleert-slimme-authenticatiemethoden-banken.html

138) Kan de regering ingaan op de relatie tussen deze implementatiewet en het stimuleren van innovatie in de financiële sector, zo vragen de leden van de VVD-fractie. Wordt met deze wet voldoende ruimte gelaten voor de sector om te innoveren?

Het stimuleren en faciliteren van innovatie in de financiële sector is een belangrijke doelstelling van PSD II. Het wetsvoorstel ter implementatie van PSD II creëert hiervoor ruimte door het reguleren van nieuwe betaaldiensten, te weten betaalinitiatiediensten en rekeninginformatiediensten. De regulering van deze type diensten – die werken op basis van toegang tot iemands rekening – kan leiden tot nieuwe klantgerichte en innovatieve oplossingen, zoals nieuwe betaalmogelijkheden of digitale huishoudboekjes. In het algemeen geldt dat bij de totstandkoming van PSD II is gezocht naar een manier om innovatie van de betaaldienstverlening te stimuleren binnen de kaders van eisen die gelden op het gebied van veiligheid van het gebruik van betaaldiensten en consumentenbescherming. Mochten marktpartijen onnodige knelpunten ervaren dan zullen zij dit naar verwachting rechtstreeks dan wel via de toezichthouders aan de Minister van Financiën kenbaar maken. Toezichthouders AFM en DNB hebben hiervoor sinds enige tijd de zogenaamde *Innovation Hub* en het programma *Maatwerk voor Innovatie* ingericht. Binnen de *Innovation Hub* kunnen marktpartijen op een laagdrempelige wijze vragen stellen over financiële innovatie en regulering. Binnen de aanpak van Maatwerk voor Innovatie wordt bij het beoordelen en toelaten van nieuwe innovatieve dienstverlening onderzocht welke ruimte wet- en regelgeving biedt bij de toepassing van regels. Mochten de ervaringen in de *Innovation Hub* of *Maatwerk voor Innovatie* aanleiding geven tot een behoefte aan aanpassing van wet- en regelgeving, dan zullen de AFM en DNB dit aan de Minister van Financiën kenbaar maken. De regering is hierdoor van mening dat voldoende ruimte is gelaten aan marktpartijen voor innovatie.

139) De leden van de VVD-fractie constateren dat in Nederland volgens de ECB relatief het meest met een betaalkaart wordt betaald. Deze leden vragen of dit nog effect heeft, en zo ja, welk effect heeft dit, op Nederlandse consumenten en aanbieders van producten? Hoe wordt voorkomen dat zij een concurrentienadeel ondervinden, zo vragen de voorgenoemde leden.

De PSD II regels hebben betrekking op debetkaarten, de meeste creditcards en op andere betaalinstrumenten. Alle partijen die in Nederland en in andere Europese landen actief zijn op het gebied van betaaldienstverlening, moeten zich aan deze regels houden. Er is daarom geen aanleiding te veronderstellen dat een verschil in populariteit in het gebruik van debetkaarten ten opzichte van andere betaalinstrumenten tussen de Europese landen tot een concurrentienadeel voor Nederlandse aanbieders van betaalproducten of voor Nederlandse consumenten zal leiden.

140) De leden van de GroenLinks-fractie vragen hoe de regering aankijkt tegen het voorstel van hoogleraar Bart Jacobs om op zijn minst wederkerigheid te eisen, waarbij ook de (Amerikaanse) ICT-sector wordt gedwongen om haar kostbare gegevens gratis aan andere bedrijven beschikbaar te stellen, uiteraard slechts na toestemming van de betrokkene?

Bijgaand wetsvoorstel voorziet in implementatie van de richtlijn. Het is staand kabinetsbeleid om richtlijnen beleidsarm, zonder nationale koppen, om te zetten, om onnodige vertraging te voorkomen. Bovendien is het onzeker of de eis van wederkerigheid is toegestaan onder de richtlijn PSD II en de AVG, nog los van de vraag of aan een dergelijke optie in de praktijk behoefte bestaat.

141) De leden van de GroenLinks-fractie vragen hoe de regering aankijkt tegen het principe van «differential pricing», waarbij de prijs afhankelijk wordt gemaakt van de persoonlijke omstandigheden van de mogelijke koper? Deelt de regering de analyse van hoogleraar Bart Jacobs dat PSD II het makkelijker maakt om differential pricing mogelijk te maken voor bedrijven als Google?

PSD II verruimt de mogelijkheden voor een bedrijf tot het verzamelen van betaaldata van een consument, mits de consument toestemming geeft aan het bedrijf. Met deze data kan een bedrijf een beter beeld van de betalingsbereidheid van de consument maken. Er kan dus ook makkelijker een gepersonaliseerde prijs berekend worden.

Ik heb geen aanwijzingen dat gepersonaliseerde prijzen vaak voorkomen. Dit neemt niet weg dat het technologisch gezien mogelijk is om prijzen aan te passen op basis van persoonlijke (zoek)gegevens. In algemene zin kan niet vastgesteld worden of de opkomst van gepersonaliseerde prijzen goed dan wel slecht is voor de consumentenwelvaart. Dit zal mede afhangen van de mate van personalisering. Voor consumenten met een relatief lage betalingsbereidheid zal een gepersonaliseerde prijs dan lager zijn dan in de huidige situatie. Dit zou ertoe kunnen leiden dat deze consumenten een product dat zij in de huidige situatie niet zouden kopen, dan wel kopen. Voor consumenten met een hogere betalingsbereidheid zal een gepersonaliseerde prijs hoger uitvallen dan in de huidige situatie. Bij voldoende concurrentie in de markt kunnen deze consumenten echter een alternatief zoeken, waardoor het niet noodzakelijk is dat zij ook meer gaan betalen.

142) Hoe kijkt de regering aan tegen de analyse van hoogleraar Jaap Koelewijn, waarin hij aangeeft dat de klant dreigt te worden ingebed in een wereld waarin hij zijn autonomie kwijtraakt? De leden van de GroenLinks-fractie vernemen graag het antwoord van de regering

Onder invloed van technologische ontwikkelingen wordt het verwerken en analyseren van grote hoeveelheden persoonsgegevens – big data analyse – steeds belangrijker en eenvoudiger. Ook in het kader van de verlening van betaaldiensten, met name rekeninginformatiediensten, kan sprake zijn van verwerking van grote hoeveelheden persoonsgegevens, aan de hand waarvan allerlei analyses gedaan kunnen worden en profielen opgesteld kunnen worden voor zowel commerciële doelen als risico-inschatting en mogelijk nog andere doelen. De regering begrijpt dat hierover zorgen bestaan in de samenleving, met name waar het gaat om bescherming van persoonsgegevens. Tegelijkertijd zijn er ook ontwikkelingen die aan deze zorgen tegemoet komen en die ertoe strekken de autonomie van de burger op dit punt te versterken. Gewezen wordt daarbij op de nieuwe Europese gegevensbeschermingsregelgeving, vanaf 25 mei 2018 in de vorm van de AVG, en de daarop betrekking hebbende uitvoeringsregelgeving. In de AVG zijn de rechten van burgers versterkt en zijn de daarmee samenhangende verplichtingen van de verwerkingsverantwoordelijken strenger geworden. Dit draagt bij aan het versterken van de autonomie van burgers waar het gaat om de verwerking van hun persoonsgegevens.

143) De leden van de GroenLinks-fractie vragen tot slot of de regering een reactie kan geven op de gestelde vragen van seniorenorganisaties KBO-PCOB, NVOG en NOOM, voor zover deze nog niet aan de orde zijn gekomen in dit verslag.

Een aantal vragen van genoemde seniorenorganisaties zijn hiervoor nog niet beantwoord. In de eerste plaats betreft dat de vraag of het is aan te bevelen om de manier waarop data gebruikt en gedeeld worden een verplicht onderdeel te laten zijn van de accountantscontrole bij alle instellingen in de betaalketen. In Nederland is de Autoriteit Persoonsgegevens belast met het toezicht op de naleving van de eisen met betrekking tot het gebruiken en delen van persoonsgegevens. Dat geldt ook voor persoonsgegevens die worden verwerkt in het kader van betaaldienstverlening. De AP ziet er daarbij op toe dat persoonsgegevens worden verwerkt in overeenstemming met de regels die de AVG op dat gebied stelt. Het is de regering niet bekend dat daarnaast behoefte zou bestaan aan een verplichte toetsing van de wijze van gegevensverwerking door betaalinstellingen in het kader van de accountantscontrole, nog afgezien van de vraag of dit juridisch mogelijk is.

Verder is een aantal vragen gesteld over «screen scraping». Zo vragen genoemde seniorenorganisaties of de beschermingsmaatregelen waar partijen zich aan hebben te houden afdoende zijn en wat er gebeurt als partijen gehackt worden. Ten aanzien van de vraag of de beschermingsmaatregelen binnen PSDII voor kwetsbare groepen voldoende zijn en in hoeverre additionele beschermingsmaatregelen mogelijk zijn, wordt opgemerkt dat het MOB inmiddels heeft aangegeven graag te zien als banken consumenten in mobiel bankieren apps en bij internetbankieren een overzicht bieden van de dienstverleners waaraan toestemming is verleend voor rekeninginformatiediensten.

Ook willen zij weten of het uitgesloten is dat er geld van de rekening wordt gehaald zonder toestemming van de rekeninghouder. Voor het antwoord op deze vraag wordt verwezen naar de beantwoording van vraag 82.

Verder vragen genoemde seniorenorganisaties zich af of adequate informatie die iedereen begrijpt mogelijk is; niet alleen voor alle consumenten, maar zeker ook voor ouderen en kwetsbare groepen in de samenleving. Al decennia worden consumenten niet alleen door de banken, maar ook door maatschappelijke organisaties als de seniorenorganisaties en de Consumentenbond erop gewezen om pincode en/of inloggegevens nooit aan een derde ter beschikking te stellen. In de perceptie van consumenten gaat dit volgens deze organisaties nu wel gebeuren. Zij vragen wat voor effect dit zal hebben op het vertrouwen van de consument in het betalingsverkeer en of meer concurrentie op het gebied van het betalingsverkeer belangrijker is dan privacy en bescherming van klantgegevens.

Op korte termijn komt het Maatschappelijk Overleg Betalingsverkeer (MOB) met een voorlichting over PSD II die speciaal bedoeld is voor onder meer consumenten. Doel daarvan is om op een voor iedereen begrijpelijke wijze uit te leggen wat PSD II inhoudt, wat de mogelijkheden zijn en ook welke risico's er zijn. Daarin zal met name ook informatie worden gegeven over de verstrekking van beveiligingsgegevens voor het verlenen van toegang tot de betaalrekening. Daarbij is en blijft het zo dat geen pincode verstrekt mag worden aan derden.

De Minister van Financiën,
W.B. Hoekstra