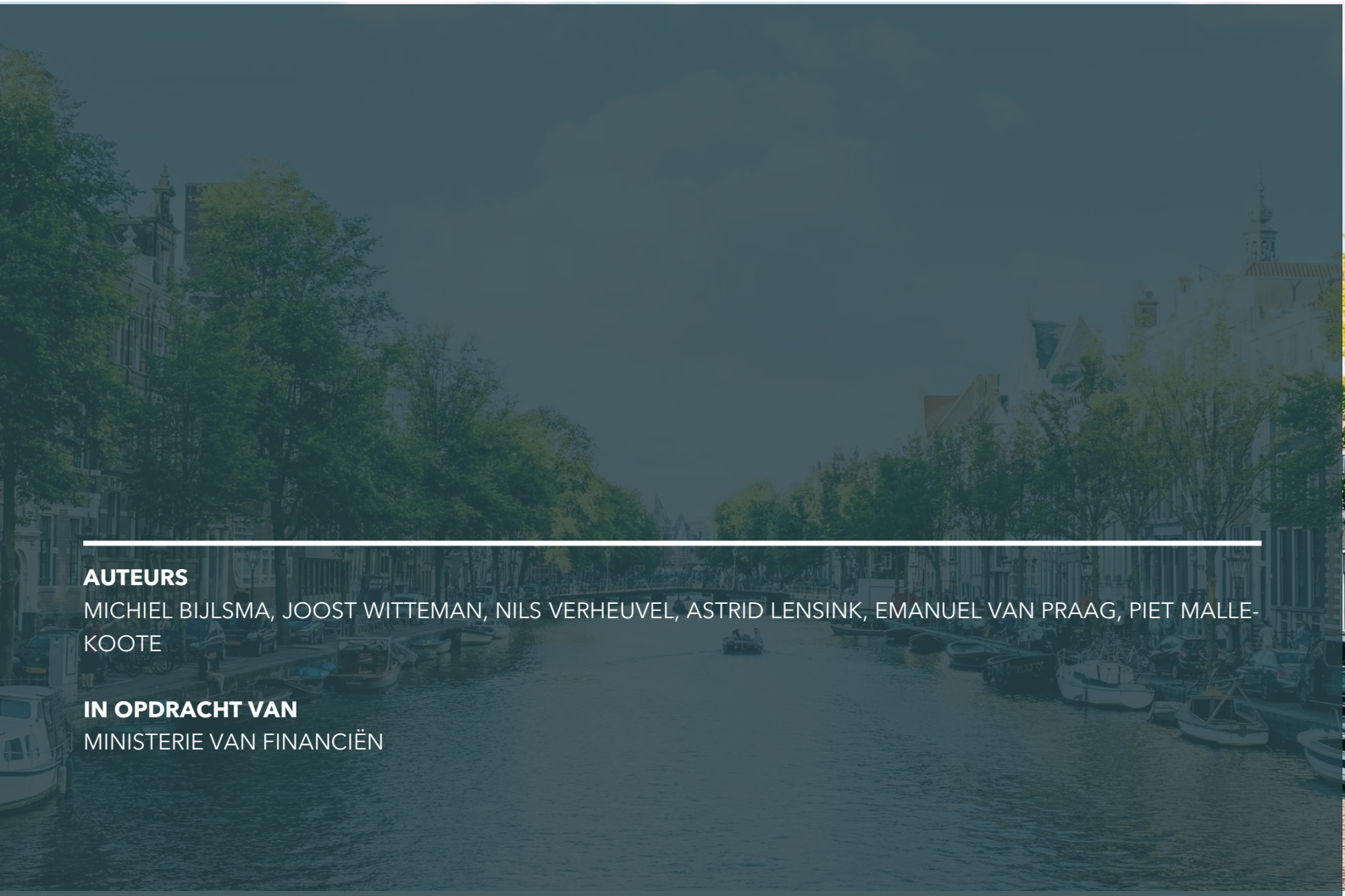
EVALUATIE PSD2

DE HERZIENE EUROPESE RICHTLIJN BETAALDIENSTEN

RAPPORT

seo • economisch onderzoek



AUTEURS
MICHIEL BIJLSMA, JOOST WITTEMAN, NILS VERHEUVEL, ASTRID LENSINK, EMANUEL VAN PRAAG, PIET MALLEKOOTE

IN OPDRACHT VAN
MINISTERIE VAN FINANCIËN

Samenvatting

PSD2 draagt bij aan meer concurrentie op de markt voor betaaldiensten en aan een gelijker speelveld tussen aanbieders. Het gebruik van PSD2-diensten is echter nog beperkt. PSD2 bevat adequate waarborgen voor gegevensbescherming. Wel zijn er enkele aandachtspunten voor de wetgever en toezichthouders.

PSD2

De herziene Europese richtlijn betaaldiensten (PSD2) verbreedt de reikwijdte van de regulering en het toezicht, qua type diensten en geografische reikwijdte. PSD2 introduceert de regulering van betaalinitiatie- en rekeninginformatiediensten en het veilig verlenen van toegang tot betaalrekeningen door derde partijen als een consument daarom verzoekt. De kerndoelstelling van PSD2 is dat banken gegevens van betaalrekeningen veilig met andere dienstverleners kunnen delen. Dit dient een gelijk speelveld tussen enerzijds banken en vergunninghoudende derde partijen en anderzijds tussen vergunninghoudende derde partijen onderling te bevorderen. PSD2 is in februari 2019 in Nederland ingevoerd. Nederland was hierin later dan andere landen. PSD2 moest officieel per januari 2018 in nationale wetgeving geïmplementeerd zijn.

De doelstellingen van PSD2 zijn:

1. Het versterken van een interne markt voor kaartbetalingen, internetbetalingen en mobiele betalingen;
2. Het stimuleren en faciliteren van innovaties;
3. Het verhelpen van gesignaleerde problemen van PSD1, zoals het gebruik van achterhaalde of vage begrippen.

Deze evaluatie, die SEO Economisch Onderzoek uitvoert in opdracht van het ministerie van Financiën, toetst in hoeverre PSD2 doeltreffend en doelmatig is geweest bij het bereiken van deze doelstellingen in Nederland. Daarbij kijkt deze evaluatie niet alleen of bovenstaande doelen zijn bereikt, maar ook in hoeverre PSD2 daar daadwerkelijk aan heeft bijgedragen. Bij deze evaluatie is gebruikgemaakt van beschikbare literatuur, een analyse van het register van de Europese Banken Autoriteit (EBA), een enquête onder consumenten en interviews met stakeholders en experts. Het onderzoeksteam heeft ook Piet Mallekoote en Emanuel van Praag als experts geraadpleegd. Piet Mallekoote heeft daarbij geadviseerd over de aspecten rond de invoering van PSD2. Emanuel van Praag heeft zich vooral gericht op de juridische aspecten. De inhoudelijke verantwoordelijkheid voor het rapport ligt volledig bij SEO Economisch Onderzoek.

Voor dit onderzoek zijn de doelstellingen onderverdeeld in de volgende vijf pijlers:

1. Het bevorderen van de concurrentie;
2. Het stimuleren en faciliteren van innovaties in het betalingsverkeer;
3. Het vergroten van de veiligheid van betalingsverkeer;
4. De bescherming van de deelnemers aan het betalingsverkeer;
5. Het bijdragen aan één Europese betaalmarkt.

Effecten van PSD2 op markt voor betaaldiensten

Concurrentie

PSD2 heeft ervoor gezorgd dat aanbieders van betaalinitiatiediensten en rekeninginformatiediensten zijn gereguleerd. De concurrentie op deze markt is toegenomen, er zijn meer partijen actief en die zijn minder afhankelijk van

banken voor toegang tot betaalgegevens dan voor de invoering van PSD2. Met PSD2 kunnen vergunninghoudende partijen, na toestemming van de rekeninghouder, gegevens van de betaalrekening gebruiken voor betaalinitiatie- of rekeninginformatiediensten. Voor PSD2 waren aanbieders van deze diensten afhankelijk van onderlinge afspraken met banken.

De producten die aanbieders leveren zijn vaak niet nieuw, maar zijn met PSD2 op een andere manier vormgegeven. De producten richten zich met name op de zakelijke markt, bijvoorbeeld met boekhoudpakketten. Hoewel dergelijke boekhoudpakketten al bestonden voor PSD2 is er op deze markt meer concurrentie tussen aanbieders ontstaan door PSD2. Het gebruik van PSD2-diensten op de consumentenmarkt is nog beperkt. De reden hiervoor is dat iDEAL al een sterke positie heeft bij consumenten en het voor nieuwe diensten lastig is hiermee te concurreren. Ook zijn consumenten redelijk onbekend met deze diensten. Daarnaast zijn consumenten terughoudend als het gaat om het delen van betaalgegevens. De markt bevindt zich nog in een vroeg stadium, de komende jaren kan er nog veel veranderen qua productaanbod en aanbieders.

Innovatie

De belangrijkste innovatie van PSD2 is dat aanbieders bestaande diensten op een andere manier aanbieden en dat het gebruik van *application programming interfaces* (API's) heeft geleid tot een efficiëntere en betere dienstverlening. Op de consumentenmarkt zijn er een aantal productinnovaties geweest, maar het gebruik daarvan is nog beperkt.

Een andere innovatie is de opkomst van tussenpartijen die fricties in de betaalketen verminderen, zogeheten *aggregators*. Een gebrek aan standaardisering van API's leidt ertoe dat het voor individuele (potentiële) aanbieders kostbaar is om een dekkend netwerk van API-koppelingen met alle banken te ontwerpen, in het bijzonder wanneer de aanbieder internationaal wil opereren. Daar komt bij dat aan een PSD2-vergunning compliancekosten verbonden zijn. *Aggregators* richten zich op het ontwerpen en bijhouden van API-koppelingen. Zij leveren dan data aan aanbieders die daarmee hun dienst leveren.

Veiligheid

PSD2 heeft de veiligheid van de betaalmarkt vergroot. Met API-interfaces zijn er minder veiligheidsrisico's bij het verzamelen van gegevens dan bij het verzamelen van gegevens middels screenscraping, zoals voor PSD2 de praktijk was. Daarnaast zijn de aanbieders actief middels een vergunningenstelsel, waar eisen worden gesteld aan de aanbieder. Dit biedt een waarborg dat niet elke partij toegang tot betaalgegevens kan verkrijgen. Ook is er doorlopend toezicht of de dienstverleners aan de eisen inzake veiligheid voldoen.

PSD2 heeft ook marktbreed *strong customer authentication* (SCA) ingevoerd. Het effect van deze eis op de veiligheid is in Nederland beperkt, omdat reeds vóór PSD2 SCA veel werd toegepast, bijvoorbeeld bij iDEAL-betalingen. Wel is er een verbetering bij enkele inlogprocedures en bij creditcardbetalingen doorgevoerd, maar het aandeel creditcardbetalingen is klein in Nederland. Daarnaast heeft de invoering van SCA niet tegen alle fraude kunnen beschermen, omdat de fraudeurs op basis van misleiding en verleiding klanten overhalen om ze, met SCA, toegang tot de betaalrekening te verschaffen. Tegen *spoofing* of *phishing* bieden PSD2 en SCA geen bescherming, omdat hier mensen verleid worden zelf geld naar criminelen over te maken, dat kan niet met behulp van technische regelgeving voorkomen worden.

Bescherming van deelnemers aan betalingsverkeer

PSD2 heeft geleid tot een betere bescherming van deelnemers aan het betalingsverkeer en is ook adequaat in deze bescherming. De technische waarborgen als SCA en de vergunningseisen voor aanbieders helpen om risico's voor

de consumenten wat betreft betalingen te beperken en de veiligheid van het betalingsverkeer te vergroten. De regels voor onbedoelde en niet-toegestane overboekingen leggen de verantwoordelijkheid voor het terugbetalen bij de betaaldienstverlener. Consumenten lopen daardoor geen risico. Bij aanvang was er vrees dat kwetsbare groepen zoals ouderen en visueel beperkten last zouden ondervinden van PSD2, maar die vrees is geen werkelijkheid geworden. De belangrijkste reden is dat deze groepen geen PSD2-gerelateerde diensten gebruiken.

Bijdragen aan één Europese betaalmarkt

PSD2 draagt bij aan één Europese betaalmarkt door één Europees regime voor nieuwe, voorheen niet gereguleerde, betaaldiensten te creëren. Een PSD2-vergunning is in heel de EU inzetbaar middels *passporting*. Een groeiend aantal aanbieders maakt hier gebruik van. Op sommige aspecten is meer harmonisatie haalbaar, zoals bij het vergunningsverleningsproces en het toezichtsregime, waarbij marktpartijen verschillen tussen lidstaten opmerken.

Waarborgen gegevensbescherming

PSD2 heeft tot doel om betaalgegevens, met uitdrukkelijke instemming van de consument, beschikbaar te maken aan derde partijen. Door de toename in de datastromen van persoonsgegevens kunnen risico's voor privacy toenemen, maar PSD2 en de Algemene Verordening Gegevensbescherming (AVG) bieden gezamenlijk een adequate waarborg voor gegevensbescherming. De Nederlandsche Bank (DNB) toetst bij de aanvraag van de vergunning de bedrijfsvoering, ook gerelateerd aan gegevensbescherming. De Autoriteit Persoonsgegevens (AP) toetst achteraf of PSD2-vergunninghouders de AVG naleven. Deze evaluatie heeft geen zicht op de vraag of de partijen de eisen van PSD2 en AVG daadwerkelijk naleven, maar de wettelijke waarborgen zijn in principe voldoende om een zorgvuldige omgang met betaalgegevens te borgen.

Door de langer wordende betaaltekens en de opkomst van *aggregators*, vallen sommige partijen die wel werken met betaalgegevens niet onder het toezicht van PSD2. Dat betekent dat voor dergelijke partijen alleen AVG-toezicht en de contractuele overeenkomsten met PSD2-vergunninghoudende partijen het gebruik van betaalgegevens reguleren. Het gebrek aan zicht op het feitelijke gebruik van betaaldata door deze partijen is een risico omdat het ex ante toezicht en doorlopende toetsen die DNB doet bij partijen die wel onder toezicht staan ontbreken. Het toezicht door de AP is op meer afstand en ex post. Dat is ook niet vreemd gezien de beperkte omvang en het brede werkveld van de AP.

Aandachtspunten

1. PSD2 biedt geen uniforme standaard voor API's, hoewel enige mate van standaardisering plaatsvond via de RTS van EBA en werk binnen de Berlin Group. Het gebrek aan standaardisering van API's had tot gevolg dat banken verschillende API's hebben ontwikkeld, wat de implementatiekosten heeft verhoogd. Ook maakte dit het lastiger voor aanbieders om dekkende koppelingen aan te bieden. Een standaard voor API's had ook een belangrijke bijdrage kunnen leveren aan helderheid voor de markt over hoe de eisen van de AVG en de PSD2 met elkaar te verenigen. Het ontwikkelen van een uniforme standaard kan ook nu nog voordelen hebben omdat het leidt tot snellere acceptatie in de markt, minder discussie met de toezichthouder en minder discussie tussen banken en betaaldienstverleners.
2. PSD2 mandateert gratis toegang tot de betaalinfrastructuur van banken, indien klanten daar toestemming voor geven. Dit vermindert aan de marge de prikkel voor banken om te investeren in die infrastructuur, zeker op het moment dat een steeds groter deel van de baten die de infrastructuur genereert 'weglekken' naar niet-bancaire aanbieders. Het effect hiervan is in Nederland nog beperkt, vanwege het beperkte gebruik. Vanuit concurrentie- en innovatieoogpunt is de keuze voor gratis toegang op dit moment te rechtvaardigen, maar naarmate het gebruik van PSD2-diensten toeneemt, wordt het belangrijker oog te hebben voor dit nadeel.

3. Het verbod op *surcharging* is voor consumenten voordelig omdat zij niet voor alle betaalproducten de werkelijke kosten dragen, hoewel consumenten uiteindelijk indirect de kosten van betalen dragen. Voor het betaalsysteem kan dit nadelige gevolgen hebben als dit de mogelijkheid wegneemt om consumenten te prikkelen efficiënte betaalproducten te gebruiken. Dit kan er volgens gesprekspartners toe leiden dat relatief dure betaalmethoden algemeen gangbaar worden.
4. Een aanzienlijk deel van de gesproken partijen vindt de samenhang tussen de AVG en PSD2 onduidelijk, hoewel er met de EDPB-*guidelines* een belangrijke stap is genomen. Deze vermeende onduidelijkheid hoeft niet noodzakelijkerwijs overeen te komen met de toezichtrechtelijke realiteit die verantwoordelijkheden juridisch regelt. Het is echter is wel een signaal dat toezichthouders beter met elkaar en de buitenwereld kunnen communiceren over deze samenhang. Een groot deel van de gesprekspartners geeft dan ook aan dat ze behoefte hebben aan praktische *guidance* in specifieke gevallen, zoals het vormgeven van dataminimalisatie in de API-interface.
5. Door langer wordende betaalketens en de opkomst van *aggregators* vallen sommige partijen die wel werken met betaaldata niet onder toezicht van PSD2. Dat betekent dat voor dergelijke partijen alleen het algemene AVG-toezicht en de contractuele overeenkomsten met partijen die wel onder toezicht staan het gebruik van betaalgegevens reguleren. Bij dat laatste speelt ook de regelgeving voor uitbesteding onder de Wft. Het gebrek aan zicht van de toezichthouder op het feitelijke gebruik van betaaldata is een risico. Tegelijkertijd is dit vooral een compliance vraag. Als alle partijen, zowel degene die binnen als degene die buiten het bereik van PSD2 vallen, zich aan de gecombineerde normen van PSD2 en de AVG houden, alsmede aan de regelgeving voor uitbesteding onder de Wft, is gegevensbescherming toereikend gewaarborgd.
6. Partijen kunnen ook via *passporting* actief zijn. Dat betekent dat zij niet onder Nederlands toezicht vallen. In dat geval hebben Nederlandse toezichthouders geen zicht op compliance. Daarbij kunnen toezichthouders uit andere EU-landen het toezicht anders invullen. Daarbij geldt wel dat alle partijen binnen de EU aan PSD2 moeten voldoen. De mogelijkheid dat toezichthouders in andere landen minder streng toezien op de eisen uit PSD2 zien sommige gesprekspartners ook als een risico.

Inhoudsopgave

Samenvatting 2
Inhoudsopgave 6
Lijst met afkortingen 8
1 Inleiding 1
1.1 Achtergrond 1
1.2 Onderzoeksvragen 6
1.3 Methoden 8
1.4 Leeswijzer 9
2 PSD2 in Nederland 13
2.1 Toezicht op PSD2 13
2.2 Implementatie PSD2 14
3 Markt voor betaaldiensten 18
3.1 Concurrentie 18
3.2 Innovatie 29
3.3 Europese betaalmarkt 35
3.4 Consumentenzijde 36
4 Veiligheid borgen 38
4.1 Bescherming toegang en betalingen 38
4.2 Consumentenbescherming 44
4.3 Gevolgen reikwijdtebepalingen en vrijstellingen 49
5 Gegevensbescherming consumenten 53
5.1 Waarborgen gegevensbescherming 55
5.2 Toegang tot gegevens 59
5.3 Gebruik van gegevens 75
6 Regelgeving en toezicht 80
6.1 Ontwikkeling regelgeving 80
6.2 Toezicht 82
7 Conclusie 90
7.1 Doeltreffendheid en doelmatigheid normen implementatiewet 90
7.1.1 Doeltreffendheid 90
7.1.2 Doelmatigheid normen implementatiewet 93
7.2 Belangrijkste effecten in de praktijk 98

7.3 Toereikendheid waarborgen gegevensbescherming 99
Literatuur 101
Bijlage A
Onderzoeksvragen 102
Bijlage B
Interviewpartners 105
Bijlage C
Consumentenenquête 107
Bijlage D Overzicht partijen met 7 en 8 vergunningen 116
Bijlage E Overzicht data EBA-register 118
Bijlage E.1 Overzicht alle landen 118
Bijlage E.2 Overzicht oprichting partijen actief in eigenmarkt 119
Bijlage E.3 Herkomst bedrijven met passport licentie 121
Bijlage E.4 Oprichting bedrijven met passport licentie 123
Bijlage F
Tijdlijn 125

Lijst met afkortingen

Afkorting	Betekenis
ACM	Autoriteit Consument & Markt
AFM	Autoriteit Financiële Markten
AISP	Account Information Service Provider
AP	Autoriteit Persoonsgegevens
API	Application Programming Interfaces
ASPSP	Account Servicing Payment Service Provider
AVG	Algemene Verordening Gegevensbescherming
B2B	Business-to-Business
B2C	Business-to-Consumer
DNB	De Nederlandsche Bank N.V.
EBA	European Banking Authority
EDPB	European Data Protection Board
EC	Europese Commissie
EG	Europese Gemeenschap
EU	Europese Unie
GDPR	General Data Protection Regulation
Kifid	Klachten Instituut Financiële Dienstverlening
MOB	Maatschappelijk Overleg Betalingsverkeer
PSD	Payment Service Directive
PISP	Payment Initiation Service Provider
PSP	Payment Services Providers
Q&A	Question & Answer
RTS	Regulatory Technical Standards
SCA	Stronger Customer Authentication
SEPA	Single Euro Payments Area
TPP	Third Party provider

1 Inleiding

SEO Economisch Onderzoek voert de evaluatie van PSD2 uit, in opdracht van het ministerie van Financiën. De inleiding beschrijft de achtergrond van deze evaluatie, de onderzoeksvragen en de toegepaste onderzoeksmethoden.

1.1 Achtergrond

Wat is PSD2?

De tweede Europese richtlijn betaaldiensten (PSD2) en de hierop gebaseerde nadere regelgeving vormen de kern van de regulering van betaaldienstverleners in Europa. PSD2 is Europese wetgeving die ook in Nederland is ingevoerd middels nationale wetgeving. In Nederland is PSD2 geïmplementeerd in de Wet op het financieel toezicht (Wft), in regelgeving die op de Wft is gebaseerd (gedelegeerde wetgeving) en in het Burgerlijk Wetboek.[1]

De eerste richtlijn uit 2007, PSD1, zorgde voor één markt voor betaaldiensten, maar had voornamelijk betrekking op (internationale) bankoverschrijvingen en creditcards, de traditionele vormen van betalingsverkeer.[2] Daarnaast zorgde PSD1 ook voor de toetreding van niet-bancaire betaalinstellingen tot de betaalmarkt, middels een vergunning (*payment institutions*). Daarbij regelde PSD1 ook prudentiële normen voor (klassieke) betaalinstellingen. PSD2 voegt aan PSD1 twee nieuwe diensten toe: betaalinitiatiediensten (*payment initiation service provider* of PISP) en rekeninginformatiediensten (*account information service provider* of AISP). Rekeninginformatiedienstverleners en betaalinitiatiedienstverleners verlenen hun diensten op basis van betaalrekeningen die betaaldienstgebruikers bij andere betaaldienstverleners aanhouden. PSD2 regelt de wijze waarop deze partijen toegang krijgen tot betaalrekeningen bij andere betaaldienstverleners. Kredietinstellingen (banken), elektronisch geldinstellingen en betaalinstellingen zijn betaaldienstverleners in de zin van PSD2 en de Wet op het financieel toezicht (Wft).

Regulatory standards (RTS) en *guidelines* van de *European Banking Authority* (EBA) vullen de PSD2 nader in. Daarnaast zijn er Q&A's van de EBA en De Nederlandsche Bank (DNB) die specifieke deelvragen verduidelijken. De EBA stelt een RTS op, en dient deze in bij de Europese Commissie, die vervolgens de RTS vaststelt, na controle door het Europees Parlement en publiceert deze vervolgens als een verordening (*Regulation*).[3] De richtsnoeren zijn bindend voor de toezichthouder en ondernemingen. Europese toezichthouders stellen een *guideline* van de EBA vast. DNB heeft aangegeven op dit moment alle EBA-*guidelines* te volgen die PSD2 invullen.

Welke diensten vallen onder PSD2?

PSD2 onderscheidt verschillende betaaldiensten, die in acht categorieën zijn opgedeeld;

1. Diensten waarbij de mogelijkheid wordt geboden contanten op een betaalrekening te storten, alsmede alle verrichtingen die voor het beheren van een betaalrekening vereist zijn;
2. Diensten waarbij de mogelijkheid wordt geboden contanten van een betaalrekening op te nemen, alsmede alle verrichtingen die voor het beheren van een betaalrekening vereist zijn;

---

1 De toezichtrechtelijke bepalingen zijn geïmplementeerd in de Wet op het financieel toezicht (Wft) en de bij deze wet behorende lagere regelgeving, zoals het Besluit prudentiële regels Wft (Bpr Wft), het Besluit Markttoegang financiële ondernemingen Wft (BMfo Wft) en het Besluit Gedragstoezicht financiële ondernemingen Wft (BGfo Wft); de civielrechtelijke bepalingen zijn opgenomen in titel 7B ('Betalingstransactie') van Boek 7 Burgerlijk Wetboek (BW).

2 Eerste richtlijn betalingsdiensten 2007/64/EG.

3 Zie https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/regulatory-process-financial-services_en

3. Uitvoering van betaaltransacties, met inbegrip van geldovermakingen, op een betaalrekening bij de betaaldienstverlener van de gebruiker of bij een andere betaaldienstverlener:
    a. Uitvoering van automatische afschrijvingen, met inbegrip van eenmalige automatische afschrijvingen;
    b. Uitvoering van betaaltransacties met behulp van een betaalkaart of een soortgelijk apparaat;
    c. Uitvoering van overmakingen, met inbegrip van doorlopende betaalopdrachten;
4. Uitvoering van betaaltransacties waarbij de geldmiddelen zijn gedekt door een kredietlijn die aan de betaaldienstgebruiker wordt verleend:
    a. Uitvoering van automatische afschrijvingen, met inbegrip van eenmalige automatische afschrijvingen;
    b. Uitvoering van betaaltransacties met behulp van een betaalkaart of een soortgelijk apparaat;
    c. Uitvoering van overmakingen, met inbegrip van automatische betaalopdrachten;
5. Uitgifte van betaalinstrumenten en/of acceptatie van betaaltransacties;
6. Geldtransfers;
7. Betaalinitiatiediensten;
8. Rekeninginformatiediensten.

Diensten 1 tot en met 6 zijn de klassieke betaaldiensten die al onder PSD1 gereguleerd werden. PSD2 introduceerde betaaldiensten 7 en 8, respectievelijk betaalinitiatiediensten en rekeninginformatiediensten.

Een betaalinitiatiedienst is "een dienst voor het initiëren van een betaalopdracht, op verzoek van de betaaldienstgebruiker, met betrekking tot een betaalrekening die bij een andere betaaldienstverlener wordt aangehouden".[4] Hiermee geeft een betaaldienstgebruiker een derde partij de opdracht een betaling namens hem of haar uit te voeren bij de betaaldienstverlener waar de rekening loopt. Dit kan alleen op verzoek van de rekeninghouder (c.q. betaaldienstgebruiker) en na diens uitdrukkelijke toestemming om toegang te verkrijgen tot zijn betaalrekening bij zijn ASPSP.

Een rekeninginformatiedienst is een "onlinedienst voor het verstrekken van geconsolideerde informatie over één of meer betaalrekeningen die de betaaldienstgebruiker bij een andere betaaldienstverlener of bij meer dan één betaaldienstverlener aanhoudt".[5] Hiermee heeft deze derde partij toegang tot de betaalgegevens van de betaalrekening, dit kan alleen op verzoek van en na diens uitdrukkelijke toestemming van de betaaldienstgebruiker. Met deze informatie kan deze partij bijvoorbeeld inzicht verschaffen in maandelijkse inkomsten en uitgaven, hulp bieden bij budgetbeheer of het kredietrisico inschatten. Deze dienst geeft alleen informatie over de betaalrekening, de derde partij kan er geen betaling mee initiëren.

Wat zijn de doelen van PSD2?

De drie doelstellingen van PSD2, zoals beschreven in de memorie van toelichting bij de implementatiewet[6], zijn:

1. Het versterken van een interne markt voor kaartbetalingen, internetbetalingen en mobiele betalingen;
2. Het stimuleren en faciliteren van innovaties;
3. Het verhelpen van gesignaleerde problemen van PSD1, zoals het gebruik van achterhaalde of vage begrippen.

Dit is een uitwerking van de volgende doelstellingen die de Europese Commissie noemt:[7]

4 Art. 4 (22) PSD2.
5 Art. 4 (16) PSD2.
6 Kamerstukken II 2017-2018, 34813, nr. 3.
7 Europese Commissie (2019). Revised rules for payment services in the EU, Document 32015L2366.

- Met PSD2 wordt de wettelijke basis gelegd voor de verdere ontwikkeling van een beter geïntegreerde interne markt voor elektronische betalingen binnen de EU. Ook wordt gezorgd voor het noodzakelijke juridische platform voor de gemeenschappelijke betalingsruimte voor de euro (*Single Euro Payments Area* (SEPA));
- Er worden uitgebreide regels voor betalingsdiensten mee ingevoerd, met als doel ervoor te zorgen dat internationale betalingen (binnen de EU) even eenvoudig, efficiënt en veilig kunnen verlopen als betalingen binnen één land;
- De richtlijn heeft als doel betaalmarkten te openen voor nieuwe deelnemers, wat moet leiden tot meer concurrentie, een grotere keuze en betere prijzen voor consumenten.

Voor dit onderzoek zijn deze doelstellingen onderverdeeld in de volgende vijf pijlers:

1. Het bevorderen van de concurrentie;
2. Het stimuleren en faciliteren van innovaties in het betalingsverkeer;
3. Het vergroten van de veiligheid van betalingsverkeer;
4. De bescherming van de deelnemers aan het betalingsverkeer;
5. Het bijdragen aan één Europese betaalmarkt.

Wat regelt PSD2?

Om deze doelen te bereiken, bevat PSD2 bepalingen die de regulering van de markt uitbreiden en ook aanscherpen. De volgende alinea's beschrijven de wijzigingen van PSD2 ten opzichte van PSD1. De wijzigingen staan ook uitgebreid beschreven in de memorie van toelichting.[8] De volgende alinea's geven de memorie van toelichting samengevat weer. Tabel 1.1 onderaan de inleiding geeft de wijzigingen schematisch weer, inclusief verwijzing naar het relevante artikel van PSD2.

De reikwijdte van de regelgeving is toegenomen onder PSD2. Alle transacties waarbij ten minste één van de partijen binnen de EU gevestigd is, vallen onder PSD2, dit is de '*one-leg-in-one-leg-out*'-bepaling. Daarnaast vallen transacties in niet-EU-valuta ook onder PSD2 als de transactie binnen de EU heeft plaatsgevonden. Verder is de reikwijdte vergroot door het aanscherpen van de verschillende uitzonderingen, zoals transacties binnen een beperkt netwerk (*limited network exemption*), de uitzondering op transacties die worden verricht via telecomapparatuur of -netwerken en de handelsagentuitzondering. Transacties binnen een beperkt netwerk met een laag transactievolume zijn nu uitgezonderd, maar aanbieders moeten het gebruik van deze vrijstelling wel melden aan DNB. Betalingen via telecomapparatuur zijn ook uitgezonderd voor transacties van maximaal € 50 voor afzonderlijke transacties per abonnee en het totaal aan transacties per abonnee mag niet uitkomen boven € 300 per maand. Ten slotte is de handelsagentvrijstelling aangescherpt, een partij komt alleen in aanmerking als deze voor één van de twee betrokken partijen als handelsagent optreedt, niet als deze voor beide partijen optreedt.

PSD2 regelt ook de regulering van en het toezicht op betaalinitatiedienstverleners en rekeninginformatiedienstverleners. Deze diensten waren onder PSD1 niet gereguleerd, maar zijn dat onder PSD2 wel. Deze partijen kunnen alleen actief zijn indien zij een PSD2-vergunning, verleend door DNB (of een bevoegde autoriteit uit een ander Europees land), hebben. Deze diensten werden ook voor de introductie van PSD1 aangeboden, maar dat gebeurde dan op basis van screenscraping, waarvoor geen contract nodig was met de bank van de gebruiker, of op basis van een specifiek hierop toegespitst contract in het geval van administratieve softwarepakketten voor bedrijven. Met de PSD2 zijn alle banken verplicht (vergunninghoudende) derde partijen -zonder dat daar een vergoeding tegenover staat of een contract voor nodig is- toegang tot de betaalrekeningen te verlenen, zodat zij de nieuwe diensten aan hun klanten kunnen aanbieden. Deze nieuwe vormen van dienstverlening bevorderen innovatie. Tegelijkertijd

[8] Kamerstukken II 2017-2018, 34813, nr. 3.

creëert de PSD2 een gelijk speelveld, omdat vergunninghoudende partijen onder identieke, objectieve, voorwaarden toegang kunnen krijgen tot de betaalrekening (mits de betaaldienstgebruiker uitdrukkelijk daarmee instemt).

De PSD2 stelt eisen aan de operationele systemen van de vergunninghoudende derde partijen. Deze hebben onder meer betrekking op de inrichting van de IT-processen, processen rond gegevensbescherming en het opzetten van een systeem voor het melden van incidenten. Soortgelijke verplichtingen bestaan ook voor andere betaaldienstverleners.

PSD2 introduceert ook regels voor niet toegestane en onbedoelde overboekingen. De betaaldienstverlener moet de betaler binnen één dag het bedrag van een niet-toegestane overboeking op zijn rekening crediteren, tenzij er een vermoeden van fraude is. Daarnaast hebben betaaldienstverleners een inspanningsverplichting om onbedoelde overboekingen te corrigeren.

PSD2 scherpt ook de regels voor betaaldienstagenten aan. Een betaaldienstagent is een persoon die bij de uitvoering van betaaldiensten voor rekening van een betaalinstelling of elektronischgeldinstelling optreedt.[9] Buitenlandse aanbieders kunnen in Nederland via een betaaldienstagent actief zijn. Zo dient een betaalinstelling (i) elke materiële wijziging in het Wwft-beleid van de betaaldienstagent onverwijld te melden aan de toezichthouder; (ii) van bestuurders en managers van een niet-gereguleerde betaaldienstagent aan te tonen dat deze betrouwbaar en deskundig zijn; en (iii) te melden voor welke betaaldiensten de betaaldienstagent wordt gemachtigd. Ook moeten betaaldienstverleners een Central Point of Contact (CCP) bij deze betaaldienstagenten aanwijzen, als aanspreekpunt voor de toezichthouders.

Een belangrijk aspect van PSD2 is dat gegevens van betaalrekeningen bij kredietinstellingen ook toegankelijk zijn voor vergunninghoudende betaalinitiatie- en rekeninginformatiedienstverleners. Dit heet ook wel *access to account*, afgekort XS2A. Dit creëert een gelijk speelveld tussen enerzijds banken en vergunninghoudende derde partijen en anderzijds tussen vergunninghoudende derde partijen onderling. Banken zijn nu verplicht, middels een interface, vaak een *application programming interface* (API), andere betaaldienstverleners toegang te verlenen tot betaalgegevens, indien de rekeninghouder daar toestemming voor geeft. Voor PSD2 ging dit zonder afspraken via screenscraping of was toegang afhankelijk van onderlinge afspraken tussen de banken en andere dienstverleners.

PSD2 staat niet toe dat winkeliers een vergoeding in rekening brengen aan consumenten voor het gebruik van betaalinstrumenten (als op deze instrumenten de *Interchange Fee Regulation* van toepassing is). Een dergelijke vergoeding heet '*surcharging*'[10]. De gedachte hierachter is dat PSD2 een gelijk speelveld creëert voor verschillende betaalinstrumenten en de consumenten beschermt. PSD2 biedt lidstaten een optie om het verbod nog verder uit te breiden, maar daar heeft Nederland geen gebruik van gemaakt. Verkopers hebben daardoor alleen nog de keuze om een bepaald betaalinstrument niet meer aan te bieden, of om de kosten daarvan door te berekenen in de prijzen van producten.

In sommige gevallen is het transactiebedrag vooraf niet bekend, bijvoorbeeld bij het tanken bij een onbemand tankstation. In dat geval bepaalt PSD2 dat de betaaldienstverlener het geld op de betaalrekening kan blokkeren tot een bepaald bedrag, mits de betaler daarmee instemt.[11] Dit voorkomt dat iemand zonder te betalen weg kan rijden

9 Wft, art. 1:1.
10 Dit geldt enkel voor de onder de IFR beperkte betaalkaarten (4-party schemes)
11 Deze instemming is vaak impliciet. Bij het gebruik van een onbemand tankstation staat vaak aangegeven dat als iemand tankt, € 150 op de bankrekening wordt geblokkeerd. Hier hoeft een betaaldienstgebruiker geen expliciete toestemming voor te geven, het gebruik van deze methode impliceert al toestemming.

bij het tankstation. Als het definitieve transactiebedrag bekend is, heft de betaaldienstverlener de blokkade op en verrekent het exacte bedrag.

Om de veiligheid van het betalingsverkeer te vergroten, introduceert PSD2 *Strong Customer Authentication* (SCA; sterke cliëntauthenticatie). Dit is in een RTS van de EBA geregeld. SCA is van toepassing bij het online toegang krijgen tot de betaalrekening, het initiëren van een elektronische betaling in de winkel of via een communicatiemiddel op afstand een handeling verrichten die een risico op fraude of ander misbruik met zich mee kan brengen. Er is sprake van SCA als de betaler minimaal twee van de volgende aspecten combineert: kennis (iets wat alleen de betaler weet, zoals een pincode), bezit (iets wat alleen de gebruiker heeft, zoals een pinpas) en inherente eigenschap (iets wat de gebruiker is, zoals een vingerafdruk of gezichtsherkenning). Dit beoogt het risico op fraude te verminderen en het betalingsverkeer veiliger te maken. Een gebruiker moet SCA uitvoeren de eerste keer dat hij een rekening of overzicht gebruikt. In geval van rekeninginformatiediensten moet toestemming via SCA elke 90 dagen opnieuw gegeven worden[12]. Bij betaalinitiatie moet de gebruiker bij elke transactie een authenticatie geven, tenzij een uitzondering van toepassing is. Er zijn namelijk enkele uitzonderingen op het gebruik van SCA, bijvoorbeeld als het bedrag onder een bepaalde grens valt (net zoals bij contactloos pinnen onder de € 50) of als de tegenpartij al goedgekeurd is door de verkoper (*'whitelisting'*).

PSD2 faciliteert het delen van betaalgegevens. Daarbij is het van belang dat deze gegevens goed beschermd zijn. De dienstverlener kan alleen persoonsgegevens verwerken met de uitdrukkelijke toestemming van de gebruiker. Hiervoor moet de aanbieder in de bedrijfsvoering het proces van gegevensbescherming en de doelen voor het gebruik van de data vastleggen. De wijze waarop de betaaldienstverlener dit van plan is, is onderdeel van de vergunningsaanvraag. Omdat het delen van persoonsgegevens toegestaan is op basis van PSD2, zijn er raakvlakken tussen PSD2 en de Algemene Verordening Persoonsgegevens (AVG).

De Europese Bankenautoriteit (EBA) heeft met de komst van PSD2 extra bevoegdheden gekregen. Zo is het de taak van de EBA om in samenwerking met de Europese Centrale Bank (ECB) richtsnoeren voor de implementatie en monitoring van PSD2 vast te stellen. Daarbij houdt de EBA een register bij waarin alle vergunninghoudende en vrijgestelde betaaldienstverleners staan geregistreerd. Ook stellen de EBA en ECB uitvoeringsvoorschriften op, waaronder *Regulatory Technical Standards* (RTS), *Implementing Technical Standards* (ITS) en richtsnoeren (guidelines).

Ten slotte bepaalt PSD2 dat betaaldienstverleners diensten moeten aanbieden in het land waar zij hun vergunning aanvragen en in die lidstaat ook een statutaire zetel of hoofdkantoor moeten hebben. Partijen die in Nederland een vergunning willen aanvragen, moeten dus in Nederland klanten bedienen en in Nederland personeel hebben. Het is dus niet mogelijk om alleen in Nederland actief te zijn met een vergunning van een toezichthouder uit een andere lidstaat. Het is wel mogelijk als de aanbieder in beide landen actief is. Dit is de zogeheten substance-eis.

Wanneer is PSD2 in Nederland ingevoerd?

De Europese Commissie publiceerde het eerste voorstel van PSD2 in juli 2013. Eind 2015 namen het Europees Parlement en de Europese Raad van Ministers PSD2 aan. In januari 2016 trad PSD2 officieel in werking, maar daarna volgden nog enkele consultatiesessies om PSD2 concreter in te vullen. In september 2018 nam de Tweede Kamer het wetsvoorstel voor de implementatie van PSD2 aan. PSD2 trad in februari 2019 in werking in Nederland. Nederland was hierin later dan andere landen, omdat PSD2 officieel per januari 2018 van kracht moest zijn.

12 De 90 dagen regel is geformuleerd als een optionele uitzondering op de regel dat een AISP bij elke toegang SCA moet toepassen.

Wat is de achtergrond van deze evaluatie?

Tijdens de behandeling van de implementatiewet PSD2 in de Tweede Kamer is besloten dat binnen drie jaar na inwerkingtreding de werking ervan wordt geëvalueerd. Deze evaluatie richt zich op de doelmatigheid, doeltreffendheid en de effecten in de praktijk van de implementatiewet. Ook wordt gekeken naar de waarborgen in de implementatiewet voor de gegevensbescherming in combinatie met bestaande regelgeving. Naast deze nationale evaluatie voert de Europese Commissie ook een Europese evaluatie van PSD2 uit in 2022.

De Tweede Kamer heeft in enkele moties aandachtspunten voor de evaluatie meegegeven. De Tweede Kamer roept op dat in deze evaluatie o.a. de privacy van mensen en hun betaalgegevens centraal moeten staan.[13] Daarbij dient bijzondere aandacht te worden besteed aan kwetsbare groepen en mogelijk ongewenst gebruik van betaalgegevens. Een andere motie verzoekt de regering om op Europees niveau de marktverhoudingen te monitoren en indien nodig maatregelen te nemen.[14] Andere aandachtspunten voor de evaluatie, die niet direct uit moties volgen, zijn de reikwijdte van de wet en het verbod op *surcharging*.

1.2 Onderzoeksvragen

Onze onderzoeksopdracht bevat drie hoofdvragen. In onze opdracht is ook een aantal deelvragen geformuleerd.

Hoofdvragen

1. In hoeverre zijn de normen in de implementatiewet doeltreffend en doelmatig in Nederland, gelet op de in de memorie van toelichting beschreven doelstellingen?
2. Wat zijn de belangrijkste effecten van de implementatiewet in de praktijk?
3. Zijn de waarborgen in de implementatiewet voor de gegevensbescherming in combinatie met bestaande regelgeving adequaat?

Deelvragen

Algemeen

a. In welke mate sluit de implementatiewet aan bij de technologische ontwikkelingen op de betaalmarkt bijvoorbeeld met het oog op technische dienstverleners die ondersteuning bieden bij het verlenen van betaaldiensten en fragmentatie in de keten van betaaldienstverleners (mede gelet op regels voor uitbesteding in PSD2)?
b. Welke effecten zijn zichtbaar van het gedeeltelijke verbod op *surcharging*? En is voldoende duidelijk voor consumenten en winkeliers welke betaalinstrumenten (met name van kleinere creditcardmaatschappijen) wel en niet onder het verbod op *surcharging* vallen?

Gegevensbescherming/privacy-risico's

c. Leveren de bepalingen in de implementatiewet in verhouding tot de AVG in de praktijk uitdagingen/problemen op (met inachtneming van de verduidelijking die de EDPB heeft geboden)?
d. Hoe worden betaalgegevens gebruikt (doelbinding)?
e. Is voldoende geborgd dat er geen toegang is tot meer gegevens dan noodzakelijk?
f. Worden betaalgegevens ook gebruikt voor maatschappelijk onaantrekkelijke doelen?
g. Werking van de uitdrukkelijke toestemming: Weten mensen voldoende waar ze ja tegen zeggen als ze toestemming geven om toegang tot hun betaalgegevens te geven? Wordt de toestemming voldoende expliciet en

13 Kamerstukken II, 2017-18, 34813, nr. 17.
14 Kamerstukken II, 2017-18, 34813, nr. 22.

specifiek gevraagd? Geeft de consument bewust toestemming (i.e. is de consument zich volledig bewust van de gevolgen van het geven van toestemming)? Voelt de consument zich vrij om toestemming te weigeren? Kunnen mensen eenvoudig terug komen op een gegeven toestemming?

h. Hoe kunnen consumenten worden geholpen bij het bewaren van overzicht ten aanzien van de gegeven toestemmingen (dat kan d.m.v. het dashboard van banken, maar zijn er ook andere manieren)?

Effecten in de praktijk

i. Is het aanbod van betaaldiensten veranderd in Nederland door PSD2 en wat heeft dat voor effect gehad op de concurrentie in de betaalmarkt?
j. Zijn er kwetsbare groepen voor wie dit wetsvoorstel tot problemen heeft geleid? Zo ja, voor welke groepen en tegen welke problemen lopen zij aan?

Onze onderzoeksopdracht benoemt hierbij vier bijzondere aandachtspunten, namelijk:

- De gevolgen voor de marktverhoudingen (concurrentie, diversiteit, monopolies, marktmacht) op de betaalmarkt van de invoering van PSD2;
- Het effect van de implementatie van PSD2 in Nederland;
- De mate waarin het voldoende duidelijk is welke betaalinstrumenten met name van kleinere creditcardmaatschappijen wel en niet onder het verbod op *surcharging* vallen; en
- De mate waarin de reikwijdte van de wetgeving voldoet in het licht van toenemende fragmentatie van de betaalketen.

Doeltreffendheid betreft de vraag of de normen waaruit PSD2 bestaat doel treffen. Met andere woorden, zijn de doelen van PSD2 gehaald (doelbereik) als gevolg van de implementatie van PSD2?

Doelmatigheid gaat over de mate waarin doelen efficiënt worden bereikt. Hiermee speelt de vraag of beleid doelmatig is pas ná de vraag of dit beleid doeltreffend is (zonder doeltreffendheid kunnen doelen überhaupt niet efficient bereikt worden). Doelmatigheid gaat over de wijze waarop de doelen gehaald wordt. Dit valt uiteen in twee onderdelen:

1. Worden de doelen op een efficiënte wijze bereikt; en
2. In welke mate heeft het beleid schadelijke neveneffecten?

Efficiëntie valt uiteen in verschillende aspecten zoals implementatiekosten, administratieve lasten, handhavingskosten en compliance kosten. Zulke kosten kunnen hoger of lager uitvallen door o.a. de vormgeving van wet- en regelgeving, de mate waarin het beleid uitvoerbaar is en eventuele neveneffecten van het beleid.

De bevindingen van dit onderzoek kunnen input voor de Europese evaluatie van PSD2 worden gebruikt. Aandachtspunten voor deze Europese evaluatie zijn aangegeven in artikel 108 PSD2 en in de strategie voor retailbetalingen in Europa van 25 september 2020.

Deze evaluatie vult deze brede onderzoeksopdracht door 34 onderzoeksvragen te formuleren. Deze benoemen we doorlopend gedurende het onderzoek. Volledigheidshalve staat een overzicht van de geformuleerde onderzoeksvragen in Bijlage A. De onderzoeksvragen zijn te groeperen in een viertal onderwerpen met een aantal deelonderwerpen die aansluiten bij de doelen van PSD2, namelijk i) de markt voor betaaldiensten, ii) veiligheid, iii) gegevensbescherming en privacy, en iv) regelgeving en toezicht. Deze groepering van onderzoeksvragen gebruiken we in het vervolg als hoofdstukindeling.

1.3 Methoden

De evaluatie maakt gebruik van een aantal verschillende onderzoekmethoden:

- Deskresearch;
- Interviews met stakeholders;
- Consumentenenquête;
- Analyse EBA-register;
- Rondetafelsessies.

Het onderzoeksteam is tijdens het onderzoek bijgestaan door een klankbordgroep. Deze klankbordgroep bestond uit vertegenwoordigers van het ministerie van Financiën, het ministerie van Justitie en Veiligheid, ACM, AFM, AP en DNB. Er zijn 4 bijeenkomsten van de klankbordgroep geweest.

Deskresearch

De verkennende fase van de evaluatie bestaat uit het bestuderen van de beschikbare literatuur over PSD2. Hierin zijn drie stromen van literatuur belangrijk. De officiële beleidsstukken, zoals de Richtlijn, de RTS, de memorie van toelichting, stellen gedetailleerd wat PSD2 inhoudt en wat de verschillen zijn met PSD1. Dit is een belangrijke bron voor de evaluatie, omdat de onderzoekers zo kunnen vaststellen wat PSD2 inhoudt. Daarnaast hebben toezichthouders, belangenorganisaties en adviesbureaus enkele rapporten geschreven over de implementatie van PSD2, de werking van PSD2. Dit is van belang voor de evaluatie, omdat deze rapporten nadere uitleg geven over PSD2 en inzicht geven in hoe PSD2 in de praktijk werkt. Ten slotte is de academische literatuur een bron voor de evaluatie, omdat wetenschappers PSD2 op een conceptueel niveau bestuderen, wat mogelijk leidt tot nieuwe inzichten.

De bevindingen uit de deskresearch dienen als input voor de evaluatie en bieden ook belangrijke aanknopingspunten voor de andere onderzoeksmethoden. Zo kan het evaluatieteam de inzichten uit de literatuur toetsen in gesprekken met stakeholders, en leidt de literatuur tot hypothesen die de data-analyse kunnen beantwoorden.

Consumentenenquête

De evaluatie stelt de bevindingen en ervaringen van consumenten vast middels een enquête. In deze enquête vraagt het onderzoeksteam consumenten onder andere of zij een PSD2-dienst hebben gebruikt, waarom ze wel of niet van deze diensten gebruik hebben gemaakt, wat de ervaringen met *surcharging* zijn en hoe consumenten denken over het delen van betaalgegevens. Bijlage C geeft de enquêtevragen weer en beschrijft de resultaten.[15] .

SEO heeft de enquête ontworpen en Centerdata[16] heeft deze enquête onder haar deelnemers verspreid. De enquête stond tussen 1 en 19 oktober 2021 open. 3.239 huishoudens hebben deze enquête ontvangen. 2.480 huishoudens (76,6 procent) hebben deze enquête volledig ingevuld, 28 huishoudens (0,8 procent) hebben de enquête deels ingevuld. 731 huishoudens hebben niet op de uitnodiging geageerd, waarmee het percentage non-respons 22,6 procent bedraagt.

---

15 We voorzien de respondenten zo goed mogelijk van informatie om de vragen zo zorgvuldig mogelijk te beantwoorden. Desondanks kan gebrek aan kennis er soms toe leiden dat antwoorden niet altijd een volledig beeld geven van de werkelijkheid. Dit leidt soms tot nuancering van het beeld dat uit de enquete naar voren komt. Als dit het geval is, merken we dat op.

16 https://www.centerdata.nl/projecten/het-centerpanel

Analyse EBA-register

De nationale bevoegde autoriteiten van een land dienen data over vergunningen en activiteiten in bij de EBA. De EBA laat bepaalde data zien in het Europese betaalinstellingenregister. Het register is zo een weergave van o.a. welke bedrijven welk type licentie hebben, waar deze bedrijven zijn gevestigd en wanneer deze zijn opgericht.

Op basis van een analyse van dit EBA-register maakt deze evaluatie een vergelijking op het niveau van de Europese Unie. Uit de analyse blijkt hoeveel PSD2-vergunningen elk land heeft en in welke mate *passporting* tussen de landen verschilt. Ook geeft de analyse informatie over of Nederland een eventueel concurrentienadeel heeft (gehad) ten opzichte van landen waarbij PSD2 eerder is geïmplementeerd.

Interviews

De evaluatie betrekt stakeholders betaaldienstverleners en experts bij het onderzoek via interviews. In deze interviews spreekt het evaluatieteam met aanbieders van betaalinitiatiediensten en rekeninginformatiediensten, banken, niet-bancaire betaaldienstverleners, hoogleraren, consultants, Nederlandse en Europese beleidsmakers, toezichthouders, brancheverenigingen, retailers en consumentenorganisaties. Bijlage B beschrijft de 51 organisaties die geïnterviewd zijn.

Het onderzoeksteam ondervraagt de interviewpartners op hun ervaringen met PSD2. De bevindingen uit de interviews dienen als input voor de evaluatie. Het onderzoeksteam heeft de bevindingen van de gesprekspartners gevalideerd in andere gesprekken. Dit leidt tot een gewogen beeld over PSD2.

Rondetafelsessies

Naast individuele interviews heeft het onderzoeksteam twee rondetafelsessies georganiseerd, waarin de conceptbevindingen zijn getoetst bij stakeholders. Na deze sessie zijn enkele bevindingen aangescherpt of genuanceerd. Aan de rondetafelsessies hebben de leden van het Maatschappelijk Overleg Betalingsverkeer, de toezichthouders, enkele ministeries en consumentenorganisaties deelgenomen.

1.4 Leeswijzer

Dit rapport is opgebouwd langs de lijnen van de verschillende thema's in de onderzoeksvragen. De inleiding beschrijft wat PSD2 is en welke wijzigingen vergeleken met PSD1 zijn opgetreden. Hoofdstuk 2 bespreekt het toezicht op PSD2 en het proces van wetgeving en implementatie. Nadat de kaders zijn geschetst, richt hoofdstuk 3 zich op de markt voor betaaldiensten. Dit hoofdstuk bespreekt onder meer de effecten van PSD2 op concurrentie en innovatie in de markt voor betaaldiensten. Daarnaast raakt de Nederlandse markt ook aan de Europese betaalmarkt. Verder beschrijft dit hoofdstuk ook de consumentenzijde van de betaalmarkt. Hoofdstuk 4 beantwoordt de onderzoeksvragen die gaan over het borgen van veiligheid. Dit rapport beschouwt veiligheid op verschillende facetten: veiligheid van toegang tot een dienst, veiligheid van betalingen en veiligheid van de dienstverleners. Hoofdstuk 5 gaat dieper in op de gegevensbescherming voor consumenten. Hieronder vallen de waarborgen die gelden, de bescherming van toegang tot gegevens en het gebruik van gegevens. Dit verschilt van hoofdstuk 4 omdat dat hoofdstuk ingaat op het voorkomen van fraude en algemene veiligheid van de diensten en systemen, hoofdstuk 5 richt zich op de privacyaspecten. Ten slotte gaat hoofdstuk 6 in op de ontwikkeling van de regelgeving en op de taken van de verschillende toezichthouders: DNB, Autoriteit Financiële Markten (AFM), Autoriteit Persoonsgegevens (AP) en de Autoriteit Consumenten en Markt (ACM).

Tabel 1.1 Vernieuwing PSD2 vergeleken met PSD1

Onderwerp	Nieuw in PSD2 ten opzichte van PSD1	Artikel PSD2
Territoriale uitbreiding	Onder PSD1 was het toepassingsbereik van de meeste bepalingen beperkt tot betalingstransacties waarbij zowel de betaaldienstverlener van de betaler alsook de betaaldienstverlener van de begunstigde of de enige bij de betalingstransactie betrokken betaaldienstverlener in de EU was gevestigd en die werden verricht in een valuta van een lidstaat. Onder PSD2 is dit gewijzigd en worden ook transacties gereguleerd waarbij slechts één van de betrokken betaaldienstverleners in de EU is gevestigd (*one-leg-in-one-leg-out transactions*). Daarnaast zullen ook transacties in niet-EU valuta binnen de reikwijdte van PSD2 worden gebracht, wanneer de bij de transactie betrokken betaaldienstverlener(s) zich in de EU bevinden.	Artikel 2
Uitzondering 'binnen beperkt netwerk'	De uitzondering voor betaaldiensten die worden verricht binnen een beperkt netwerk wordt in PSD2 verduidelijkt. PSD2 maakt duidelijk dat betaalinstrumenten (bijv. klantenkaarten, tankkaarten, maaltijdcheques) niet meer worden gebruikt voor betalingstransacties ten behoeve van de aankoop van goederen en diensten binnen meer dan één beperkt netwerk, noch voor de aankoop van een onbeperkte reeks goederen en diensten. Hoewel PSD2 beoogde duidelijkheid te bieden heeft EBA niettemin *draft guidelines* over de *limited network* vrijstelling geconsulteerd.[17]	Artikel 3 sub k en overwegingen 13 en 14
Uitzondering 'betalingstransacties die worden verricht via telecomapparatuur of -netwerken'	De uitzondering die geldt voor betalingstransacties die worden verricht via telecomapparatuur of -netwerken wordt in PSD2 aangescherpt. Dit betreft onder meer betalingen die via de telefoonrekening lopen zoals betalingen voor muziek, spelletjes en deelname aan TV- en radioprogramma's (zoals stemmen). Om in aanmerking te komen voor de uitzondering introduceert PSD2 een limiet van € 50 voor afzonderlijke transacties per abonnee en mag het totaal aan transacties per abonnee niet uitkomen boven € 300 per maand. Daarnaast zijn betalingstransacties in verband met giften aan liefdadigheidsinstellingen en betalingen met een laag risicoprofiel (als het bedrag van de betalingstransactie onder een in de wet bepaalde drempel ligt) uitgezonderd.	Artikel 3 sub l en overwegingen 15 en 16
Uitzondering 'handelsagenten'/*commercial agent exemption*	De uitzondering voor handelsagenten/commerciële agent vrijstelling is aangescherpt in PSD2. Deze geldt uitsluitend wanneer die handelsagent middels een overeenkomst gemachtigd is om voor rekening van alleen de betaler of alleen de begunstigde de verkoop of aankoop van goederen of diensten via onderhandelingen tot stand te brengen of te sluiten. Indien agenten voor rekening van zowel de betaler als de begunstigde handelen (zoals op bepaalde platformen voor elektronische handel), worden zij slechts van het toepassingsbereik van PSD2 uitgesloten indien zij op geen enkel ogenblik in het bezit zijn van of de controle hebben over de geldmiddelen van de cliënten.	Artikel 3 sub m en overweging 11
Substance	PSD2 maakt expliciet dat een betaalinstelling die een vergunning in een lidstaat aanvraagt, ten minste een deel van haar betaaldienstverlening in die lidstaat moet verrichten. Deze 'substance-eis' geldt ook voor betaalinstellingen die reeds een vergunning hadden op grond van PSD1.	Artikel 11

17 https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-limited-network-exclusion-under-PSD II

Onderwerp	Nieuw in PSD2 ten opzichte van PSD1	Artikel PSD2
Vergunningsplicht voor Betaalinitiatiedienstverleners en Rekeninginformatiedienstverleners	Als nieuwe categorie betaaldienstverlener moeten zowel rekeninginformatiedienstverleners alsook betaalinitiatiedienstverleners een vergunning als betaalinstelling aanvragen op grond van PSD2. Europees recht verlangt van AISPs slechts een registratie, maar Nederland eist een vergunning.	Artikel 11 en Bijlage 1 punt 7 en 8
Notificaties	Indien een betaalinstelling per lidstaat gebruikmaakt van meerdere agenten kunnen lidstaten eisen dat de betaalinstelling een Central Point of Contact aanwijst en organiseert. De host toezichthouder heeft verdergaande bevoegdheden om bij de genotificeerde entiteit informatie op te vragen.	Artikel 15
Betaaldienstagenten	PSD2 voorziet in een aanscherping van de regels ten aanzien van agenten die door betaalinstellingen worden ingeschakeld, de zogenaamde betaaldienstagenten. Zo dient een betaalinstelling (i) elke materiële wijziging in het Wwft-beleid van de betaaldienstagent onverwijld te melden; (ii) van bestuurders en managers van een niet gereguleerde betaaldienstagent aan te tonen dat deze betrouwbaar en deskundig zijn; en (iii) te melden voor welke betaaldiensten de betaaldienstagent wordt gemachtigd.	Artikel 19
Toegang tot de betaalrekeningdiensten van kredietinstellingen	Op basis van PSD2 dienen vergunninghoudende betalingsinstellingen. op objectieve, niet-discriminerende en evenredige basis toegang te hebben tot de betaalrekeningen van kredietinstellingen. Dergelijke toegang dient uitgebreid genoeg te zijn om betalingsinstellingen in staat te stellen op onbelemmerde en efficiënte wijze betalingsdiensten aan te bieden. Merk op dat artikel 36 niet ziet op betaalinitiatiedienstverleners en rekeninginformatiedienstverleners	Artikel 36
Nieuwe betaaldienst: Betaalinitiatiedienst	De betaalinitiatiedienst is een nieuwe dienst voor het initiëren van betaalopdrachten, op verzoek van de betaaldienstgebruiker met betrekking tot een betaalrekening die bij een andere betaaldienstverlener wordt aangehouden. Daarbij kan gedacht worden aan een niet-bancaire aanbieder die een betaaldienst aanbiedt aan de webwinkel waarbij de consument via een betaalknop van de betaling van een consument aan een webwinkel kan initiëren. Met de komst van PSD2 kunnen betaalinitiatiedienstverleners via hun internetapplicaties betaaldiensten verlenen in opdracht van een rekeninghouder bij zijn bank. Banken zijn verplicht deze functionaliteit mogelijk te maken. Dit maakt onderdeel uit van *access to the account* (XS2A) en betreft één van de kerninnovaties in PSD2.	Artikel 66
Nieuwe betaaldienst: Rekeninginformatiedienst	De rekeninginformatiedienst is een online dienst voor het verstrekken van geconsolideerde informatie over een of meer betaalrekeningen die de betaaldienstgebruiker bij een of meer betaaldienstverleners aanhoudt. Rekeninginformatiedienstverleners krijgen toegang tot rekeninginformatie – als de rekeninghouder hier toestemming voor geeft – en kunnen die rekeninginformatie gebruiken voor het aanbieden van hun diensten. Banken moeten de betreffende rekeninginformatie aan derde partijen beschikbaar stellen. Deze dienst valt ook onder XS2A en betreft de tweede kerninnovatie die PSD2 mogelijk maakt.	Artikel 67
Transactiebedrag vooraf onbekend	Wanneer bij een betalingstransactie het bedrag vooraf onbekend is, bijvoorbeeld bij een hotelreservering of een onbemand tankstation, dan mag de betaaldienstverlener alleen na instemming van de betaler een bedrag op de rekening blokkeren.	Artikel 75

Onderwerp	Nieuw in PSD2 ten opzichte van PSD1	Artikel PSD2
Privacy	De verwerking van persoonsgegevens wordt slechts toegestaan voor zover dit noodzakelijk is voor de betaaldienst en met de uitdrukkelijke toestemming van de gebruikers, of indien dit noodzakelijk is in het kader van het voorkomen van betalingsfraude.	Artikel 94
Vereisten voor Operations en IT	PSD2 introduceert operationele eisen om de gegevens van de klant te beschermen en te waarborgen dat alleen de klant betaaltransacties kan opgeven. Betaalinstellingen moeten daartoe waarborgen dat gegevens beschermd zijn tegen onrechtmatig inzien en/of verwerken en een veilige communicatie en gegevensopslag plaatsvinden. De beschikbaarheid van gegevens en de geautomatiseerde gegevensverwerking moeten daarbij gewaarborgd zijn.	Artikel 95 en 98
Melding van incidenten	Een betaalinstelling moet een systeem voor classificatie en melding van operationele- en beveiligingsincidenten hebben en een proces hebben om majeure incidenten te melden aan DNB. Deze moeten tevens door DNB aan ECB en EBA worden gerapporteerd. Daarnaast moet een betaalinstelling periodiek en minstens jaarlijks statistische gegevens over fraude verstrekken aan de toezichthouder. Deze regels gelden voor alle betaaldienstverleners	Artikel 96
Authenticatie	Betaalinstellingen moeten toereikende beveiligingsmaatregelen nemen om de veiligheid van betalingstransactie te vergroten en de vertrouwelijkheid en integriteit van de persoonlijke beveiligingsgegevens van betalingsdienstgebruikers te beschermen. Om die redenen dienen betaalinstellingen op grond van PSD2 gebruik te maken van een sterke cliëntauthenticatie (*Strong Customer Authentication* (SCA)) wanneer een betaler: (i) zich online toegang tot zijn betaalrekening verschaft, (ii) een elektronische betalingstransactie initieert of (iii) via een communicatiemiddel op afstand een handeling van eender welke aard uitvoert die een risico op betalingsfraude of andere vormen van misbruik met zich mee kan brengen.	Artikel 97

2 PSD2 in Nederland

2.1 Toezicht op PSD2

Bij het toezicht op de wet zijn vier toezichthouders betrokken: Autoriteit Consument & Markt (ACM), (Autoriteit Financiële Markten) AFM, Autoriteit Persoonsgegevens (AP) en De Nederlandsche Bank (DNB).

DNB verleent vergunningen aan de twee categorieën betaaldienstverleners (betaalinstellingen en elektronischgeldinstellingen) en oefent het prudentieel en integriteitstoezicht op deze partijen uit zoals vastgelegd in de wet.[18] DNB verleent ook de vergunningen aan alle betaaldienstaanbieders (behalve banken[19]) in de zin van PSD2. Daarbij ziet DNB toe op de beveiligingsmaatregelen en authenticatieprocedures van deze betaaldienstverleners zoals die voorvloeien uit de RTS. Als prudentieel toezichthouder kijkt DNB of de betaaldienstverleners kunnen voldoen aan hun financiële verplichtingen. Ook kijkt DNB naar de integere bedrijfsvoering van betaaldienstverleners en de betrouwbaarheid en geschiktheid van hun bestuurders. Daarnaast kijkt DNB naar de beveiligingsmaatregelen die instellingen moeten treffen, om hun dienstverlening veilig te kunnen aanbieden.

Naast het toezicht op de verwerking van persoonsgegevens overeenkomstig de AVG, houdt de AP toezicht op de toegang van betaaldienstverleners tot de persoonsgegevens van de gebruikers. Banken moeten het mogelijk maken dat derde partijen toegang krijgen tot de betaalrekening van hun klanten. Een belangrijke voorwaarde is dat klanten hiervoor hun uitdrukkelijke toestemming hebben gegeven.[20] De AP houdt toezicht op de voorwaarde van uitdrukkelijke toestemming in PSD2.

De ACM houdt, naast het toezicht op de naleving van de algemene mededingingsregels, toezicht op de toegang van betaalinstellingen in de zin van PSD2 tot betaalsystemen (zoals bijvoorbeeld *payment s*chemes) en betaalrekeningdiensten (dus een betaalrekening bij een bank waar een betaalinstelling gelden op kan laten binnenkomen). Betaalinstellingen moeten op objectieve, niet-discriminerende en evenredige basis toegang hebben tot betaalrekeningdiensten en betaalsystemen. Bij weigering van toegang (waaronder de ACM ook begrijpt een opzegging van een betaalrekening) moeten partijen dat melden bij de ACM. Als een grond voor een dergelijke toegangsweigering ontbreekt, kan de ACM sancties opleggen.[21] Verder ziet de ACM toe op het berekenen van toeslagen voor het gebruik van een betaalmiddel (*surcharging*).[22]

De AFM oefent het gedragstoezicht op betaaldienstverleners uit. Dit houdt in dat de AFM toezicht houdt op de informatieverstrekking door betaaldienstverleners, de inrichting van klachtenprocedures en het recht van rekeninghouders om gebruik te maken van rekeninginformatiediensten en betaalinitiatiediensten. Dit betekent onder meer dat de AFM toezicht houdt op de informatieverstrekkingseisen die gelden voor betaaldienstverleners, zoals opgenomen in de Wft en het Besluit Gedragstoezicht financiële markten. Ook gaat de AFM na of er bij het verlenen van

18 De belangrijkste betaaldienstverleners zijn banken. Die krijgen hun vergunning van ECB, maar staan voor zover het PSD2 betreft weer onder toezicht van DNB.
19 De Europese Centrale Bank (ECB) verleent vergunningen aan banken.
20 Artikel 94 PSD2.
21 Artikelen 35 en 36 van de PSD2-richtlijn, geïmplementeerd in artikelen 5:88 (toegang tot betalingssystemen) en 5.88a (toegang tot betaalrekeningdiensten) van de Wet op het financieel toezicht (Wft). De ACM kan een bestuurlijke boete of een last onder dwangsom opleggen bij niet-naleving van deze toegangsbepalingen of een bindende aanwijzing geven. Voor de ACM geldt wel de verplichting om de AFM en DNB om hun zienswijze te vragen.
22 art. 62 lid 4 PSD2, artikel 520, derde en vierde lid, van Boek 7 van het Burgerlijk Wetboek.

betaaldiensten geen oneerlijke handelspraktijken plaatsvinden, op basis van de Wet handhaving consumentenbescherming (Whc). De AFM houdt tevens toezicht op betaaldienstverleners bij het naleven van de rechten van de consument bij het aangaan van betalingstransacties, zoals vastgelegd in het Burgerlijk Wetboek (Titel 7B van Boek 7). Met de komst van PSD2 is aan deze wet onder andere het recht van de consument om gebruik te maken van derde partijen, voor het leveren van betaalinitiatiediensten of rekeninginformatiediensten, toegevoegd. Deze partijen moeten daar wel de benodigde DNB-vergunning voor hebben.

2.2 Implementatie PSD2

PSD2 kent een lange ontstaansgeschiedenis. Bijlage F bevat een tijdslijn met de belangrijkste stappen. De introductie van PSD2 startte medio januari 2016, toen de richtlijn in werking trad. De EU-lidstaten kregen de tijd tot uiterlijk 13 januari 2018 om deze Europese Richtlijn in hun nationale wetgeving te implementeren[23]. Met ingang van die datum moesten de lidstaten dan ook voldoen aan de Richtlijn, op een aantal veiligheidsprocedures en -maatregelen na. De EBA heeft met betrekking tot een aantal veiligheidsprocedures *Regulatory Technical Standards* (RTS) ontwikkeld. De belangrijkste hiervan heeft betrekking op sterke klantauthenticatie (dubbele beveiliging) en veilige communicatie (tussen de derde partijen – zie hierna - en de banken). Deze RTS zijn in maart 2018 als gedelegeerde verordening gepubliceerd. Banken moesten hieraan uiterlijk 14 september 2019 voldoen. Ze zijn van toepassing op elektronische betalingen op afstand en transacties aan de toonbank en, meer algemeen, op de interactie tussen banken en derde partijen, die in opdracht van de rekeninghouder via betalingsinitiatiediensten en rekeninginformatiediensten toegang krijgen tot de betaalrekening van de houder van deze rekening bij zijn bank. Deze derde partijen moeten hiervoor een vergunning hebben van de bevoegde autoriteit (in Nederland DNB). Een betaaldienstverlener kan bij DNB een notificatieverzoek indienen, waarna de dienstverlener, via een Europees paspoort, ook in het buitenland actief kan zijn, omdat de vergunning geldt binnen elke lidstaat van de EU.

Ook Nederland had de verplichting PSD2 op 13 januari 2018 te implementeren in de Nederlandse wetgeving. In Nederland liep de implementatie echter vertraging op en daarom is de wetgeving ter implementatie van PSD2 in Nederland uiteindelijk pas op 19 februari 2019 in werking getreden.

PSD2 is -qua implementatie- een complexe wetgeving gebleken, zowel vanuit het oogpunt van regelgeving, technologie als toezicht. Zo was lange tijd niet duidelijk hoe de wisselwerking tussen artikel 94(2) van PSD2 en de AVG op het gebied van persoonsgegevens was geregeld. Met name de afstemming van het toezicht over het vereiste van de uitdrukkelijke toestemming van betaaldienstgebruikers, voor de toegang tot verwerking van persoonsgegevens die nodig is voor het verlenen van betaaldiensten, heeft veel tijd gekost. Reden hiervoor was het bestaan van onduidelijkheid (ook bij andere lidstaten) over de interpretatie van het gelijkluidende begrip 'uitdrukkelijke toestemming;' in artikel 94(2) PSD2. Nadat uit discussies op Europees niveau bleek dat met dit begrip niet hetzelfde werd bedoeld als hetzelfde begrip in de AVG[24], werd duidelijk dat de naleving van dit vereiste in Nederland in beginsel onder toezicht van DNB kwam. Dit werd vanwege de wisselwerking met de AVG als een te complexe rolverdeling gezien. Daarom is besloten dit toezicht in Nederland bij de AP te beleggen, die de meest passende expertise heeft om toezicht op betaaldienstverleners uit te oefenen met betrekking tot de uitdrukkelijke toestemming voor toegang van betaaldienstverleners tot de betaalgegevens van betaaldienstgebruikers. Om dit onder toezicht van de AP te brengen was echter nog een aparte wetswijziging vereist van de Uitvoeringswet AVG, waarin dit onderdeel expliciet onder toezicht van de AP werd gebracht. Hierop werd ook de concepttekst van het

23 Nederland rondde de transpositie van de Europese richtlijn in Nederlandse wetgeving in februari 2019 af.
24 EDPB letter regarding the PSD2 directive, https://edpb.europa.eu/news/news/2018/letter-regarding-psd2-directive_en

wetsvoorstel aangepast en kon de verdere onderlinge afstemming van de toezichttaken tussen de verschillende toezichthouders plaatsvinden. Op 21 februari 2019 ondertekenden DNB en de Autoriteit Persoonsgegevens (AP) een samenwerkingsprotocol dat als doel had om effectief en efficiënt toezicht te houden op de PSD2. Beide toezichthouders beogen hiermee de kwaliteit van het toezicht te bevorderen waar raakvlakken zijn in de toezichtstaken. Begin 2018 hadden de betrokken toezichthouders op de PSD2 (DNB, ACM, AFM en AP) al een taskforce opgericht met als doel om de doelmatigheid van het toezicht rondom PSD2 te borgen door het maken van concrete samenwerkingsafspraken en zoveel mogelijk duidelijkheid te scheppen voor sector en consument en daar waar het toezicht elkaar raakt gezamenlijke communicatieafspraken te maken. Deze taskforce spreekt ook met verschillende marktpartijen.

Om marktpartijen behulpzaam te zijn bij de implementatie van de regelgeving hebben gedurende het implementatieproces zowel de EBA als DNB vragen vanuit de markt verduidelijkt via Q&A's op hun websites. Ook heeft DNB diverse voorlichtingsbijeenkomsten georganiseerd. Daarnaast kwam de *European Data Protection Board* (EDPB) in haar richtsnoeren over het samenspel van de PSD2 en de AVG van 15 december 2020 met nadere duiding over een aantal begrippen in de PSD2 en de toepasselijkheid van begrippen in de AVG.[25]

Ondanks het complexe traject, dat de wetgeving met zich meebracht, is de implementatie, relatief gezien, betrekkelijk efficiënt en effectief verlopen. Dit is mede toe te schrijven aan het overleg over de collectieve (niet-concurrentiële) aspecten tussen alle betrokkenen in het Maatschappelijk Overleg Betalingsverkeer (MOB) voor de aanbod- en vraagzijde en het zogenoemde NISP-NL-overleg (aanbodzijde), onder auspiciën van de Betaalvereniging, tussen banken, derde partijen en overige belanghebbenden, waarbij DNB als waarnemer aanwezig was. Dit is mede toe te schrijven aan de taskforce van de vier toezichthouders.

In het NISP-NL-overleg, waarover de ACM vooraf was geïnformeerd, konden deelnemers onder meer onduidelijkheden in de regelgeving, rond de gehanteerde API-specificaties van de zogenaamde "Berlin Group", die de meeste banken hanteerden, en de testplannen, die op grond van de RTS verplicht waren, bespreken. Naast de banken vervulde een aantal derde partijen (potentiële vergunninghouders voor de nieuwe diensten) in dit overleg een belangrijke rol, hetgeen bijdroeg aan een snelle feedback tussen de deelnemers. DNB was als toehoorder bij dit overleg betrokken en gaf uitleg over de eisen en het proces die DNB-toezicht stelde aan de individuele banken voor onder meer de vrijstelling van de implementatie van de uitwijkvoorziening ('fall-back') via de consumenteninterface[26]. DNB-toezicht heeft de API's van de banken die een ontheffing hebben aangevraagd en de werking daarvan in de praktijk voor 14 september 2019 beoordeeld en daarover een (individuele) opinie verstrekt, al dan niet leidend tot een besluit tot een ontheffing tot eind 2020 voor de verplichting van het aanbieden van een uitwijkvoorziening. Eind 2020 zijn de API's opnieuw beoordeeld in het licht van de intussen opgedane ervaring.

In het MOB zijn, met name door consumentenorganisaties en organisaties van kwetsbare groepen, zorgen geuit rond de veiligheids- en privacyaspecten van de regelgeving. Op basis hiervan heeft het MOB de voorkeur

---

25 Uiteindelijk publiceerde de EDPB pas in 2020, dus na de invoering van PSD2 richtlijnen die dit verduidelijkten, zie Guidelines 06/2020 on the interplay of the Second Payment Service Directive and the AVG, Version 2 15 December 2020 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf

26 Toegang via de consumenteninterface wordt ook wel screenscraping genoemd. De derde partij maakt hierbij gebruik van de inloggegevens van de consument en logt vervolgens in op de internetbankieromgeving van de consument. Hiermee krijgt de derde partij toegang tot en zicht op alle transactiegegevens van de consument. Onder de RTS is dit alleen toegestaan via identificatie van de derde partij. Het MOB sprak dan ook een duidelijke voorkeur uit voor dedicated (API-) interfaces, zodat de consument meer " in control" is en de veiligheid en privacy van de rekeninggegevens van de consument bovendien beter gewaarborgd zijn.

onderschreven voor API-interfaces (boven de relatief onveilige en privacy onvriendelijke screenscraping-methode) voor veilige toegang tot de rekening. De meeste banken hebben deze dan ook geïmplementeerd, zij het niet geheel geharmoniseerd, ondanks het gebruik van de "Berlin-Group"-specificaties[27]. Ook heeft het MOB (ondersteund door de minister van Financiën) de banken verzocht hun klanten via de online-bankierenomgeving een overzicht aan te bieden van de toestemmingen die zij hebben verleend voor toegang tot de betaalrekening. Hoewel het blokkeren van toegang van alle derde partijen via dit dashboard volgens een Q&A van EBA niet is toegestaan, is het wel mogelijk dat consumenten via het dashboard van hun bank de toestemming die men aan een derde partij gegeven heeft, kunnen intrekken.

In maart 2019, vlak na de inwerkingtreding van de PSD2, startte DNB namens het MOB een voorlichtende publiekscampagne over de PSD2: "PSD2 Bankieren, Nieuwe mogelijkheden, U beslist". Uit de evaluatie van de campagne, later dat jaar, bleek dat de campagne had bijgedragen aan de kennis van het publiek van de PSD2, maar niet aan de waardering en acceptatie daarvan. Zes op de tien consumenten hadden er na de campagne nog steeds geen vertrouwen in dat "PSD2-bankieren" veilig is. DNB constateert in het Jaarverslag van het MOB over 2019 "dat het overgrote deel van de Nederlandse bevolking er nog niet aan toe is om in dat kader toegang te verlenen aan een derde partij".

Voorts heeft het MOB op verzoek van met name consumentenorganisaties '*good practices*' opgesteld rond transparantie over rekeninginformatiediensten. Dit met als doel dat consumenten en ondernemers het verzoek voor toegang op een eenduidige manier kunnen beoordelen. Vanwege de mededingings- en privacyaspecten waren bij uitwerking van de "*good practices*" de ACM en AP betrokken. In mei 2020 stemde het MOB in met deze *good practices*, die zeven vragen bevatten en riep rekeninginformatiedienstverleners op deze vragen bondig en begrijpelijk richting de gebruiker te beantwoorden voorafgaand aan het moment dat de gebruiker toestemming geeft voor toegang tot zijn betaalrekening. Het MOB zal de toepassing hiervan monitoren en heeft de desbetreffende MOB-werkgroep dan ook gevraagd hierover in 2022 te rapporteren.[28]

Daarnaast heeft Privacy First in juli 2019 een PSD2-me-niet-register opgezet, dat een vervolg heeft gekregen in een PSD2-me-niet-filter[29]. Doel hiervan is consumenten de mogelijkheid te bieden bijzondere (persoonsgevoelige) gegevens te filteren om te voorkomen dat banken deze delen met derde partijen. Ook kunnen consumenten kiezen voor een volledige opt-out. Banken mogen, op grond van de PSD2, een dergelijke volledige *opt-out* niet actief aanbieden aan hun klanten.

Sluitstuk van de PSD2 invoering was het doorvoeren van sterke klantauthenticatie voor online betalingen. Bij iDEAL is deze veiligheidseis het uitgangspunt en zijn consumenten hier al jaren aan gewend, maar bij het gebruik van creditcards is dit niet vanzelfsprekend. Om de markt meer tijd te geven, heeft de EBA halverwege 2019 voor online kaartbetalingen een aanvullende aanpassingstijd van 14 maanden toegezegd. Partijen moesten per 1 januari 2021 ook voor deze betalingen volledig voldoen aan de RTS. Net als in andere landen pleitten ook in Nederland betaaldienstverleners en webwinkeliers voor verder uitstel. Achtergrond hiervan was de vrees voor omzetverlies bij webwinkeliers, als de bank van de consument – op de einddatum - de dubbele beveiliging zou aanzetten terwijl de webwinkelier op die datum nog niet gereed zou zijn met de implementatie. Betalingen worden in zo'n situatie afgewezen. De EBA (en ook DNB) hebben niet aan verder uitstel van deze veiligheidseisen toegegeven. In

27 De PSD2 is technologieneutraal en schrijft geen harmonisatie voor. Ondanks dat de meeste banken gebruikmaken van de API-specificaties van de "Berlin Group", een Europees samenwerkingsorgaan, bestaan er verschillen in de precieze toepassing daarvan.

28 Zie MOB rapportage 2020, p.6, https://www.dnb.nl/media/wvrbahrb/mob_jaarverslag_2020.pdf

29 https://psd2meniet.nl

het Verenigd Koninkrijk, waar webwinkels voor hun betalingen aanzienlijk sterker afhankelijk zijn van creditcards, heeft de *Financial Conduct Authority* de markt een verder uitstel verleend tot 14 maart 2022.

Om de migratie in Nederland in goede banen te leiden heeft de Betaalvereniging samen met relevante marktpartijen een migratieproject ingericht. Doel hiervan was een zo soepel mogelijke invoering van dubbele beveiliging bij online creditcards. Het bestond onder meer uit een graduele invoering van *soft-blockades* om te testen hoeveel uitval dit zou veroorzaken. Dit bleek toch moeizamer te verlopen dan verwacht. Het traject werd begin 2021 afgerond. DNB was als toezichthouder betrokken bij de desbetreffende aanpassingen van de individuele betaaldienstverleners.

PSD2 richt zich niet op de huidige dienstverlening van Big Techs in het betalingsverkeer. Big Techs vallen vanwege de huidige vormgeving van hun dienstverlening niet onder de reikwijdte van PSD2. Zij bieden namelijk *technische diensten* aan en niet rechtstreekse betaaldiensten. De ACM (2020) constateert in het onderzoek naar Big Techs in het betalingsverkeer dat het mogelijk is dat Big Techs de doelstellingen van de PSD2 ondermijnen, bij een verdere uitbouw van hun positie in de markt. Eén van de beleidsopties die ACM (2020) in haar rapport noemt is de PSD2 zodanig aan te passen dat betaaldienstverleners toegang krijgen tot de "technische schil" van de desbetreffende Big Techs. De ACM adviseert deze beleidsoptie te betrekken bij de nationale en Europese evaluatie van PSD2 [30].

[30] ACM-studie: Big Techs in het betalingsverkeer | ACM.nl

3 Markt voor betaaldiensten

Hoe is de markt voor betaaldiensten veranderd door de introductie van PSD2?

3.1 Concurrentie

Onderzoeksvragen

1. Is het aanbod van betaaldiensten veranderd in Nederland door PSD2 en wat heeft dat voor effect gehad op de concurrentie?
2. Verloopt toegang tot de betaalrekening en transactiedata op non-discriminatieve wijze?
3. Hoe verloopt toegang tot betalingssystemen, met name rekening houdend met de mate van concurrentie (108 lid c)**
4. Wat zijn de gevolgen voor de marktverhoudingen (concurrentie, diversiteit, monopolies, marktmacht)?
5. Is het voldoende duidelijk welke betaalinstrumenten er wel en niet onder het verbod op *surcharging* vallen?

Is het aanbod van betaaldiensten veranderd in Nederland door PSD2 en wat heeft dat voor effect gehad op de concurrentie?

Als we kijken naar de verandering van het aanbod van (nieuwe) betaaldiensten 7 en 8 door PSD2, is het belangrijk om onderscheid te maken tussen het doen van betalingen (dienst 7: betaalinitiatiediensten) en het gebruik van informatie op basis van betaaldata (dienst 8: rekeninginformatiediensten). Een tweede relevant onderscheid is dat tussen diensten gericht op bedrijven en diensten gericht op consumenten. In Nederland zijn in het register[31] van DNB 24 aanbieders van betaaldiensten geregistreerd (waarvan 23 actief), 9 met vergunning 8 en 15 met vergunning 7&8. Daarvan zijn er 6 gericht op consumenten (B2C), 16 op bedrijven (B2B), 1 op zowel B2B als B2C en over 1 (inactief[32]) bedrijf is geen informatie bekend, zie Bijlage D. Ook heeft een groot aantal buitenlandse bedrijven een *passporting* vergunning voor Nederland. Dit komt later in dit hoofdstuk aan de orde.

Als het gaat om het doen van betalingen is er voor consumenten in Nederland nauwelijks iets veranderd door invoering van PSD2. Er zijn geen nieuwe betaaldiensten voor consumenten op de markt gekomen en consumenten zijn niet op een andere manier gaan betalen. In Nederland was online betaalmethode iDEAL al breed geaccepteerd en gebruikt door consumenten, waardoor de consumentenbehoefte voor nieuwe, op PSD2 gebaseerde, betaaloplossingen beperkt was. Tijdens corona groeide iDEAL naar een totaal 890 miljoen betalingen in 2020. Dit was een toename van 34 procent ten opzichte van 2019. Tegelijkertijd nam de totale omzet toe met 31 procent naar € 70 miljard in 2020.[33]

Als het gaat om de mogelijkheid om rekeninginformatiediensten te gebruiken, is er meer veranderd voor consumenten. Er is een aantal nieuwe aanbieders van diensten opgekomen zoals huishoudboekjes die een overzicht van uitgaven voor consumenten bieden, mogelijkheden om geautomatiseerd kleine bedragen te beleggen, mogelijkheden om aan budgetbeheer te doen, hulp bij het opzeggen van abonnementen of het verstrekken van leningen op basis van een geautomatiseerde inschatting van kredietwaardigheid. Onderstaande box geeft een aantal

31 Geraadpleegd op 05-07-2021
32 Is op 29-04-2021 in staat van faillissement verklaard.
33 https://www.ideal.nl/actueel/nieuws/explosieve-groei-van-ideal-in-coronajaar-2020/

voorbeelden van zowel B2B- als B2C-partijen (zowel van rekeninginformatiedienstverleners als betaalinitiatiedienstverleners).

Hoe FinTechs PSD2 gebruiken.

FinTechs zijn bedrijven die financiële diensten combineren met innovatieve technologie. Ze zijn moderne aanvullingen dan wel alternatieven voor traditionele banken, vermogensbeheerders en verzekeraars. Hieronder noemen we vier voorbeelden van dergelijke bedrijven en hun diensten.

Voorbeeld 1
Verzekeringsmaatschappij ASR werkt samen met de rekeninginformatiedienstverlener Ockto. Met 'Ik denk vooruit' kan een klant via ASR een overzicht maken hoe hij/zij er financieel voorstaat en wat nodig is om financiële doelen haalbaar te maken. Gegevens die hiervoor nodig zijn kunnen handmatig worden ingevoerd op de website, of via de Ockto-app. Via de Ockto-app geeft een consument toestemming dat Ockto zijn of haar data van de betaalrekening, bij het UWV, de Belastingdienst en mijnpensioenoverzicht.nl mag gebruiken om berekeningen te maken. Hierdoor hoef de klant zelf niet meer handmatig de gegevens in te voeren.

Voorbeeld 2
Klarna is een internationaal bedrijf van Zweedse origine dat zich richt op betalingen en in Nederland een vergunning heeft als betaalinstelling. Klarna gebruikt PSD2 voor toegang tot de betaalrekening om haar dienstverlening aan klanten mogelijk te maken. Voordat PSD2 van kracht werd, gebruikte zij daarvoor zogenoemde screenscraping. Het bedrijf opereert als betaalplatform dat probeetr bedrijven en klanten bij elkaar te brengen, waarbij ze klanten de mogelijkheid tot achteraf betalen biedt.

Voorbeeld 3
Mijngeldzaken biedt een huishoudboekje waarmee consumenten inzicht kunnen krijgen in hun inkomsten en uitgaven. Transacties worden gecategoriseerd, zodat consumenten een beeld krijgen hoe ze hun inkomen besteden, wat hun vaste lasten zijn, en wat de bestedingsruimte is binnen hun budget. De app biedt ook de mogelijkheid om vooruit te plannen en om bonnetjes te koppelen aan transacties.

Voorbeeld 4
Bizcuit is een bedrijf dat boekhoud- en salarispakketten van bedrijven koppelt aan bankrekeningen bij banken. Op basis van deze koppeling hebben zij een app ontwikkeld waarmee ondernemers mobiel kunnen bankieren, en facturen en bonnen kunnen ontvangen, factureren en direct betalen. Op deze manier kunnen bedrijven al hun administratieve gegevens centraal op één plek beheren en inzien.

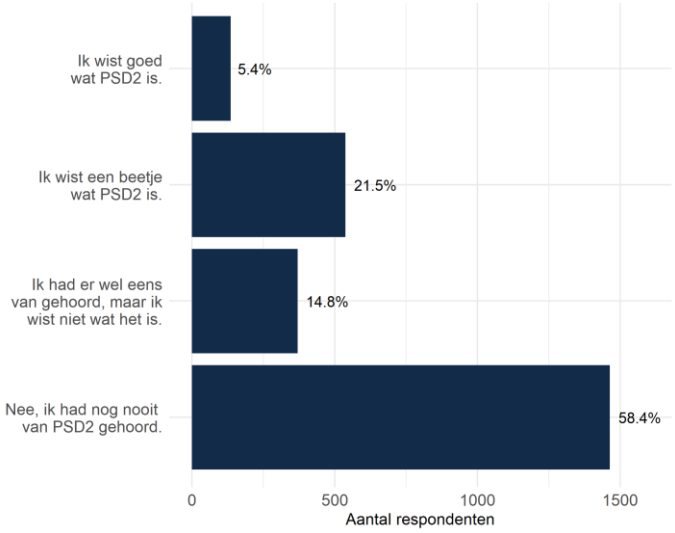
Consumenten gebruiken zowel rekeninginformatie- als betaalinitiatiediensten echter relatief weinig.
Figuur 3.1 laat zien dat bijna 60 procent van de consumenten niet weet wat PSD2 is. De nieuwe diensten uit PSD2 zijn dan ook beperkt bekend bij consumenten of worden niet als zodanig herkend door consumenten. Ook geeft slechts circa 10 procent aan ooit gebruik te hebben gemaakt van rekeninginformatie- en/of betaalinitiatiediensten (Figuur 3.2). Het werkelijke gebruik kan anders zijn dan aangegeven, omdat consumenten niet goed weten wanneer wel en wanneer niet sprake is van een PSD2 dienst 7 of 8. Voor bedrijven geldt dat het aanbod van betaaldiensten in grotere mate veranderd is omdat er een aantal nieuwe aanbieders van betaaldiensten actief is geworden waar bedrijven gebruik van kunnen maken (Figuur 3.3).

Sommige gesprekspartners uit de markt en belangenorganisaties stellen dat PSD2 niet direct aansluit op een behoefte van consumenten maar dat het vanuit het perspectief van potentiële aanbieders is ontworpen. Een consumentenorganisatie geeft aan dat PSD2 vooral de wens was van fintechpartijen, maar dat er voor de toegevoegde waarde voor consumenten beperkt aandacht was. Een aanbieder vraagt zich af of er überhaupt wel een markt is voor diensten in het B2C-segment in Nederland.

De grotere betaalinitiatiedienstverleners zijn vooral PSP's met een vergunning in een andere lidstaat, die voorheen zonder toestemming van banken via screenscraping de account van klanten benaderden, denk hierbij aan Sofort, Klarna en Trustly, en in feite concurreren met iDEAL. Het aantal maandelijkse transacties van deze partijen is in Nederland relatief beperkt volgens gesprekspartners. Bedrijven maken over het algemeen nog steeds gebruik van de traditionele aanbieders voor betaaldiensten. We hebben echter geen gegevens over marktaandelen.

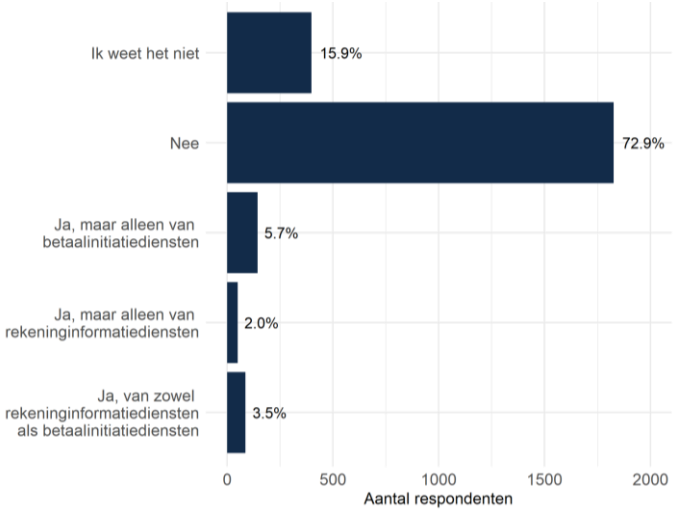
Hoewel in de consumentenenquête meer mensen aangeven dat ze van betaalinitiatiediensten gebruik hebben gemaakt, melden gesprekspartners dat consumenten en bedrijven rekeninginformatiediensten in de dagelijkse praktijk het meest gebruiken. Hier ontvangen volgens hen banken de meest API-calls. In het begin waren dit vooral banken onderling, waarbij klanten van de ene bank hun gegevens bij andere banken ophaalden. Volgens gesprekpartners valt het in de praktijk tegen hoeveel klanten bij een bank gebruikmaken van de mogelijkheid om via de app van die bank toegang tot betaalrekeningen bij andere banken te krijgen. Inmiddels zijn er ook meer calls van derde partijen, zoals van zogenaamde *aggregators*.

Figuur 3.1 Wist u voor u deze vragenlijst invulde wat PSD2 was?



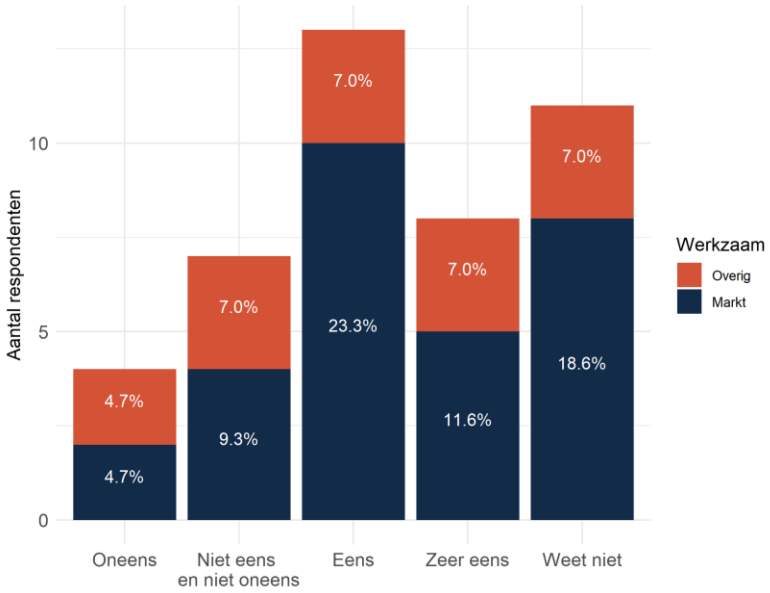
Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2508

Figuur 3.2 Hebt u wel eens gebruikgemaakt van rekeninginformatiediensten of betaalinitiatiediensten?



Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2506

Figuur 3.3 Stelling: De meest succesvolle toepassingen van PSD2-betaalinitiatiediensten en rekeninginformatiediensten richten zich op bedrijven



Bron: SEO Economisch Onderzoek op basis van een mini-enquête onder 43 interviewpartners

Voor de komst van PSD2 boden de grote aanbieders van administratieve softwarepakketten de mogelijkheid aan bedrijven om directe koppelingen met betaalrekeningen in te bouwen, om zo het administratieve proces bij bedrijven te optimaliseren. De aanbieders hadden daarvoor bilaterale contracten met banken. De uitwisseling van gegevens verliep via geïndividualiseerde systemen waarbij bijvoorbeeld CSV-files met rekeningnummers werden uitgewisseld. Uit interviews met gesprekspartners komen twee gevolgen van de invoering van PSD2 naar voren. Ten eerste is het door PSD2 ook voor kleinere spelers mogelijk geworden om dergelijke diensten aan te bieden. Banken wilden voor PSD2 met hen geen bilaterale contracten afsluiten omdat dit te veel administratieve lasten met zich meebracht. PSD2 verplichtte banken hen ook (gratis) toegang te geven, als ze over de juiste PSD2-vergunning beschikten. Denk daarbij aan Cobase en Bizcuit die treasurydiensten verlenen aan bedrijven. Figuur 3.7 laat de opkomst van Nederlandse bedrijven met PSD2-vergunning zien. Een tweede gevolg van de invoering van PSD2 is dat bestaande diensten (bijvoorbeeld gerelateerd aan de boekhouding en betalen van salarissen) via een ander technisch kanaal gaan lopen omdat zij gebruikmaken van de API's die banken hebben ontwikkeld. Dit leidt tot standaardisatie en meer efficiëntie bij aanbieders van administratieve softwarepakketten (zij het wel dat de API's per bank verschillen). Over het algemeen geven gesprekspartners aan dat PDS2 in Nederland nog niet heeft geleid tot diensten die anders of veel efficiënter zijn dan reeds bestaande diensten.

De opkomst van zogeheten *aggregators* is een andere ontwikkeling die gesprekspartners noemen. Dit zijn ondernemingen met een PSD2-vergunning die API-interfaces hebben ontwikkeld voor veel verschillende banken en tussen de TPP en de bank in gaan zitten. Voorbeelden van *aggregators* zijn de Nederlandse Invers en Plaid, het Spaanse Salt Edge en het Britse TrueLayer. Als een onderneming diensten aan klanten wil aanbieden op basis van betaaldata, en ze wil dat doen aan de hand van toegang tot betaalrekeningen zoals PSD2 dat mogelijk maakt, dan kan zo'n onderneming ervoor kiezen om dat via een *aggregator* te doen. Dit heeft twee voordelen voor de betreffende onderneming. Ten eerste hoeft de onderneming zelf mogelijk geen PSD2-vergunning aan te vragen. Omdat het

aanvragen van zo'n vergunning geld en tijd kost, en daarnaast doorlopende compliance-activiteiten met zich meebrengt, bespaart gebruikmaken van een *aggregator* kosten. Ten tweede bespaart het ook software ontwikkelkosten, omdat betaaldienstverleners (TPPs) de API's niet meer zelf hoeven te ontwikkelen en bijhouden, dat doen de *aggregators* immers.

Conclusie

- Het beeld in de markt, bij consumentenorganisaties en bij toezichthouders is dat het gebruik van PSD2-diensten nog beperkt is, zowel bij bedrijven als bij consumenten. Er is geen concreet cijfermateriaal over gebruik of marktaandelen uit publieke bron beschikbaar.
- Gesprekspartners geven aan dat PSD2 in Nederland nog niet heeft geleid tot diensten die anders of veel efficienter zijn dan reeds bestaande diensten. Dit is ook gerelateerd aan de hoge mate van efficiëntie van het Nederlandse betalingsverkeer.
- Wel heeft PSD2 ertoe geleid dat er meer – uit andere lidstaten afkomstige - aanbieders van betaalinitiatiediensten op de markt zijn, zowel voor consumenten als voor bedrijven. Ook zijn er nieuwe diensten ontstaan op basis van betaalrekeninginformatie.
- Daarnaast kunnen kleine partijen op de markt voor administratieve software, die voorheen geen bilateraal contract met banken konden krijgen, nu ook directe koppelingen met de betaalrekening van banken aanbieden op basis van PSD2-toegang.
- Een bijkomend gevolg van PSD2 is de opkomst van *aggregators*, die fricties in de markt verminderen, door compliancekosten en ontwikkelkosten te centraliseren.
- We concluderen dat PSD2 de concurrentie heeft vergroot, zij het beperkt. Daarbij is een belangrijke kanttekening dat de wet nog maar relatief kort van kracht en de markt nog sterk in ontwikkeling is.

Verloopt toegang tot de betaalrekening en transactiedata op non-discriminatieve wijze?

De PSD2-richtlijn legt een non-discriminatieverplichting op aan banken in artikel 66 en 67 PSD2.[34] Dit betekent dat banken derde partijen niet anders mogen behandelen – bijvoorbeeld qua mogelijkheden, termijn en voorrang – dan wanneer de klant zelf om deze informatie of dienst zou vragen. Toegang tot (de gegevens van) online betaalrekeningen kan alleen worden ontzegd op basis van objectieve redenen. Een bank die toegang ontzegt, dient hiervan melding te maken bij DNB. Omdat het recht op toegang een recht is van de rekeninghouder, zou de rekeninghouder bij de AFM ook terecht kunnen met klachten als een bank hem of haar de mogelijkheid ontzegt om van dat recht gebruik te maken.

De invulling van de toezichthouders bestaat uit een proces van goedkeuring voor de API's van banken. De API moet aan dezelfde eisen wat betreft beschikbaarheid en functionaliteit voldoen als de klantinterface, anders mag de TPP gebruikmaken van de zogeheten uitwijkvoorziening ('fall-back') voor de klanteninterface. Banken kunnen een uitzondering krijgen voor het bieden van deze uitwijkvoorziening. Eisen zijn onder meer dat de API aan een aantal kwaliteits- en beschikbaarheidseisen voldoen als TPP voldoende betrokken waren bij het ontwerp- en testproces van de API's.[35] Ook is er de eis van een obstakelvrije klantreis. Banken mogen niet onnodige stappen inbouwen om de toegang onaantrekkelijk te maken. Een obstakelvrije klantreis voor betaalinitiatie- en rekeninginformatiediensten bestaat onder meer uit eisen over de wijze waarop de authenticatie verloopt, welke informatie de dienstverlener biedt en hoe.[36]

---

34 Art. 66 lid 4 (c) en 67 lid 3 (b) PSD2

35 Zie de EBA guidelines the exemption from the fall back mechanism under the RTS on SCA and CSC.

36 Zie DNB Q&A Een obstakelvrije klantreis voor betaalinitiatie- en rekeninginformatiediensten via een speciale interface op basis van redirection

Partijen met een vergunning krijgen in de praktijk meest toegang via de door DNB goedgekeurde API's. Dit geldt voor alle derde partijen die gebruik willen maken van toegang tot de betaalrekening via PSD2 goedgekeurde dienstverlening. In die zin verloopt de toegang op non-discriminatieve wijze. Ook aspecten als storingsgevoeligheid zijn gereguleerd.

We hebben in de interviews met marktpartijen en toezichthouders DNB en AFM geen indicaties gekregen dat er sprake zou zijn van non-compliance door banken met de eisen die de toezichthouder stelt aan de API's.[37] Marktpartijen die specifiek gebruikmaken van API's noemen in gesprekken onder meer:

- Het gebrek aan controle van de TPP over de klantreis, bijvoorbeeld omdat goedkeuring plaatsvindt via remote access in de klantomgeving van de bank, waarbij de gebruiker nog regelmatig twee keer door een SCA heen moeten, één keer om in te loggen in de bankomgeving en één keer om goedkeuring te geven. Echter, onderdruk van onder andere een Q&A van DNB en een *'Opinions on Obstacles'* van de EBA komt twee keer SCA (inloggen en bevestigen) in Nederland sinds medio 2021 minder vaak voor;
- Discussie tussen TPP's en banken over welke toegang tot data banken wel en niet onder PSD2 zouden moeten leveren. Sommige typen betaalrekeningen vallen bijvoorbeeld in Nederland niet onder PSD2, terwijl die betaalrekeningen in andere Europese landen wel onder PSD2 vallen. Deze signalen zijn bij de AFM bekend;
- Enkele partijen klagen over de snelheid waarmee banken problemen met API's oplossen. Ze geven voorbeelden waarbij gebruikers met de algemene helpdesk van banken bellen, die vervolgens niet weten of begrijpen waar de vraag over gaat, of voorlichting krijgen over betaalproducten van een bank zelf.

Aanbieders van API's geven aan dat ze veel aandacht hebben besteed aan documentatie. In het ontheffingsproces voor het onderhouden van een uitwijkvoorziening (de fall-back) is door partijen ook veel informatie aangeleverd aan DNB hierover. Gegeven de ingrijpende aard van de verandering en de zoektocht naar de precieze interpretatie van de RTS is het proces volgens aanbieders relatief soepel verlopen. Het goed werkend krijgen van API's vereist volgens hen veel communicatie tussen technische experts van de verschillende instellingen. Dat was in het begin vaak zoeken en leidde soms tot fricties, maar inmiddels weten mensen elkaar beter te vinden, vooral als het gaat om grootgebruikers van de API-interfaces.

Voor toegang tot de betaalrekening mogen banken geen kosten in rekening brengen.[38] Een ander punt wat gesprekspartners als gevolg hiervan noemen, is dat gratis toegang de prikkels voor banken om te blijven investeren in de betaalinfrastructuur vermindert (zie ook Bijlsma, Bolt & Jonker, 2021). Zowel het bouwen en onderhouden van API's als het doorontwikkelen van de betaalinfrastructuur vragen om investeringen. Omdat banken toegang gratis moeten verstrekken, kunnen zij die investeringen niet terugverdienen. Daardoor hebben ze minder prikkels om te investeren in de kwaliteit van toegang, zo luidt het argument. Andere partijen brengen hier tegenin dat klanten van banken met een betaalrekening al betalen voor die rekening en dat tarifering van derde partijen tot dubbel beprijzen zou leiden. Daarnaast noemen marktpartijen dat de wettelijk gemandateerde toegang tot een *unlevel playing field* zorgt vis-a-vis bijvoorbeeld Big Techs??, waarbij Big Techs middels de bepalingen in PSD2 wel toegang kunnen krijgen tot betaaldata bij banken, en deze data kunnen combineren met andere gegevens over de consumenten

37 OK IT heeft in 2020 bij de ACM een handhavingsverzoek ingediend tegen ING, de Rabobank, de Volksbank en ABN Amro. Deze banken zouden volgens OK IT de Mededingingswet overtreden door OK IT de toegang te weigeren tot hun betalingssystemen en betaalrekeningen. OK IT wilde zelf de SCA uitvoeren, terwijl banken alleen SCA via een redirect toestaan. De ACM heeft dit verzoek afgewezen omdat OK IT niet over een vergunning van DNB beschikte om PSD2-diensten uit te voeren en het derhalve niet doelmatig en doeltreffend is het handhavingsverzoek in behandeling te nemen. Zie ACM/20/042562 Besluit afwijzing handhavingsverzoek OK IT.

38 Artikel 66 lid 5 PSD2 en artikel 67 lid 4 PSD2.

die de Big Techs hebben, maar banken andersom geen toegang hebben tot de gegevens van Big Techs. Dit kan tot een concurrentienadeel voor banken leiden. Dit is ook een punt dat de ACM (2020) in haar Big Tech-studie naar voren heeft gebracht.

Conclusie

- Hoewel een deel van de gesprekspartners in de mini-enquête aangeeft zorgen te hebben over mate waarin toegang op non-discriminatieve wijze plaatsvindt, documenteert dit onderzoek geen signalen voor non-compliance met dit vereiste;
- Toezichthouders hebben eisen voor ontheffing van de verplichting een uitwijkvoorziening aan te bieden, vastgesteld en aangegeven wanneer sprake is van een obstakel voor de klantreis;
- Daarmee zijn de randvoorwaarden voor toegang op non-discriminatieve wijze gecreëerd;
- Dat banken derde partijen geen kosten in rekening mogen brengen voor toegang tot de betaalrekening kan de prikkels van banken voor investeringen hun betaalinfrastructuur verminderen. Ook vermindert het de prikkel om te investeren in de kwaliteit van de toegang voor diensten 7 & 8.

Hoe verloopt toegang tot betalingssystemen, met name rekening houdend met de mate van concurrentie?
PSD2 bepaalt dat deelnemers aan een betalingssysteem andere betaaldienstverleners op objectieve, evenredige en niet-discriminerende wijze toegang verstrekken tot het betalingssysteem en dat banken ervoor zorgen dat betaalinstellingen op een objectieve, niet-discriminatoire en evenredige wijze toegang hebben tot een betaalrekening.[39] PSD2 beoogt hiermee betaalinstellingen te faciliteren. Dit is een nieuwe categorie van niet-bancaire partijen die met een aparte vergunning betaaldiensten kunnen verlenen. Om deze partijen daartoe in staat te stellen, reguleert PSD2 de toegang voor deze betaalinstellingen tot de betalingssystemen. Dit kan op twee manieren. Een betaalinstelling kan of rechtstreeks toegang krijgen tot betaalsystemen (artikel 35 PSD2/5:88 Wft) of indirect via het openen van een zakelijke betaalrekening bij een bank (artikel 36 PSD2/5:88a Wft). De ACM ziet toe op naleving van beide bepalingen. Als banken toegang van een betaalinstelling tot de betaalrekeningen weigeren of een bestaande bankrelatie met een betaalinstelling opzeggen, moeten ze dat melden bij de ACM. De ACM kan controleren of de toetsing van de bank op objectieve, evenredige en niet-discriminerende wijze heeft plaatsgevonden. Het betreft hierbij open normen, waarbij toetsing op basis van dossiervorming plaatsvindt. Als de ACM vaststelt dat er geen goede gronden zijn om toegang te weigeren of opzeggen, bijvoorbeeld omdat partijen categorisch uitgesloten worden in plaats van op basis van een individuele beoordeling, kan ze actie ondernemen, waaronder een last onder dwangsom of een bestuurlijke boete. Voor zover bekend is dit in de praktijk niet voorgekomen.

Partijen waar de ACM toezicht op houdt in het kader van artikel 5:88a Wft zijn betaalinstellingen die voldoen aan de vereisten uit artikel 1:1 Wft en artikel 2:3a Wft. Een voorbeeld daarvan zijn partijen die grensoverschrijdende betalingen aanbieden en dergelijke betalingen willen faciliteren op een kostentechnisch aantrekkelijke manier. De klanten van dit type betaalinstellingen zijn in geval van dienst 6 bijvoorbeeld arbeidsmigranten. Deze betaalinstellingen ondervinden in de praktijk volgens gesprekspartners soms problemen bij het openen van een betaalrekening bij een bank.

Eén van de achterliggende oorzaken dat betaalinstellingen moeite hebben om een betaalrekening te openen, is dat banken in lijn met de Wwft eisen stellen aan de klanten aan wie ze een betaalrekening verlenen en dat banken

[39] Art. 35, 36 PSD2, geïmplementeerd in artikelen 5:88 (toegang tot betalingssystemen) en 5.88a (toegang tot betaalrekeningdiensten) Wft. De Europese Commissie moet over de marktontwikkelingen op dit vlak rapporteren aan het Europees Parlement, Artikel 108, lid c van de PSD2.

daarbij *derisken*.[40] Banken nemen daarbij afscheid van klanten omdat het risico van de sector waarin de klant opereert, hoog is. Hier speelt dat de Wwft strenge eisen stelt aan banken die hen terughoudend maakt met het verstrekken van betaalrekeningdiensten aan betaalinstellingen. Hierbij is sprake van een afruil tussen concurrentie (doordat meer partijen actief worden) en financiële inclusie enerzijds en eisen rondom AML en CTF die tot doel hebben risico's in te perken anderzijds.[41]

Neem een betaaldienstverlener met veel klanten in de boeken die door DNB en banken als hoog risico worden gepercipieerd, zoals goksites, massagesalons en adult entertainment. Als zulke partijen aankloppen bij een bank zal deze mogelijk geneigd zijn toegang te weigeren omdat deze partijen gezien worden als risicovolle partijen vanuit witwasperspectief. *Derisking* leidt ertoe dat sommige betaalinstellingen veel moeite ervaren bij het verkrijgen van een betaalrekening (en daarmee indirect bij de toegang tot de betalingssystemen) bij banken. Sommige gesprekspartners stellen dat de oorzaak hiervan ligt in de omstandigheid dat banken *overcompliant* zijn met betrekking tot AML-eisen. Banken mogen categorieën klanten op voorhand niet uitsluiten en moeten de toegang tot een betaalrekening door een betaalinstelling op individuele wijze beoordelen. Een bank mag een hele groep niet op voorhand weigeren, zonder individuele beschouwing van de klant. Wij hebben er in gesprekken geen aanwijzingen voor gekregen dat dit wel zou gebeuren. In de praktijk treedt hier soms een soort catch-22 situatie op, waarbij een onderneming het proces voor de benodigde DNB-vergunning doorloopt, maar nog geen transacties kan doen door het ontbreken van een zakelijke betaalrekening waardoor die onderneming dus ook niet feitelijk aan de hand van transacties kan aantonen dat de risico's voor de bank beperkt zijn.

Daarnaast is mogelijk sprake van een weeffout in de implementatiewet. Artikel 36 PSD2 ziet op betaaldienstverleners met een zetel in een van de lidstaten. In de Nederlandse wetgeving staat de definitie van betaalinstelling in art. 1:1 van de Wft en die verwijst naar art. 2:3a, dat zijn betaalinstellingen met een zetel in Nederland en een vergunning van DNB en niet naar 2.3e betaaldienstverleners met een zetel elders of zonder vergunning. Het gevolg is dat vrijgestelde betaaldienstverleners, betaalinstellingen met zetel elders en/of met een PSD2-vergunning van een andere Europese toezichthouder niet onder de reikwijdte van art 1:1 van de Wft vallen en daarmee niet onder de reikwijdte van artikel 5:88a Wft, de equivalent van artikel 36 PSD2. Of dit ertoe leidt dat dergelijke betaalinstellingen in de praktijk minder makkelijk een betaalrekening kunnen openen bij Nederlandse banken hebben wij niet kunnen vaststellen. Wel is het zo dat de ACM op deze betaalinstellingen geen toezicht kan houden, omdat daarvoor de juridische basis ontbreekt.

Conclusie

- Sommige betaalinstellingen hebben in de praktijk volgens gesprekspartners moeite om een betaalrekening te openen bij banken. Een achterliggende reden kan zijn dat banken de risico's van bepaalde groepen klanten niet afdoende kan mitigeren. Dit leidt tot *derisking* en daarmee tot terughoudendheid bij acceptatie van bepaalde klanten door banken. Hier is sprake van een afruil tussen concurrentie en financiële inclusie enerzijds en eisen rondom AML en CTF anderzijds.
- Banken mogen betaalinstellingen niet categorisch uitsluiten. We hebben geen concrete aanwijzingen gekregen in de gesprekken met commerciële partijen dat dit zou plaatsvinden. De ACM houdt hier toezicht op.
- Er is mogelijk sprake van een weeffout in de implementatiewet waardoor buitenlandse betaalinstellingen niet onder de reikwijdte van artikel 5:88a Wft, de equivalent van artikel 36 PSD2, vallen.

---

40 Het regelgevend kader voor het beheersen van de risico's op witwassen en terrorismefinanciering, is risicogebaseerd. Het is dus een eigen verantwoordelijkheid van een Wwft-instelling om een inschatting te maken van de relevante risico's en daar vervolgens voldoende mitigerende maatregelen tegenover te stellen.

41 Zie bijvoorbeeld https://www.worldbank.org/en/topic/financialsector/brief/de-risking-in-the-financial-sector

Wat zijn de gevolgen voor de marktverhoudingen (diversiteit, monopolies, marktmacht)?
Gesprekspartners zien veel meer spelers in de betaalmarkt, maar geven ook aan dat eerder sprake is van correlatie dan van causaliteit. Al voor de inwerkingtreding van PSD2 nam het aantal marktpartijen toe en was sprake van innovatie op de betaalmarkt. Tot op zekere hoogte was PSD2 ook bedoeld om bestaande innovatie (de opkomst van nieuwe niet-gereguleerde betaaldiensten) in goede banen te leiden. Daarbij geven gesprekspartners aan dat het nog erg vroeg is om te zien hoe de markt zich ontwikkelt door de komst van PSD2. In Nederland is de wet bijna drie jaar van kracht, waarbij het eerste jaar nog veel moest uitkristalliseren en SCA pas in januari 2021 definitief werd ingevoerd voor online kaartbetalingen. Voor andere toepassingen was SCA al vanaf september 2019 ingevoerd.

PSD2 heeft vooral het gebruik van API's in de markt versneld. Banken gingen aan de slag met het bouwen van API's omdat het moest van PSD2, niet omdat ze dat zelf als commerciële strategie hadden. Het heeft het kennisniveau van API's verhoogd en het gebruik van API's in het betalingsverkeer genormaliseerd. Door de ontwikkeling van API's ontstonden er voor banken ook nieuwe technische mogelijkheden voor dienstverlening en dat zorgde ervoor dat ze goedkoper en sneller konden werken. Banken zelf hebben dus een belangrijke stap gemaakt richting een efficientere digitalisering als gevolg van PSD2.

Voor kleinere partijen die rekeninginformatiediensten willen aanbieden (vooral aan bedrijven) op basis van toegang tot de betaalrekening is er wel degelijk wat veranderd als gevolg van PSD2. Voorheen waren ze kostentechnisch onaantrekkelijk voor banken om bilaterale contracten mee af te sluiten en konden ze daardoor niet de concurrentie aangaan met grotere aanbieders van boekhoudkundige pakketten die wel bilaterale contracten met banken hadden over toegang. Deze partijen kregen via een PSD2-vergunning (en later via een *aggregator*) wel toegang tot de betaalrekening. Door het gebruik van API's zijn dergelijke partijen nu ook kostenefficiënt te bedienen zonder contracten. Banken moeten deze diensten gratis aanbieden. Hierbij geldt wel dat deze partijen over een vergunning voor dienst 7 of 8 moeten beschikken, wat ook de nodige kosten en inrichting met zich meebrengt. Dit verklaart ook de groei van de diensten van *aggregators* in de markt. *Aggregators* zijn partijen met een PSD2-vergunning die API-interfaces hebben ontwikkeld voor veel verschillende banken en tussen de TPP en de bank in gaan zitten. Zoals eerder in dit hoofdstuk beschreven kwamen deze op als gevolg van PSD2.

Er zijn vooralsnog geen nieuwe spelers op de markt gekomen die substantieel marktaandeel winnen dankzij het gebruik dat ze maken van nieuwe PSD2-diensten. Mogelijk is er sprake van toegenomen concurrentiedruk door potentiële toekomstige toetreders. Gesprekspartners noemen vaak Big Techs als potentieel belangrijke (toekomstige) spelers. In de praktijk is hier echter nog weinig van te merken, hoewel partijen als Google wel de vergunningen hebben om (via *passporting*) actief te worden op de Nederlandse markt, maken ze geen gebruik van de mogelijkheden die PSD2 biedt om rekeninginformatie- of betaalinitiatiediensten te bieden. Al met al lijkt de concurrentie beperkt toegenomen, maar heeft PSD2 nog weinig gevolgen gehad voor de marktverhoudingen in Nederland.

Conclusie

- Het beeld in de markt, bij consumentenorganisaties en bij toezichthouders is dat het gebruik van de nieuwe PSD2-diensten nog beperkt is en dat geen sprake is van monopolies of marktmacht.
- Er is meer concurrentie en diversiteit in de markt, maar dit was een beweging die al voor PSD2 en los van PSD2 plaatsvond.
- Daarnaast hebben kleinere partijen die administratieve software voor bedrijven aanbieden nu ook toegang tot betaalrekeninggegevens.
- Hoewel er veel nieuwe partijen actief zijn geworden op de Nederlandse markt, zijn vooralsnog geen partijen in de markt gekomen met een aanzienlijk marktaandeel.

- Big Techs maken vooralsnog geen gebruik van de mogelijkheid om rekeninginformatie- of betaalinitiatiediensten te bieden.
- De gevolgen voor marktverhoudingen zijn daarmee op dit moment beperkt. Het is echter nog te vroeg om te concluderen dat de opkomst van PSD2 geen effect heeft op de marktverhoudingen in Nederland.

Is het voldoende duidelijk welke betaalinstrumenten er wel en niet onder het verbod op surcharging vallen?
Per februari 2019 (januari 2018 in veel andere Europese lidstaten) werd *surcharging* verboden via de implementatie van PSD2, Artikel 62(3), (4) en (5).[42] *Surcharging* is het berekenen door de winkelier van toeslagen voor het gebruik van een betaalmiddel. PSD2 voorziet in de mogelijkheid dat lidstaten zelf mogen bepalen of *surcharging* geheel of gedeeltelijk verboden is. Nederland heeft gekozen voor een gedeeltelijk verbod. Dit houdt in dat winkeliers enkel bij bepaalde betaalinstrumenten waarbij nog wel een vergoeding in rekening mag worden gebracht, dit vooraf kenbaar moeten maken aan de consument.

Met het verbod op surcharging mogen winkeliers geen kosten meer in rekening brengen bij de consument voor het gebruik van debet- en de meeste creditcards. Het verbod geldt ook voor overschrijvingen en automatische incasso's. Het verbod geldt niet voor creditcards van een zogeheten drie-partijenschema, waaronder bijvoorbeeld American Express valt. Voor betalingen waarbij het verbod op *surcharging* niet geldt, blijft de huidige regelgeving gelden. Dit betekent dat verkopers alleen de daadwerkelijke kosten in rekening mogen brengen.[43]

Uit de consumentenenquête komt naar voren dat consumenten over het algemeen nog nooit hadden gehoord van een verbod op *surcharging* (Figuur 3.4). Uit de consumentenenquête blijkt ook dat de meeste consumenten hier afgelopen jaar nooit mee te maken hebben gehad (Figuur 3.5). Slechts een klein deel van de consumenten geeft aan in de praktijk in het afgelopen jaar wel eens met *surcharging* te maken te hebben gehad, vooral waar het online betalingen met een creditcard of betalingen in het buitenland betrof (Figuur 3.5). Dit betekent niet dat ongeoorloofd *surcharging* ook echt in de praktijk voorkomt in de mate die de enquête suggereert. De indruk is dat consumenten vaak niet weten wat *surcharging* inhoudt en denken dat ze met *surcharging* te maken hebben gehad, terwijl dat niet het geval is. Gesprekspartners geven ook aan dat het vrijwel nooit voorkomt dat een bedrijf toch doet aan *surcharging*. Mogelijk verwarren sommige respondenten bezorgkosten met *surcharging*. De ACM heeft wel meldingen van consumenten ontvangen over extra kosten die in rekening werden gebracht bij de keuze voor een bepaald betaalmiddel (vaak bij creditcards) bij online betalingen. Ook de Consumentenbond krijgt dergelijke meldingen binnen. Het is niet duidelijk of bij dergelijke meldingen ook daadwerkelijk sprake is van illegale *surcharging*. Consumenten weten namelijk vaak niet wat het inhoudt (Figuur 3.4).

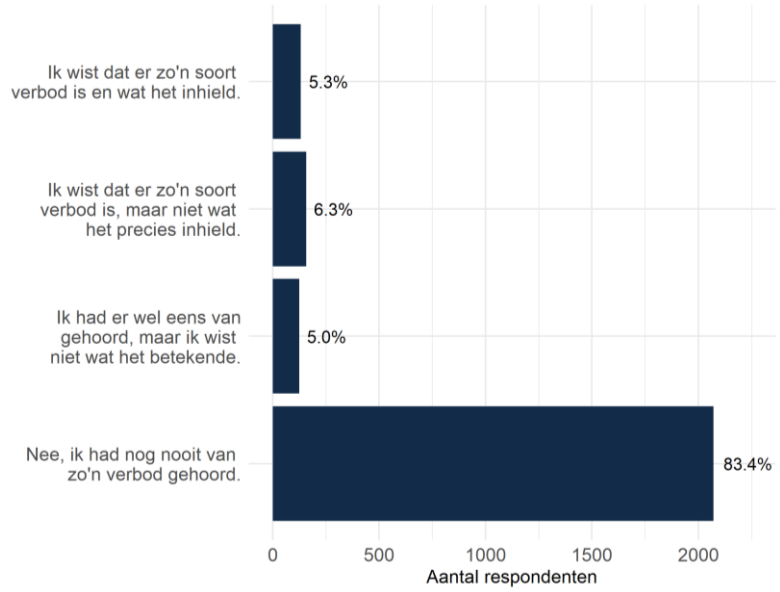
Surcharging kwam voordat PSD2 in werking trad met name bij creditcardbetalingen voor. Aangezien het aandeel betalingen met creditcard in Nederland relatief laag is, hebben consumenten ook weinig gemerkt van het verbod op *surcharging*. Dit verklaart waarom een aanzienlijk aandeel van de consumenten niet te maken heeft gehad met *surcharging*. Verder komen er uit gesprekken geen aanwijzingen naar voren dat marktpartijen illegaal aan *surcharging* doen. Eén gesprekspartner gaf aan dat hij een heel enkele keer een geval was tegengekomen.

---

42 Al in vergaderjaar 2015/2016 kwam Nederland met een 'Wet verbod toeslag gebruik betaalkaarten', wat een verbod op surcharging voorstelde. Het voorstel sloot aan op artikel 62, lid 4, van PSD2 (EU richtlijn 2015/2366,1) die in 2018 sowieso in Nederlandse wetgeving moet zijn geïmplementeerd . Het Nederlandse voorstel werd echter op 21 juni 2016 verworpen in de Tweede Kamer. Dit voorstel was achterhaald door de inwerkingtreding van de IFR.

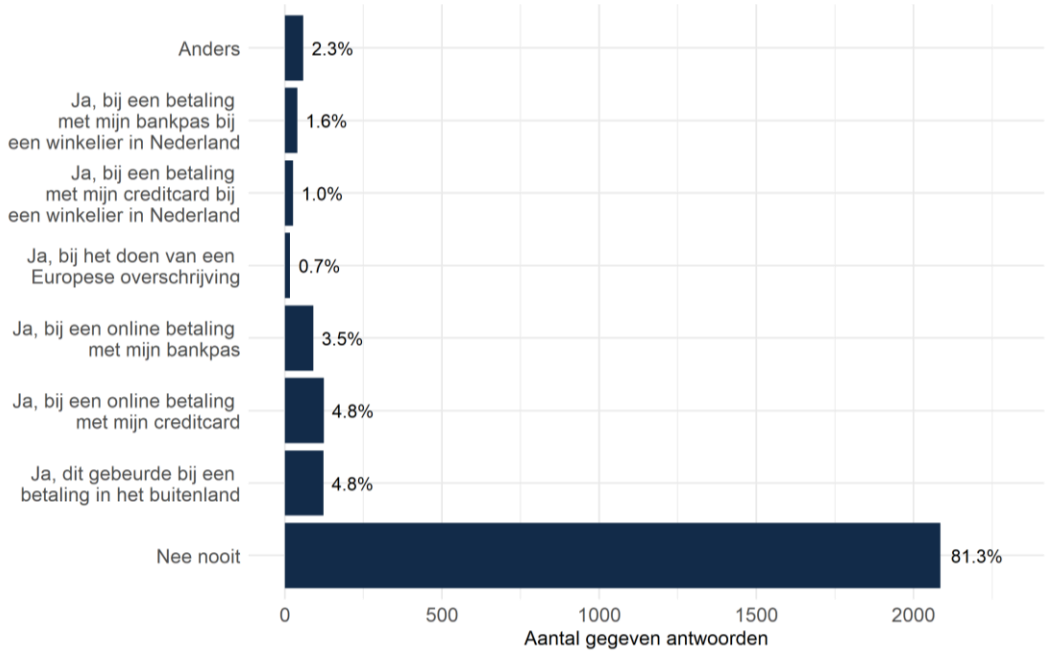
43 https://www.acm.nl/nl/publicaties/invoering-psd2-wat-gaat-er-voor-u-veranderen (Benaderd op 01-12-2021)

Figuur 3.4 Wist u voor u deze vragenlijst invulde dat er een verbod op surcharging bestond?



Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2484

Figuur 3.5 Hebt u in het afgelopen jaar wel eens te maken gehad met surcharging?



Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2484. Bij deze vraag konden respondenten meerdere antwoorden geven. Het percentage geeft daarom het aandeel antwoorden ten opzichte van het totaal aantal gegeven antwoorden (k = 2566) weer.

Wel weten aanbieders volgens gesprekspartners goed wat er wel en niet mag en proberen ze klanten soms te sturen richting betaalinstrumenten waar *surcharging* wel mogelijk is. Denk bijvoorbeeld aan bezorgers van maaltijden, die graag zien dat klanten met iDEAL betalen, omdat daar *surcharging* wel toegestaan is. [44] Gesprekspartners noemen als nadeel van het verbod op *surcharging* dat het instrumenten uit handen neemt voor bedrijven om consumenten te sturen naar voor hen efficiënte betaalmiddelen. Het verbod op *surcharging* zorgt er namelijk voor dat bij consumenten prikkels ontbreken te kiezen voor meer efficiënte betaalmiddelen, omdat het gebruik van minder efficiënte betaalmiddelen door de consument niet duurder kan worden gemaakt. *Surcharging* wordt doorgaans gezien als een instrument voor de winkelier om te sturen naar een efficiënt betaalmiddel. Het verbod op *surcharging* leidt er nu toe dat, aldus gesprekspartners, consumenten die via een efficiënte betaalmethode betalen, indirect moeten bijdragen aan de kosten van minder efficiënte betaalmethodes (omdat de verkoper die in zijn prijs verwerkt).

Tegenover het verbod op surcharging staan limieten op de *interchange fees* in de *Interchange Fee R*egulation (IFR).[45] Gesprekspartners geven aan dat deze limieten in de praktijk weinig effect hebben, omdat de tarieven die te maken hebben met afhandeling van transacties via de betaalnetwerken naar de *interchange fee* bestaan uit andere componenten die niet gereguleerd zijn, waarbij er een 'waterbed' effect optreedt tussen de tarieven voor het interchange gedeelte en andere componenten. Wij hebben hier echter geen cijfermatige onderbouwing van kunnen achterhalen. De Europese Commissie publiceerde in juni 2020 een rapport over de impact van de IFR.[46] Het rapport concludeerde dat de hoofdoelen van de regulatie zijn gehaald aangezien de *interchange fees* voor consumenten kaartbetalingen zijn verminderd. Dit zorgt weer voor lagere kosten voor kaartbetalingen door Merchants en uiteindelijke tot betere dienstverlening aan consumenten aan lagere consumentenprijzen.

Conclusie

- Het begrip *surcharging* is bij het grootste deel van de consumenten onbekend.
- Dit is mogelijk specifiek voor Nederland. *Surcharging* kwam in Nederland ook weinig voor omdat er relatief weinig creditcard betalingen plaatsvinden.
- De ACM en de consumentenbond krijgen desondanks wel regelmatig klachten die ze als *surcharging* classificeren. Onduidelijk blijft echter in hoeverre hier echt sprake is van ongeoorloofde *surcharging*. Wij hebben er geen concrete verifieerbare voorbeelden van gekregen of gevonden.
- Aanbieders weten volgens gesprekspartners wat wel en niet mag wat betreft *surcharging* en geven aan dat illegaal *surcharging* in de praktijk nauwelijks voorkomt.
- Het verbod op *surcharging* belemmert *merchants* en betaaldienstverleners om consumenten te prikkelen om meer efficiënte betaalmethodes te gebruiken. Dit kan volgens gesprekspartners op termijn negatieve gevolgen hebben voor de efficiëntie van betalingsverkeer.
- De limieten op *interchange fees* (die als 'ruilmiddel' fungeerden voor het verbod op *surcharging*) worden als weinig effectief ervaren.
- We concluderen dat het voldoende duidelijk is wat wel en niet onder het verbod op *surcharging* valt.

3.2 Innovatie

Onderzoeksvragen

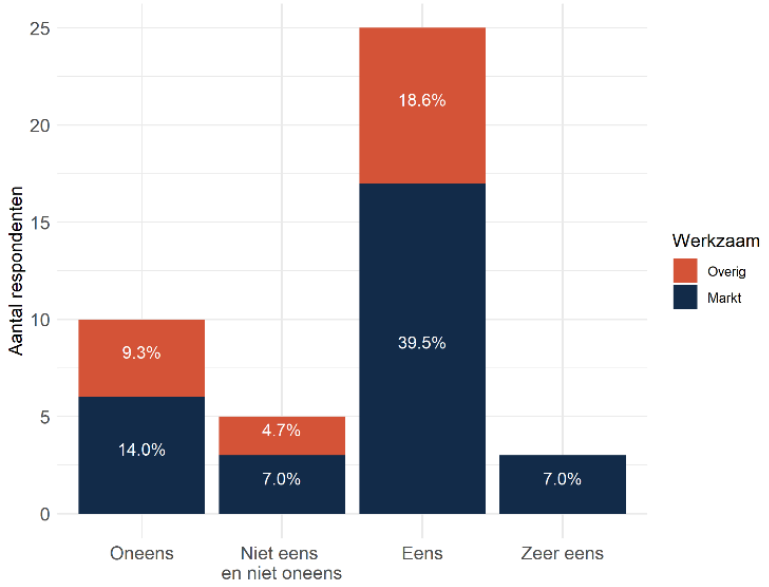
[44] Voor zogeheten aanvullende diensten, niet voor het overschrijvingsdeel van de transactie. Daarbij geldt dat retailers alleen werkelijk gemaakte kosten in rekening mogen brengen.
[45] EUR-Lex - 32015R0751 - EN - EUR-Lex (europa.eu)
[46] kd0120161enn.pdf (europa.eu)

1. In welke mate faciliteert en stimuleert PSD2 innovaties?
2. Zijn nieuwe spelers en nieuwe producten op de markt gekomen?

In welke mate faciliteert en stimuleert PSD2 innovaties?

PSD2 faciliteert innovaties door de mogelijkheid te creëren om betaalinitiatiediensten en rekeninginformatiediensten aan te bieden. Dat heeft sommige partijen gestimuleerd om eigen en deels nieuwe producten te ontwikkelen. Over het algemeen stellen gesprekspartners dat deze producten nog niet echt succesvol zijn. Van de gesprekspartners geeft 58,1 procent aan dat PSD2 heeft gezorgd voor innovatie (Figuur 3.6). In de gesprekken geven ze aan dat deze innovatie wel beperkt is. De kern van de dienstverlening is niet veranderd en nieuwe diensten die zijn ontwikkeld of momenteel worden ontwikkeld zijn beperkt. Een vraag die wordt opgeworpen is in hoeverre de nieuwe diensten zijn ontstaan door PSD2 of anders ook zouden zijn ontstaan. Veel ontwikkelingen in de markt waren al gaande voordat PSD2 in werking trad. PSD2 heeft er daarnaast voor gezorgd dat de nieuwe diensten op een uniforme manier Europees breed zijn aan te bieden, wat de prikkels voor innovatie vergroot doordat opschaling door succesvolle aanbieders makkelijker is.

Figuur 3.6 Stelling: Innovatie in de markt voor betaaldiensten is toegenomen door de introductie van PSD2



Bron: SEO Economisch Onderzoek op basis van een mini-enquête onder 43 interviewpartners

Bij het traditionele betalen is er weinig innovatie als gevolg van PSD2. Betaaldiensten zijn in Nederland al zo volwassen en efficiënt dat er beperkte toegevoegde waarde is van de nieuwe diensten. iDEAL en pin zijn zulke sterke producten dat dit het moeilijk maakt nieuwe producten succesvol en kostenefficiënt in de markt te zetten. Er zijn wel enkele nieuwe toetreders op deze markt zoals Klarna en Trustly (die reeds voor de implementatie van PSD2 bestonden), maar deze partijen slagen er vooralsnog nog niet in marktaandeel te winnen van iDEAL.

Bij rekeninginformatiediensten zijn er wel nieuwe, deels innovatieve, diensten ontstaan, denk aan het bieden van geautomatiseerd inzicht in uitgaven voor consumenten, mogelijkheden om geautomatiseerd met kleine bedragen te beleggen, mogelijkheden om aan budgetbeheer te doen, hulp bij het opzeggen van abonnementen, of het

verstrekken van een kredietwaardigheidsscore, die vervolgens gebruikt kan worden om een lening te verstrekken. De vraag blijft wel hoeveel vraag er naar deze diensten is en of consumenten ervoor willen betalen, omdat banken deze soms zelf ook (gratis) aanbieden. Daarnaast zijn sommige aanbieders rekeninginformatiediensten en betaalinitiatiediensten gaan combineren, wat de mogelijkheid creëert van innovatieve toepassingen. Bovendien is er door PSD2 een mogelijkheid gekomen om betaalrekeningen bij verschillende banken aan elkaar te koppelen, iets wat voor PSD2 niet mogelijk was.

PSD2 heeft ook op een aantal andere vlakken, die minder zichtbaar zijn voor consumenten, gezorgd voor innovatie. Zo heeft PSD2 innovatie gestimuleerd doordat het banken dwong een API-interface te bouwen voor hun betalingssysteem. Deze technologische stap vooruit heeft het denken van banken over de toekomst van betaaldiensten veranderd. Banken zijn ook gaan inzien dat zij op basis van API-technologie nieuwe diensten kunnen ontwikkelen. Daarnaast zijn bestaande diensten (denk aan aansluiting van bedrijfssoftwarepakketten op de betaalrekeningen van bedrijven) efficiënter en veiliger geworden doordat deze nu via een API-interface lopen.

Ondanks dat banken een standaard voor API's proberen aan te houden, verschilt de uitwerking van API's per bank. Een belangrijke oorzaak hiervan is het ontbreken van een API-standaard in PSD2. Het ontbreken van uniforme standaarden voor API's heeft ertoe geleid dat er meer fricties zijn voor betaaldienstverleners die gebruik willen maken van de mogelijkheden die PSD2 biedt. Het bouwen van een koppeling met een API, en deze aansluiting up-to-date houden, brengt immers kosten met zich mee. Dit heeft een markt gecreëerd voor (vergunninghoudende) aggregators. Deze bedrijven bieden applicaties om via één centraal punt toegang te krijgen tot rekeninginformatie bij verschillend vormgegeven API's van verschillende banken in verschillende landen. Een derde partij die gebruikmaakt van een *aggregator* hoeft zich dus niet meer bezig te houden met het koppelen met API's en *kan* zich richten op het ontwikkelen van hun dienst. Ook hoeven dergelijke derde partijen, in tegenstelling tot de aggregators, geen PSD2-vergunning meer te hebben, waardoor zij de kosten en complicaties van de vergunningsaanvraag niet hebben. Dit heeft tot gevolg dat derde partijen zonder een PSD2-vergunning diensten kunnen aanbieden die vergelijkbaar zijn met diensten die derde partijen aanbieden die wel een PSD2-vergunning hebben. Hierbij zijn de derde partijen overigens wel gehouden aan de afspraken die zijn gemaakt met de vergunninghoudende aggregator. In de betaalmarkt bestonden al *aggregators* bij bijvoorbeeld internationale betalingen. Dat deze ontwikkelingen zich ook bij PSD2 zouden voordoen was te verwachten.

Tot slot heeft PSD2 gezorgd voor een vervanging van bilaterale contracten in de zakelijke markt (met een vergoeding) naar een vorm van gratis toegang tot de betaalrekening. Voor PSD2 hadden aanbieders van boekhoudsoftware bilaterale contacten over de uitlevering van data. Een grotere partij kon 'gemakkelijk' toegang krijgen tot zo'n contract, maar dat gold niet voor kleinere partijen. Voor deze partijen is PSD2 vooral een vervanging van de oude infrastructuur die hen in staat stelt bestaande diensten op een efficiëntere manier in te vullen. PSD2 zorgt hiermee voor een versnelling van de ontwikkeling. Met PSD2 hebben ook de kleinere partijen (gratis) toegang gekregen tot betaalinitiatiediensten en betaaldata mits deze partijen over een vergunning voor dienst 7 of 8 beschikken. Dit kan leiden tot verdere innovatie.

Conclusie

- Er zijn in Nederland maar beperkt nieuwe innovatieve ontwikkelingen op de betaalinitiatiemarkt als gevolg van de inwerkingtreding van PSD2. iDEAL is hier al erg sterk en het is lastig om hiermee te concurreren.
- Bij rekeninginformatiediensten zijn er wel enkele nieuwe, deels innovatieve, diensten ontstaan.
- Door PSD2 hebben kleinere aanbieders van boekhoudpakketten ook toegang tot de betaalrekening gekregen, wat leidt tot meer innovatie.
- PSD2 heeft ervoor gezorgd dat banken API's zijn gaan gebruiken voor hun betalingsverkeer. Dit is een technologische stap vooruit geweest en maakt nieuwe diensten mogelijk.

- Innovatie komt daarmee ook uit de hoek van bestaande aanbieders: zij voelden druk om te innoveren na de komst van PSD2.
- Het gebrek aan standaardisatie van API's bij invoering van PSD2 heeft het ontstaan van een nieuw type dienstverlener gestimuleerd: *aggregators*. Kanttekening hierbij is dat *aggregators* ook in de UK, waar wel een API-standaard bestaat, belangrijke spelers zijn. *Aggregators* zijn geen nieuw businessmodel en bestonden al op andere aspecten van de betaalmarkt.

Zijn nieuwe spelers en nieuwe producten op de markt gekomen?
Er is een groot aantal nieuwe spelers geregistreerd met nieuwe PSD2-dienst vergunningen. Het EBA-register en het DNB-register geven het beeld dat er in Nederland 24 nieuwe partijen zijn bijgekomen met een vergunning voor diensten 7 en 8 (9 met een vergunning voor dienst 7 en 24 met een vergunning voor diensten 8). Het EBA-register registreert de datum wanneer een bedrijf een van de diensten 1 t/m 8 is gaan aanbieden. Figuur 3.7 en Figuur 3.8 geven dit goed weer. Hieruit is duidelijk dat enkele bedrijven met dienst 7 en/of 8 al bestonden voor de komst van PSD2. Zij hebben later een PSD2-vergunning aangevraagd. Uit Figuur 3.8 blijkt ook dat buitenlandse partijen gebruik kunnen maken van *passporting* naar Nederland. Deze vergunningen kwamen in 2018 op gang en piekten in 2019. Figuur 3.9 laat zien dat de meeste bedrijven met een *passporting* vergunning voor Nederland uit Litouwen komen. Ook Frankrijk, Duitsland en Zweden zijn relevante *herkomstlanden*. Niet bekend is in hoeverre deze partijen met een formeel paspoort naar Nederland, ook daadwerkelijk diensten aanbieden aan Nederlandse consumenten.

Uit de gesprekken komt naar voren dat actieve spelers vaak een beperkt marktaandeel hebben. Zo kunnen nieuwe betaalinitiatiediensten nog lastig concurreren met al langer bestaande betaalmethoden. Wel zijn er enkele nieuwe producten op de markt gekomen. Op basis van het EBA-register en het DNB-register hebben we de volgende nieuwe diensten geïdentificeerd die in Nederland een vergunning hebben gekregen (zie het overzicht in appendix D): huishoudboekjes voor consumenten, producten die consumenten helpen om hun betaalgedrag in de gaten te houden, applicaties die partijen in staat stellen om een toekomstige iDEAL-betaling te agenderen (bijvoorbeeld voor een te betalen boete in de toekomst), hulp bij automatisch beleggen met kleine bedragen, leningverstrekking op basis van een geautomatiseerde kredietbeoordeling.

Analyse EBA-register

De analyse is uitgevoerd met data van 05-07-2021 uit het EBA-register

Op basis van een analyse van het (payment institutions) EBA-register kan een vergelijking worden gemaakt op het niveau van de Europese Unie. Uit deze analyse komt naar voren dat de meeste bedrijven met een PSD2-vergunning zijn gevestigd in Duitsland en Zweden. Ook Frankrijk, Nederland, Litouwen en Polen vertegenwoordigen een aanzienlijk aantal bedrijven met PSD2-vergunningen. België en Denemarken volgen respectievelijk (Figuur Appendix). Hoewel, deze analyse een vergelijking maakt tussen alle landen van de Europese Unie, is een verdiepende vergelijking gemaakt tussen de zeven landen met de meeste PSD2-vergunningen, de bovenstaand genoemde landen.

Opvallend is dat Duitsland en Nederland (en enkele landen met minder vergunninghouders), geen enkel bedrijf met alleen dienst 7 hebben. Uit de analyse blijkt ook dat slechts een fractie van het totaal aantal bedrijven enkel licentie 7 bezitten. Bijna de helft van alle Europese bedrijven biedt enkel een rekeninginformatiedienst aan en circa de andere helft combineert rekeninginformatiediensten met betaalinitiatiediensten.

Na de implementatie van PSD2 is een aanzienlijk aantal PSD2-vergunningen aangevraagd. Uit de analyse blijkt dat Nederlandse bedrijven niet uitzonderlijk laat een PSD2-vergunning verkregen vergeleken met de andere zes landen. Want hoewel er in Duitsland, Frankrijk en Litouwen al snel na de Europese implementatie bedrijven met een PSD2-vergunning van de grond kwamen, duurde dit langer in België, Denemarken, Polen en Zweden. De verlate implementatie van PSD2 in Nederland, lijkt daarmee niet tot een significant concurrentienadeel voor Nederlandse bedrijven te hebben geleid. Wel konden een bedrijven met een eerder verkregen PSD2-vergunning in een ander land reeds passporten naar Nederland.

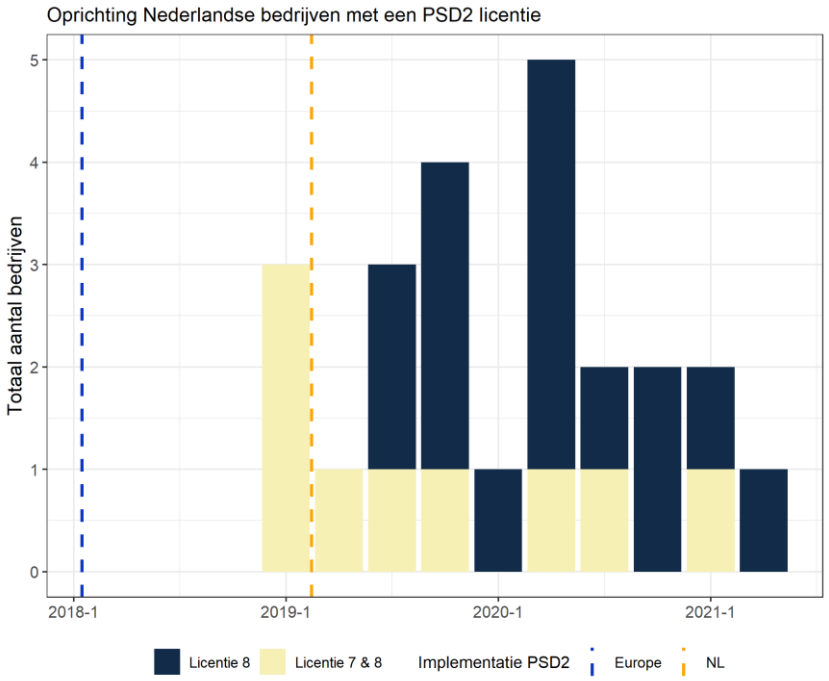
Tot slot komt uit de analyse naar voren dat zowel Litouwen en Duitsland een relatief hoog aantal PSD2-passport vergunningen hebben naar andere landen van de EU. Dit valt te verklaren door het relatief hoge aantal PSD2-vergunninghouders in deze landen.

Conclusie

- In Nederland zijn er tussen de invoering van PSD2 en de Q3 2021 24 vergunningen voor dienst 7 en 8 afgegeven (waarvan 23 nu nog actief zijn).
- Daarnaast zijn er nu ook meer spelers uit het buitenland actief, die via een passportlicentie toegang hebben gekregen tot de Nederlandse markt. De meeste partijen komen nu uit Litouwen, Frankrijk en Duitsland (eerder waren dit partijen uit het Verenigd Koninkrijk, maar door de Brexit is dit veranderd).

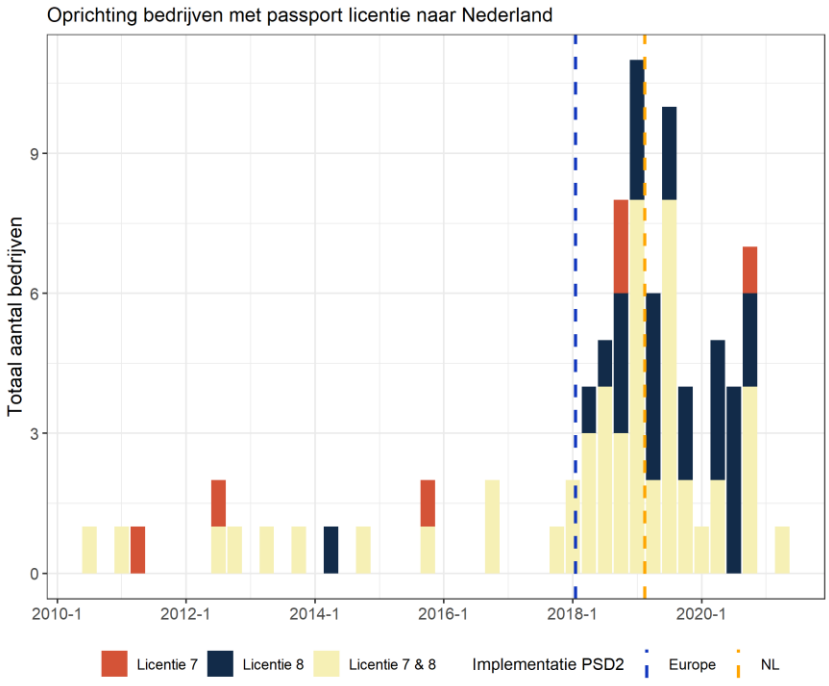
- Met de toename van partijen is er ook een (beperkte) toename van het aantal nieuwe producten gekomen.
- Het is nog te vroeg om te concluderen of de toestroom van nieuwe partijen tijdelijk is of niet.

Figuur 3.7 Vergunningverlening Nederlandse bedrijven met diensten 7 en of 8



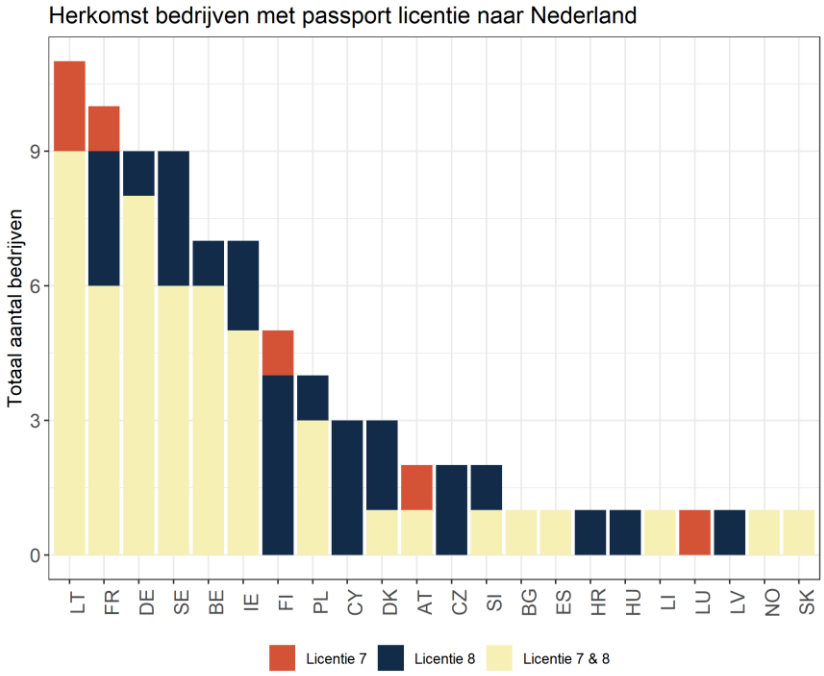
Bron: EBA (2021), o.b.v. analyse EBA register

Figuur 3.8 Registratie buitenlandse bedrijven met diensten 7 en of 8 die passporten naar Nederland



Bron: EBA (2021), o.b.v. analyse EBA-register

Figuur 3.9 De oorsprong van buitenlandse bedrijven met diensten 7 en/of 8 die passporten naar Nederland



Bron: EBA (2021), o.b.v. analyse EBA-register

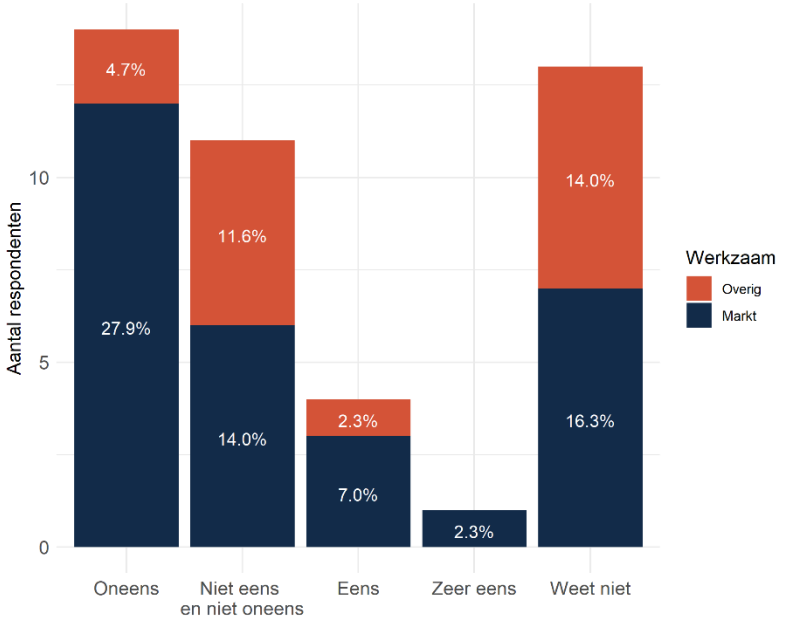
3.3 Europese betaalmarkt

Onderzoeksvraag

1. Is grensoverschrijdend betalen voor consumenten en bedrijven gemakkelijker en goedkoper geworden?

Is grensoverschrijdend betalen voor consumenten en bedrijven gemakkelijker en goedkoper geworden?

Figuur 3.10 Stelling: Grensoverschrijdende transacties zijn eenvoudiger geworden met PSD2



Bron: SEO Economisch Onderzoek op basis van een mini-enquête onder 43 interviewpartners

Vanuit Nederlands perspectief gezien is grensoverschrijdend betalen door PSD2 niet gemakkelijker of goedkoper geworden. Binnen Europa was grensoverschrijdend betalen al gemakkelijk en relatief goedkoop vanwege de mogelijkheid van SEPA-betalingen. Daarnaast bieden buitenlandse partijen die actief willen zijn in Nederland, steeds vaker iDEAL aan (echter is iDEAL verder beperkt overschrijdend).

Het beeld dat grensoverschrijdende transacties niet eenvoudiger zijn geworden blijkt ook uit de online enquête met onze gesprekspartners (Figuur 3.10). 32,6 procent gaf aan het oneens te zijn met de stelling dat grensoverschrijdende transacties eenvoudiger zijn geworden met PSD2. Slechts 11,6 procent gaf aan dat het wel gemakkelijker was geworden. De overige gesprekspartners gaven aan het niet te weten of het noch eens, noch oneens te zijn met de stelling.

Conclusie

- Vanuit Nederlands perspectief zijn grensoverschrijdende transacties niet gemakkelijker of goedkoper geworden. Het was al relatief makkelijk via SEPA-betalingen.

3.4 Consumentenzijde

Onderzoeksvragen

1. Zijn er kwetsbare groepen voor wie dit wetsvoorstel tot problemen heeft geleid? Zo ja, voor welke groepen en tegen welke problemen lopen zij aan?
2. Toepasselijkheid en effect van bepalingen over tarifering van klanten voor PSD2-diensten (108 lid a)

Zijn er kwetsbare groepen voor wie dit wetsvoorstel tot problemen heeft geleid? Zo ja, voor welke groepen en tegen welke problemen lopen zij aan?

Het beeld dat uit de gesprekken en de enquête onder interviewpartners naar voren komt is dat er geen kwetsbare groepen zijn voor wie het wetsvoorstel tot problemen heeft geleid. Belangenorganisaties maakten zich bij de invoering zorgen dat met name kwetsbaardere groepen zoals ouderen en visueel beperkten last zouden ondervinden van PSD2, bijvoorbeeld doordat diensten te veel digitale kennis vragen of omdat ze het risico zagen op nieuwe vormen van fraude. Er zijn echter weinig klachten hierover gekomen en de zorgen over PSD2 zijn in de praktijk tot nu toe ongegrond gebleken. Een reden daarvoor is dat deze kwetsbare groepen (en consumenten in het algemeen) op dit moment nog nauwelijks gebruikmaken van PSD2-diensten. Toezichthouders zien een vergelijkbaar beeld. Zij verklaren ook dat consumenten (en dus ook kwetsbare groepen) zich vooral zorgen maakten om het verspreiden van hun data. Hoewel gesprekspartners vanuit de vertegenwoordigers van consumenten aangeven dat zij wel eens horen dat sommige gebruikers moeite hebben met SCA-hulpmiddelen, hebben wij niet het beeld gekregen dat hier grote problemen spelen.

Conclusie

- Hoewel er rond de implementatie van PSD2 angsten waren voor problemen bij kwetsbare groepen, heeft het wetsvoorstel niet daadwerkelijk tot problemen geleid bij kwetsbare groepen. Kwetsbare groepen maken volgens gesprekspartners, net zoals consumenten in het algemeen, nog weinig gebruik van specifieke PSD2-diensten.

4 Veiligheid borgen

Wat zijn de gevolgen van de invoering van PSD2 geweest voor de veiligheid van betalingen?

4.1 Bescherming toegang en betalingen

Onderzoeksvragen

1. Wat zijn de effecten van strong customer authentication? Wat is de impact van SCA op de omvang van de betalingsfraude en moeten aanvullende maatregelen worden overwogen?
2. Wat zijn oplossingen die gebruikers in staat stellen hun transacties makkelijker te monitoren, rekening houdend met aanbevelingen ERPB?*

Wat zijn de effecten van strong customer authentication?

PSD2 stelt eisen aan de wijze waarop klanten toegang kunnen krijgen tot hun betaalrekening (cliëntauthenticatie). Een sleutelstuk hierbij is de *strong customer authentication* (SCA). SCA heeft tot doel om de identiteit van de betaaldienstgebruiker vast te stellen om zo te borgen dat het de klant zélf is die een opdracht geeft voor een transactie. Deze identificatie van de klant vormt dus een veiligheidswaarborg. SCA vereist dat bij een authenticatie minstens twee van de drie volgende eigenschappen gebruikt worden:

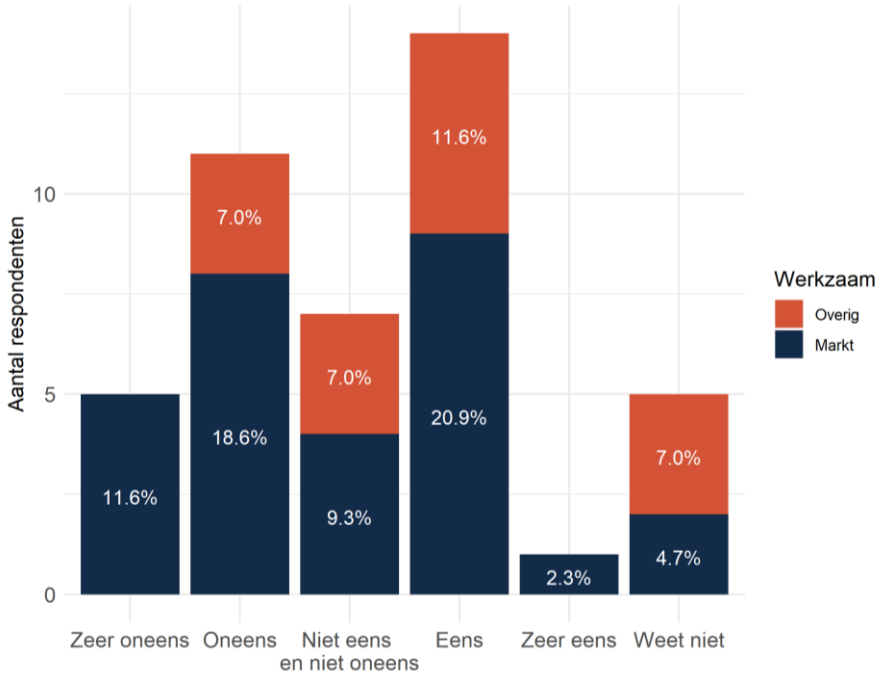
- Kennis (iets dat alleen de gebruiker weet, zoals een pincode);
- Bezit (iets dat alleen de gebruiker heeft, zoals een pinpas);
- Inherente eigenschap (een unieke persoonlijke eigenschap van de gebruiker zoals een vingerafdruk).

Bij betalingen is SCA nodig, behalve als er een vrijstelling van toepassing is. Vrijstellingen bestaan voor vertrouwde begunstigden, gedelegeerde autorisatie, bedrijfstransacties, op basis van een transactierisicoanalyse, of voor transacties onder een bepaalde drempel. In aanvulling hierop is er een aantal uitsluitingen waarop SCA geheel niet van toepassing is. Ook bij rekeninginformatiediensten moeten gebruikers SCA toepassen, die vervolgens voor een termijn van 90 dagen geldig is. Daarna is er wederom SCA nodig.

Interviewpartners zijn verdeeld over de mate waarin de introductie van SCA soepel verlopen is. Van de gesproken partijen met een mening is circa 37,2 procent van mening dat dit niet het geval is geweest terwijl 34,8 procent dit wel vindt (zie Figuur 4.1). Dit verschil in mening is terug te voeren op een paar factoren. Ten eerste was er aanvankelijk discussie over de manier waarop toegang voor derden ingevoerd moest worden, waarbij banken hebben gekozen voor het *redirect* model, terwijl andere betaaldienstverleners een implementatie wilden waarbij ze zelf controle hielden over de klantreis. Ten tweede benoemen gesprekspartners van zowel de gebruikers- als de aanbiederskant in de interviews dat de invoering van SCA voor veel onrust zorgde. Bij e-commercepartijen en *card schemes* bestond de zorg dat de invoering van de SCA-eis zou leiden tot conversieverlies door meer fricties in de klantreis. Zij hebben daarom bij herhaling aangedrongen om uitstel van de deadline voor invoering (1 januari 2021). DNB en EBA zijn hier niet in meegegaan, maar de Engelse toezichthouder wel, terwijl sommige andere landen ook soepeler met de invoering omgingen. De afweging voor toezichthouders was dan vasthouden aan de invoering van aanvullende veiligheidswaarborgen binnen de door de wetgever gestelde overgangstermijn versus het voorkomen van implementatiefricties voor aanbieders. De toezichthouder heeft voor het eerste gekozen. Gelet op het feit dat online kaartbetalingen in Nederland een relatief gering aandeel van de e-commercebetalingen uitmaken was de

noodzaak voor uitstel ook gering geweest. In 2020 was het aandeel van creditcards in online bestedingen 13 procent. Bij toonbankbetalingen is dit aandeel 0,5 procent.[47] Ten derde duurde het relatief lang tot de markt pas echt in actie kwam, terwijl het eind van de wettelijke overgangstermijn ver van tevoren duidelijk was. Het momentum ontstond pas toen de deadline dichterbij kwam. In het proces van invoering speelde de SCA-werkgroep van de betaalvereniging een belangrijke rol, waar veel energie is gaan zitten in het testen met *soft-blockades*. Ondanks deze aspecten van de invoering heeft de consument er in de praktijk weinig last van gehad.

Figuur 4.1 Stelling: De invoering van Strong Customer Authentication (SCA) is in Nederland soepel verlopen



Bron: SEO Economisch Onderzoek op basis van een mini-enquête onder 43 interviewpartners

Het doel van SCA is om te garanderen dat het de klant zelf is die opdracht geeft voor een transactie. Zo voorkomt SCA dat een ongeautoriseerde gebruiker een (daarmee frauduleuze) betaling doet. Doordat een autorisatie meerdere onderdelen vereist, wordt de kans kleiner dat een niet-gemachtigde gebruiker over voldoende onderdelen van een autorisatie beschikt om een frauduleuze betaling uit te voeren. Hoewel dit de veiligheid kan verhogen, kunnen hier ook neveneffecten uit volgen, bijvoorbeeld een afname van het gebruiksgemak voor klanten doordat meer handelingen nodig zijn of omzetverlies voor e-commerce aanbieders doordat transacties stuklopen op SCA.

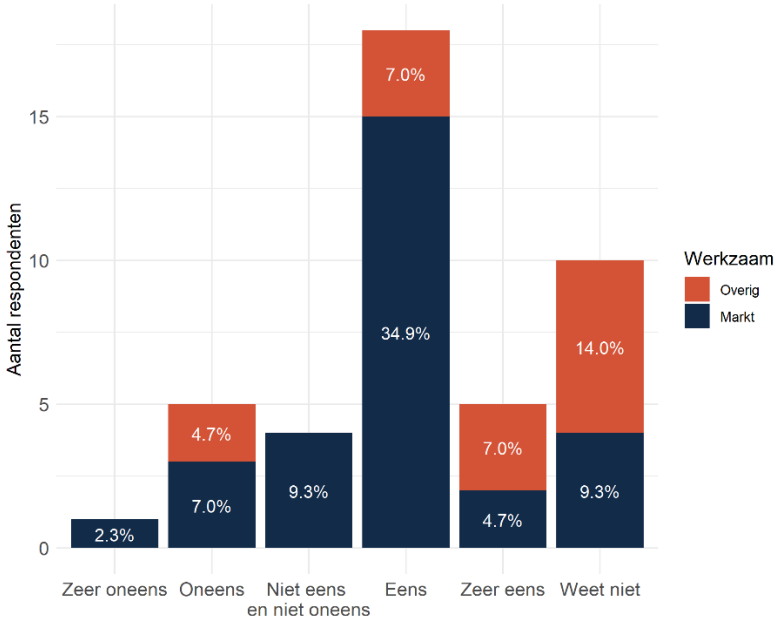
Fraude

Interviewpartners zijn overwegend positief over het effect van SCA op fraudereductie. In de online mini-enquête onder gesprekspartners benoemt 70 procent van de respondenten met een mening het eens of zeer eens te zijn met de stelling dat SCA leidt tot minder fraude met transacties (zie Figuur 4.2). Er zijn twee redenen waarom sommige gesprekspartners het oneens te zijn met de stelling dat invoering van SCA tot minder fraude heeft geleid. Ten eerste omdat invoering van SCA hun ogen vrijwel geen effect heeft gehad op fraude en dus ook niet tot minder fraude heeft geleid. Specifiek voor de Nederlandse markt geldt dat reeds voor PSD2 het beveiligingsniveau van de Nederlandse betaalmarkt hoog was, mede door het grote marktaandeel van iDEAL en het feit dat iDEAL reeds vóór

[47] Zie https://www.betaalvereniging.nl/wp-content/uploads/Infographic_Thuiswinkel_Markt_Monitor_2020.pdf en https://www.dnb.nl/media/e34bo5zu/betalen_kassa_2020.pdf.

de invoering van de SCA-eis SCA-*compliant* was. De SCA-eis heeft waarschijnlijk wel fraude met online creditkaartbetalingen moeilijker gemaakt, hoewel we dit niet feitelijk hebben kunnen vaststellen aan de hand van data. Voor Nederland is het totale effect hiervan op het fraudevolume effect beperkt omdat het marktaandeel van online kaartbetalingen in Nederland klein is. Daarnaast zijn betalingsfraudes steeds vaker vooral het gevolg van directe misleiding (*phishing, spoofing,* etc.), en is de zwakste schakel dus niet de techniek (waarbij SCA een technische drempel voor fraude opwerpt) maar menselijk handelen. Ten tweede suggereren sommigen dat er een waterbedeffect is, waarbij strengere SCA-eisen leiden tot een verschuiving naar andere vormen van fraude.

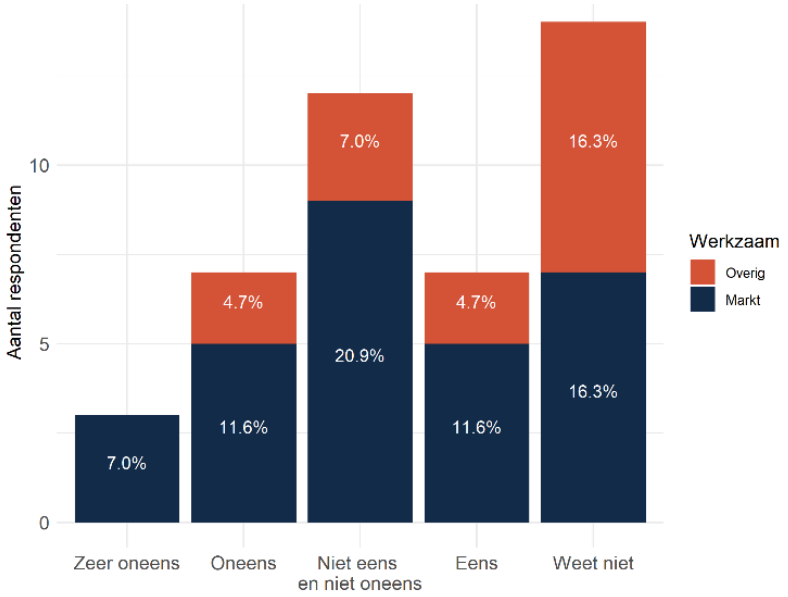
Figuur 4.2 Stelling: Strong Customer Authentication (SCA) leidt tot minder fraude met transacties



Bron: SEO Economisch Onderzoek op basis van een mini-enquête onder 43 interviewpartners

In aanvulling hierop is 24,3 procent van de gesprekspartners het oneens of zeer oneens met de stelling dat PSD2-betaalinitiatie- en rekeninginformatiediensten nieuwe mogelijkheden voor fraude met betaaldiensten hebben gecreëerd (zie **Fout! Ongeldige bladwijzerverwijzing.**). 16,3 procent van de respondenten vind dat PSD2-betaalinitiatie en -rekeninginformatiediensten nieuwe mogelijkheden voor fraude hebben gecreëerd. Navraag bij gesprekspartners geeft niet het beeld dat er daadwerkelijk nieuwe fraudemogelijkheden zijn ontstaan door invoering van PSD2. Bij sommigen leeft de gedachte dat persoonlijke inloggegevens worden gedeeld en dat derde partijen daar op nieuwe manieren misbruik van kunnen maken. Daarvan is bij *redirect* echter geen sprake. Andere noemen dat PSD2 mogelijk tot verwarring onder klanten heeft geleid of ze hun pincode nu wel of niet mogen delen met derde partijen. Dit betreft geen nieuwe vorm van fraude. Daarnaast geven de gesprekken niet het beeld dat dit een groot probleem is. Ten slotte zijn er ook gesprekspartners die benoemen dat banken geen controle mogen uitvoeren op de derde partijen die toegang vragen, maar volledig moeten vertrouwen op de aanwezigheid van een eIDAS certificaat.

Figuur 4.3 Stelling: PSD2-betaalinitiatie- en rekeninginformatiediensten hebben nieuwe mogelijkheden voor fraude met betaaldiensten gecreëerd

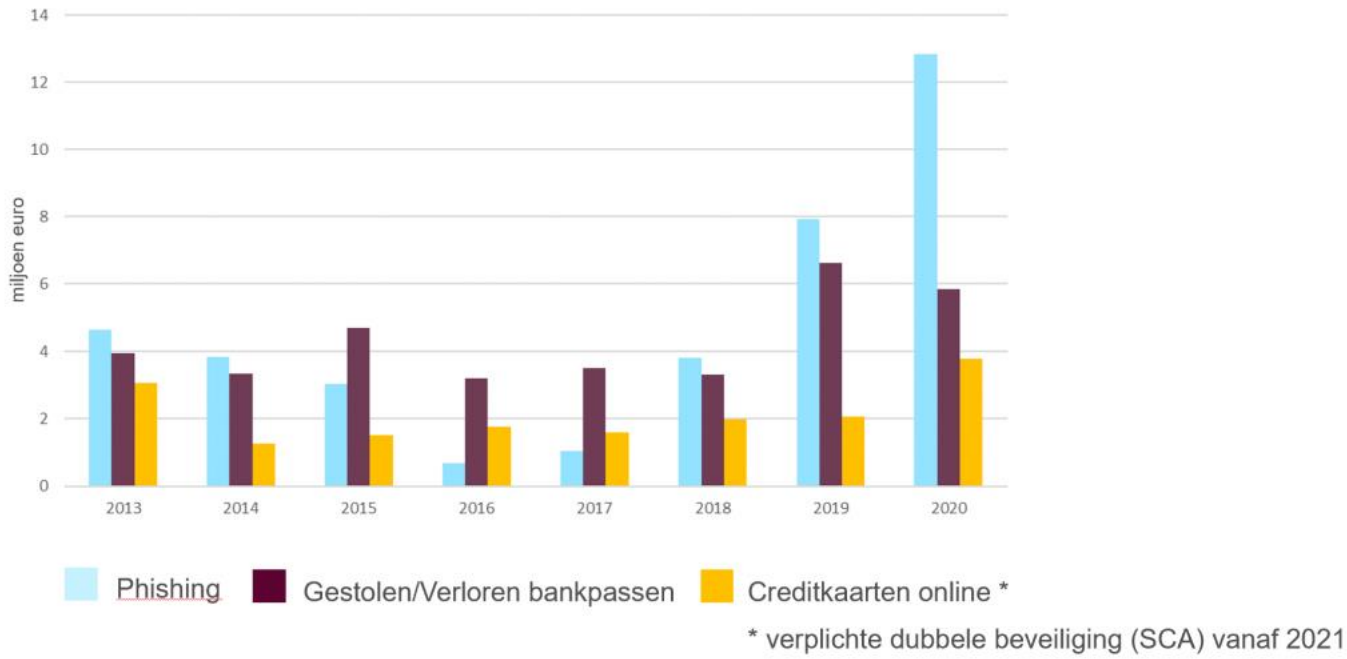


Bron: SEO Economisch Onderzoek op basis van een mini-enquête onder 43 interviewpartners

Gesprekspartners benoemen dat het belangrijk is om onderscheid te maken tussen verschillende producten. Bancaire overboekingen via bijvoorbeeld iDEAL maakten al gebruik van multifactorauthenticatie. Hetzelfde was het geval met pinnen aan de toonbank. In zulke gevallen is het gebruik van SCA nog altijd een goed instrument om de veiligheid te verhogen, maar hangt gebruik van het instrument niet samen met de invoering van de PSD2-richtlijn. Daarnaast is het effect van PSD2 op fraude bij zulke producten beperkt: er is immers weinig veranderd ten opzichte van voor de introductie van PSD2.

Voor andere producten is het effect groter. Gesprekspartners wijzen hier met name op creditcardbetalingen, waar de invoering van de SCA-verplichting tot grotere veranderingen in de *customer journey* heeft geleid. Marktpartijen en toezichthouders benoemen dat SCA voor zulke betalingen tot minder fraude heeft geleid. In Nederland vormen creditcardbetalingen echter maar een beperkt onderdeel van het totale betalingsverkeer. Door dit 'samenstellingseffect' in het betalingsverkeer is het effect van de invoering van de SCA-verplichting op de Nederlandse markt betrekkelijk klein.

Figuur 4.4 Toename fraudelast in Nederland door met name phishing



Bron: Betaalvereniging Nederland

Gesprekspartners wijzen er verder op dat SCA weliswaar een goed 'technisch' slot op de deur is, maar dat in de praktijk fraudes vaak tot stand komen via kanalen waar SCA niet op ziet. Bij fraude met *social engineering* misleidt bijvoorbeeld de oplichter de gebruiker *zelf* om een overboeking te doen en die 'gewoon' via SCA te autoriseren (e.g. bij *phishing*). Technische waarborgen zoals SCA helpen hier maar beperkt tegen. Voor zover SCA fraude tegengaat, gaan kwaadwillenden op zoek naar andere manieren om consumenten geld afhandig te maken. Er is dan vooral sprake van verschuiving, en minder van een algehele afname van fraudegevallen. In algemene zin is er ook geen afname geweest van de totale schadelast van fraude in Nederland. In plaats daarvan neemt deze schadelast toe, de laatste jaren vooral als het gevolg van een toename van *phishing, telefoonspoofing,* en andere vormen van *social engineering*. Gesprekspartners wijzen erop dat hier niet per se een samenhang met PSD2 achter zit. Voor een groot deel is sprake van een autonome trend als gevolg van het feit dat het betalingsverkeer digitaliseert en dat fraudeurs hun pijlen richten op het direct misleiden van klanten. Dit is overigens ook geen specifiek Nederlands verschijnsel: ook in andere landen neemt het aandeel van *social engineering*-fraudes toe.

Het feit dat veel fraudegevallen het gevolg zijn van directe misleiding van consumenten, begrenst de mate waarin aanvullende maatregels overwogen moeten worden. Aanvullende maatregelen die nieuwe technische eisen stellen zijn maar beperkt effectief als consumenten vervolgens misleid worden om zelf informatie te geven die leidt tot betalingsfraude of zelf daadwerkelijk de 'frauduleuze' betalingen te doen. Verschillende interviewpartners wijzen hiermee vooral op de rol van bewustwording aan de kant van de consument. Het feit dat de *customer journey* steeds minder fricties kent, maakt ook dat de consument meer aandacht moet hebben voor de juistheid van de betaling die hij of zij doet. Juist deze aandacht staat volgens sommige interviewpartners onder druk omdat consumenten in toenemende mate wennen aan het gemakkelijk en snel afgeven van toestemming, niet alleen voor betalingen maar ook voor andere digitale diensten.

Gebruiksgemak, toegankelijkheid en veiligheidsbewustwording

In de marktsegmenten waar de invoering van PSD2 heeft geleid tot de introductie van SCA wijzen marktpartijen op de afname van het gebruiksgemak voor klanten. Voor producten waar SCA al de *de facto* standaard in Nederland was (e.g. iDEAL, pinnen, internet- en mobielbankieren) speelt dit uiteraard niet. Deze afname van het gebruiksgemak volgt vooral uit het feit dat de klant extra handelingen moet verrichten alvorens hij of zij de betaling kan afronden. Parallel daaraan benoemen gesprekspartners dat marktpartijen sturen op een zo soepel mogelijke klantreis. Ze benoemen daarmee dat hier ook deels sprake is van een tijdelijk probleem dat verdwijnt naarmate de markt zich verder ontwikkelt.

Sommige gesprekspartners benoemen dat dit de toegankelijkheid van de betaalinfrastructuur kan verminderen. Mensen die minder digitaal vaardig zijn kunnen meer moeite ervaren in het doen van een betaling naarmate het aantal handelingen dat vereist is toeneemt. Dit probleem is echter niet specifiek voor PSD2. Veel banken maken al sinds jaar en dag bij betalingen gebruik van een vorm van multifactorauthenticatie. PDS2 heeft hier geen verandering in gebracht. Voor toegang tot rekeninginformatie heeft een aantal banken wel de bakens verzet en SCA ingevoerd. Ook is het gebruik van nieuwe PSD2-diensten op de consumentenmarkt nog laag, en waarschijnlijk niet geconcentreerd bij consumenten die digitaal minder vaardig zijn. De SCA-eisen die voortvloeien uit PSD2 zetten de toegankelijkheid van het betalingsverkeer in de praktijk dus niet verder onder druk. Waar hier druk op bestaat vloeit dat voort uit digitalisering in den brede, en niet uit PSD2 in het bijzonder.

Een aantal gesprekspartners benoemt dat vanuit de introductie van de SCA-eis mogelijk een veiligheidsbevorderend gedragseffect uitgaat. Het feit dat voor sommige betaaldiensten nu een sterkere authenticatie vereist is kan consumenten opvallen en ze bewust maken van het feit dat ze bewust moeten instemmen met een betaling. Andersom zouden consumenten het ook prettig kunnen vinden dat ze door authenticatie een gevoel van controle houden over het doen van een betaling. Niet alle gesprekspartners delen deze zienswijze volledig, en wijzen erop dat consumenten graag ook een soepele klantreis hebben. Voor sommige groepen consumenten is veiligheid mogelijk belangrijker dan een frictieloze klantreis, maar voor anderen misschien juist andersom.

Op de markt voor rekeninginformatiediensten benoemen gebruikers en aanbieders van boekhoudpakketten dat de SCA-eis (1x / 90 dagen) strenger is ten opzichte van de oude situatie waarin van een File Transfer Protocol (FTP)-koppeling gebruik werd gemaakt en waar maar één autorisatie voor nodig was.[48] Dat was volgens sommige respondenten gebruiksvriendelijker, mede omdat het eigenlijk slecht voorstelbaar is dat gebruikers na 90 dagen ineens niet langer hun boekhouding willen bijhouden. In bredere zin lijkt er meer onvrede in de markt te bestaan waar de EBA zich ook gevoelig voor toont: er loopt momenteel een consultatie over de SCA i.r.t. de 90-dagentermijn.[49]

Conversieverlies

Rond de introductie van PSD2 bestonden bij marktpartijen veel zorgen over conversieverlies als gevolg van de invoering van de SCA-verplichting. Gesprekspartners verschillen van mening over de mate waarin daadwerkelijk sprake is van omzetkrimp. Sommige gesprekspartners benoemen daadwerkelijk conversieverliezen te zien in de praktijk, anderen noemen dat ondanks zorgen hierover rond de introductie van PSD2 zulke verliezen zijn uitgebleven, en weer anderen stellen dat eventuele conversieverliezen vooral een tijdelijk probleem zijn omdat marktpartijen hun processen zullen verbeteren.

Conclusie

48 Deze mogelijkheid bestaat overigens nog steeds.

49 EBA consults on the amendment to its technical standards on strong customer authentication and secure communication in relation to the 90-day exemption for account access | European Banking Authority (europa.eu)

- SCA helpt om de veiligheid van betalingen en toegang tot de rekening te vergroten. Met name bij online creditcardbetalingen is de klantreis veranderd als gevolg de SCA-eis, terwijl sommige banken ook aanpassingen in hun inlogprocedures hebben gedaan.
- Tegelijkertijd is de impact van de introductie van de SCA-eis op de Nederlandse markt relatief beperkt, omdat iDEAL reeds voor de invoering van de SCA-eis SCA-compliant was. Voor creditcard betalingen leidden de SCA-eisen wel tot aanpassingen, het aandeel van creditcard betalingen is in Nederland echter beperkt (13 procent online, 0,5 procent aan de toonbank).
- Er is sprake van een toename van fraudes die gebruikmaken van *social engineering*. SCA, een technische maatregel, helpt hier maar beperkt tegen omdat het de consument zélf is die wordt misleid. Verdere technische beschermingsmaatregelen zijn daarmee beperkt effectief. Bewustwording van de consument is kansrijker.

Wat zijn oplossingen die gebruikers in staat stellen hun transacties makkelijker te monitoren, rekening houdend met aanbevelingen Euro Retail Payments Board (ERPB)?*

De verlenging van de betaalketen kan het voor consumenten moeilijker maken om hun transacties te monitoren als hiermee voor de consument onduidelijker wordt met wie, waar en wanneer hij of zij een transactie heeft gehad. Voor consumenten kan het bijvoorbeeld verwarrend zijn als de naam van een betaaldienstverlener die werkt voor de verkoper op hun rekeningafschrift verschijnt, in plaats van de handelsnaam van een verkoper waar een consument een goed of dienst heeft afgenomen. De ERPB heeft onlangs oplossingsrichtingen voor dit probleem verkend, en aanbevelingen gedaan voor harmonisatie van gegevens over wie, waar en wanneer door de betaalketen heen zodat dit voor de consument inzichtelijk gemaakt kan worden (ERPB, 2021). Dit lijkt ons een passende oplossing die overigens aansluit bij de bestaande praktijk in Nederland. Enkele jaren geleden zijn hier in het MOB reeds afspraken over gemaakt.[50]

Conclusie

- De aanbevelingen van het ERPB sluiten goeddeels aan bij de geldende Nederlandse praktijk. Waar het ERPB verder gaat is dat een positieve ontwikkeling die gebruikers in staat stelt hun transacties makkelijker te monitoren.

4.2 Consumentenbescherming

Onderzoeksvragen

1. Voldoen de regels over niet-toegestane en onbedoelde overboekingen?
2. Bieden de wettelijke grenzen voor uitzonderingen bij contactloze betalingen voldoende evenwicht gemak en frauderisico?
3. Wenselijkheid van maximumbedragen bij betalingen waarbij autorisatie vooraf gegeven wordt (108 lid f)

Voldoen de regels over niet-toegestane en onbedoelde overboekingen?

PSD2 regelt de aansprakelijkheid voor niet-toegestane en onbedoelde overboekingen. De grondgedachte hierbij is consumentenbescherming: consumenten moeten een waarborg hebben dat zij beschermd zijn indien er sprake is van een frauduleuze betaling buiten hun schuld. In PSD2 betekent dit dat de consument moet instemmen met

[50] Zie Jaarrapportage MOB 2018, p. 13, https://www.dnb.nl/media/l5abf5ru/mob-rapportage-2018-juni-2019_tcm46-384460.pdf

een transactie. Deze instemming kan óók ontbreken indien er SCA is toegepast, bijvoorbeeld als de pinpas inclusief pincode van de consument gestolen wordt. In gevallen waarin de consument geen instemming heeft gegeven ligt de aansprakelijkheid voor niet-toegestane en onbedoelde overboekingen in eerste aanleg bij de bank, behalve in het geval dat de klant grof nalatig is geweest of frauduleus heeft gehandeld.

De Nederlandse implementatie van PSD2 biedt consumenten meer bescherming dan het minimum dat PSD2 vereist. PSD2 staat toe dat bij niet-toegestane transacties de eerste € 50 aan schade voor rekening van de klant komt. Nederland heeft geen gebruikgemaakt van deze optie. Daarnaast is er in Nederland voor gekozen om bij grove nalatigheid van de klant het aan de rechter te laten om de verdeling van de schade tussen de bank en de klant te bepalen. Ook hierin biedt de Nederlandse implementatie van PSD2 de consument meer bescherming dan de minimumnormering in de regelgeving.

Artikelen 73, 74 en 90 PSD2 over niet-toegestane overboekingen leggen de verantwoordelijkheid voor het terugbetalen bij de betaaldienstverlener (de bank). Die moet het bedrag uiterlijk aan het eind van de volgende werkdag terugbetalen, tenzij een redelijk vermoeden van fraude bestaat. De verlener van betaalinitiatiediensten moet de bank compenseren als hij niet kan bewijzen dat de initiatie goed is verlopen. Verder bevat PSD2 een inspanningsplicht voor de bank om een onjuiste transactie zoveel mogelijk (door de onterechte begunstigde) te laten terugboeken, ook als de betaler per ongeluk een verkeerd rekeningnummer heeft ingevuld.

Voor Nederland geldt daarnaast dat Nederlandse banken in de regel de schade die consumenten lijden door *phishing* en *spoofing* waarbij de naam en/of het nummer van de bank wordt gebruikt voor een groot deel of volledig vergoeden.[51] Daarnaast hebben enkele Nederlandse banken sedert enkele jaren een IBAN-naamcheck ingevoerd om consumenten te kunnen waarschuwen bij een verhoogde kans op een onbedoelde overboeking.[52] Ook bestaat er een maximum voor het volume aan overboekingen per dag. Deze kan weliswaar verhoogd worden, maar alleen met SCA en met een paar uur vertraging. Ook dit is een rem op onbedoelde overboekingen.

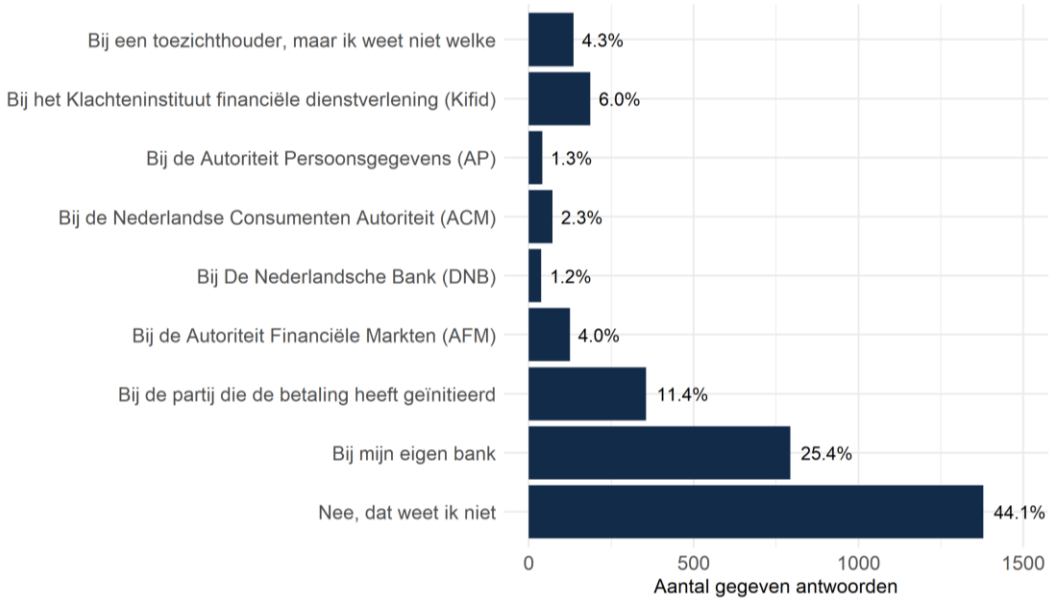
Consumenten zijn dus veelal goed 'verzekerd' en beschermd. Consumenten zijn 'verzekerd' doordat de bank in de meeste gevallen consumenten bij fraude (moeten) compenseren. Zij zijn beschermd doordat banken door hun aansprakelijkheid voor fraudeschade een prikkel hebben om processen zo in te regelen dat fraude voorkomen wordt. Een nadeel hiervan is dat doordat PSD2 feitelijk ál het risico voor fraudeschade bij banken legt, de prikkel voor consumenten om fraude te voorkomen mogelijk afneemt.

Uit het consumentenonderzoek komt naar voren dat een groot deel van de consumenten niet weet waar ze terechtkunnen met klachten over een betaling door een andere partij dan hun eigen bank. Wel geeft ook een relatief groot deel van de consumenten antwoord dat aansluit bij waar de wetgever de verantwoordelijkheid voor bij niet-toegestane en onbedoelde overboekingen primair heeft neergelegd, namelijk de eigen bank. De mini-enquête onder gesprekspartners spiegelt ten dele de resultaten van de consumentenenquête. Iets meer dan 37 procent van de gesprekspartners is het oneens of zeer oneens met de stelling dat consumenten weten waar ze terechtkunnen met klachten over betaalinitiatie en rekeninginformatiediensten. De keuze in de regelgeving om de verantwoordelijkheid voor het herstellen van niet-toegestane en onbedoelde overboekingen strookt in elk geval met de verwachtingen van consumenten over het loket waartoe zij zich moeten wenden (ook als zij in meerderheid verklaren geen idee te hebben waar ze moeten zijn).

---

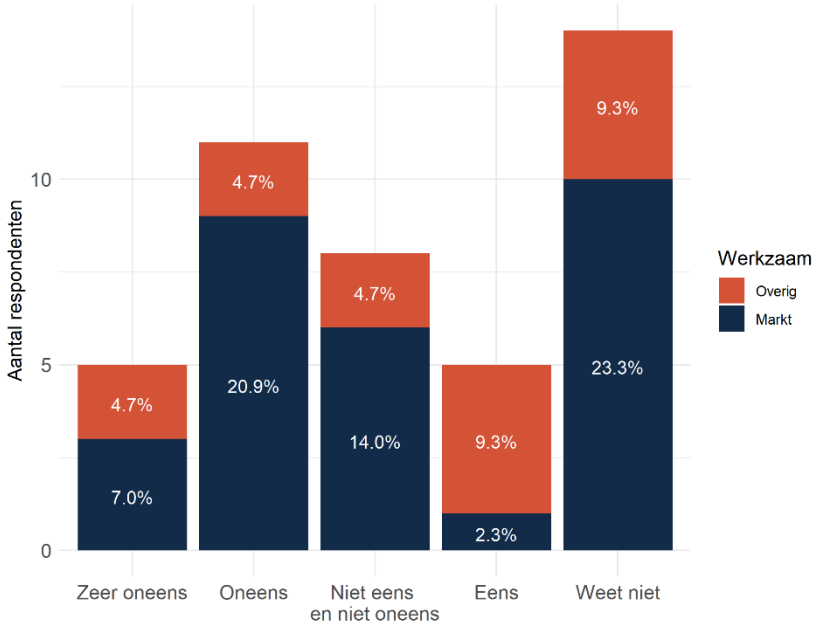
51 Zie e.g. Toetsingscriteria voor coulance bij bankhelpdesk fraude (spoofing) (nvb.nl)
52 Zie e.g. Invoering IBAN-Naam Check - Betaalvereniging Nederland

Figuur 4.5 Als een betaling door een andere partij dan uw bank is uitgevoerd en u hebt hier een klacht over, weet u dan waar u terechtkunt?



Bron: SEO Economisch Onderzoek (2021) o.b.v. consumentenenquête, n = 2485. Bij deze vraag konden respondenten meerdere antwoorden geven. Het percentage geeft daarom het aandeel antwoorden ten opzichte van het totaal aantal gegeven antwoorden (k = 3128) weer.

Figuur 4.6 Stelling: Consumenten weten waar zij terechtkunnen met klachten over betaalinitiatiediensten en rekeninginformatiediensten



Bron: SEO Economisch Onderzoek op basis van een mini-enquête onder 43 interviewpartners

Conclusie

- De regels voor onbedoelde en niet-toegestane overboekingen leggen de verantwoordelijkheid hiervoor in veel gevallen bij de bank. Dit sluit aan bij de verwachting van consumenten. Voorts maakt Nederland geen gebruik van de lidstaatoptie om een deel van het risico bij de klant te beleggen en zetten banken technische

beschermingsmaatregelen in om consumenten (en de bancaire schadelast) te beperken. Nederlandse consumenten weten zich dus goed beschermd.
- Een mogelijke adverse prikkel is dat ál het risico bij de banken ligt. De prikkel voor consumenten om goed op te letten wordt hiermee zwakker, terwijl hierboven reeds is gewezen op het feit dat veiligheidsbewustwording bij consumenten belangrijk is om fraude door *spoofing* en *phishing* tegen te gaan.

Bieden de wettelijke grenzen voor uitzonderingen bij contactloze betalingen voldoende evenwicht tussen gemak en frauderisico?

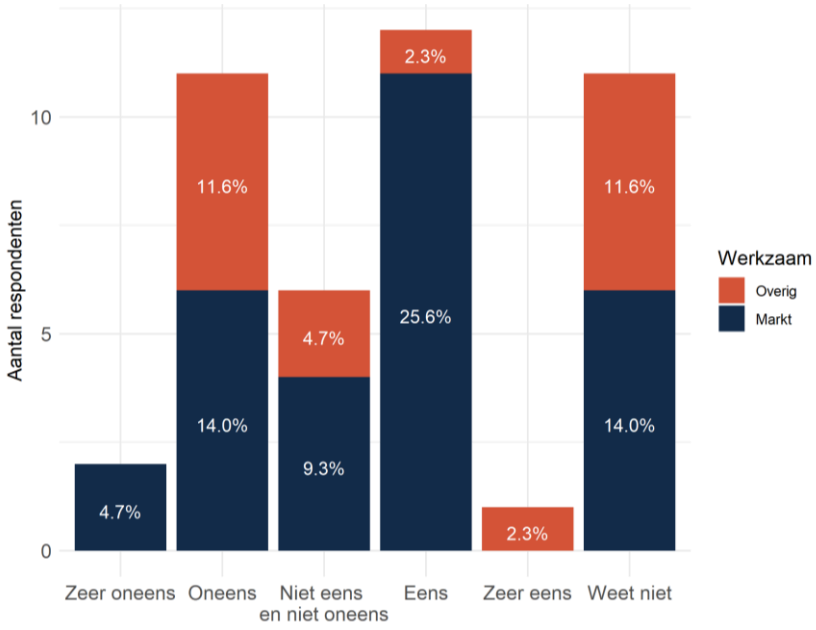
De PSD2-regelgeving staat toe dat geen SCA toegepast hoeft te worden bij contactloze betalingen beneden een bepaald drempelbedrag. Dit drempelbedrag is nu vastgesteld op € 50, tenzij er de laatste vijf betalingen geen pincode is gebruikt of het totaal aan achtereenvolgende betalingen zonder pincode boven de € 150 komt. De ASPSP mag kiezen welke van deze twee criteria zij hanteert. Dit drempelbedrag probeert een brug te slaan tussen het beperken van schade voor consumenten indien hun pas ontvreemd wordt en het vereenvoudigen van het doen van betalingen.

Gesprekspartners verschillen van mening over de mate waarin de balans tussen deze doelen nu passend is. Ruwweg evenveel van hen geven in de mini-enquête aan dat de grens voor contactloze betalingen verhoogd kan worden zonder een hogere kans op fraude. De ervaringen met de tijdelijke verhoging van de uitzondering als gevolg van COVID zijn in dit opzicht positief, want dit heeft niet tot hogere fraudepercentages bij dergelijke betalingen geleidt. Marktpartijen geven vaker aan dat verhogen van het drempelbedrag kan dan andere partijen. Marktpartijen zijn van mening dat zij zelf goed in staat zijn om de risico's van hogere limieten te mitigeren, bijvoorbeeld door ze afhankelijk te maken van risico-inschattingen die zij per betaling maken.

In gesprekken benoemen consumentenorganisaties dat maximumbedragen een manier zijn om de schade voor de consument te beschermen bij verlies van een pas of diefstal daarvan. Ook zou het bijdragen aan bewustwording aan de kant van de consument dat hij of zij zorgvuldig met de betaalpas moet omgaan. Andere gesprekspartners zien vooral ruimte voor meer differentiatie. Voor sommige consumenten zal de huidige grens prima functioneren, terwijl anderen mogelijk een voorkeur hebben voor ruimere grenzen. Deze gesprekspartners suggereren dat consumenten mogelijk zelf bij hun bank zouden moeten kunnen aangeven waar zij een drempel willen voor contactloze betalingen. Mogelijk zullen banken hier wel paal en perk aan willen stellen indien zij opdraaien voor eventuele schade die ontstaat bij hogere grenswaarden. Sommige gesprekspartners geven ook aan dat fraude bij contactloze betalingen beperkt is ten opzichte van andere vormen van fraude.

Het gemiddeld pinbedrag ligt in 2020 rond de € 26 per transactie. De grens van € 50 per transactie knelt vooralsnog dus niet.

Figuur 4.7 Stelling: De grens voor contactloze betalingen kan worden verhoogd zonder dat er een hogere kans op fraude is



Bron: SEO Economisch Onderzoek op basis van een mini-enquête onder 43 interviewpartners

Conclusie

- In Nederland lijkt de grenswaarde voor contactloze betalingen niet te knellen.
- De verhoging van de limieten tijdens COVID heeft niet tot hogere fraudecijfers met contactloze betalingen geleid.
- Partijen verschillen van mening over de mate waarin het wenselijk is de grens op te hogen. Marktpartijen zien ruimte voor een hogere grens, terwijl niet-marktpartijen hier minder vaak op wijzen.
- In onze ogen is sprake van een goede balans tussen veiligheid en gebruiksgemak, waarbij de hogere grenzen gehandhaafd zouden kunnen blijven.
- Een optie zou zijn om te experimenteren met hogere grenzen en daarbij gecontroleerd het effect op fraude te meten.

Wenselijkheid van maximumbedragen bij betalingen waarbij autorisatie vooraf gegeven wordt

Ten aanzien van betalingstransacties waarbij het transactiebedrag niet vooraf bekend is (bijvoorbeeld bij betaling aan een autoverhuurder voor eventuele schade aan de gehuurde auto), bepaalt PSD2 dat de betaaldienstverlener van de betaler geldmiddelen op de betaalrekening van de betaler kan blokkeren, mits de betaler ingestemd heeft met het exacte bedrag aan te blokkeren geldmiddelen. De betaaldienstverlener geeft de op de betaalrekening van de betaler geblokkeerde geldmiddelen na de ontvangst van de informatie over het exacte bedrag van de betalingstransactie onverwijld vrij en uiterlijk onmiddellijk na de ontvangst van de betaalopdracht. Overigens kende Nederland reeds voor PSD2 de mogelijkheid om zulke pre-autorisatie te geven, bijvoorbeeld bij onbemand tanken. Voor zulke transacties vereist PSD2 in de Nederlandse context vooral dat dit expliciet aan de klant wordt duidelijk gemaakt.

Bij de wenselijkheid van maximumbedragen spelen twee aspecten. Aan de ene kant bieden maximumbedragen bescherming aan consumenten. Door maximumbedragen in te voeren bij betalingen waarbij autorisatie vooraf

gegeven wordt, is het bedrag dat per ongeluk of met opzet verkeerd kan worden overgeboekt, beperkt. Daartegenover staat dat het inperken van dit maximumbedrag de mogelijkheden van PSD2 inperkt: het aantal transacties dat frictieloos uitgevoerd kan worden neemt immers af.

Vooralsnog heeft PSD2 niet geleid tot hogere fraudecijfers. Hoewel de fraudecijfers zijn toegenomen (zie Figuur 4.4 hierboven), is dit niet het gevolg van PSD2, maar van andere ontwikkelingen (zie ook sectie 4.1). Het is dan ook onwaarschijnlijk dat het invoeren van maximumbedragen bij betalingen waarbij autorisatie vooraf gegeven wordt een substantieel effect zal hebben op fraude.

Conclusie

- Invoering van maximumbedragen bij betalingen waarbij autorisatie vooraf gegeven wordt zal waarschijnlijk geen substantieel effect hebben op de totale fraudelast.

4.3 Gevolgen reikwijdtebepalingen en vrijstellingen

Onderzoeksvragen

1. Is de huidige reikwijdte van PSD2 adequaat met het oog op technische dienstverleners bij betaaldiensten en fragmentatie in de keten van betaaldienstverleners (mede gelet op regels voor uitbesteding in PSD2)?
2. Welke nieuwe risico's vloeien voort uit niet-gereglementeerde diensten?
3. Zijn de vrijstellingen in PSD2 toereikend en moeten de prudentiële, operationele en consumentenbeschermingsvereisten worden gewijzigd?
4. Toepassing en effect van bepalingen rondom drempelwaardes en vrijstellingen (108 lid e)

Is de huidige reikwijdte van PSD2 adequaat met het oog op technische dienstverleners bij betaaldiensten en fragmentatie in de keten van betaaldienstverleners (mede gelet op regels voor uitbesteding in PSD2)?; Welke nieuwe risico's vloeien voort uit niet-gereguleerde diensten?

Sinds de komst van PSD2 is het financiële ecosysteem steeds complexer geworden met een meer gefragmenteerde keten. Bij de betalingsketen zijn veel spelers betrokken (sommige zijn gereguleerd, andere niet) en de complexiteit en onderlinge afhankelijkheid neemt alsmaar toe. Vraag is dan ook of de huidige reikwijdte van PSD2 adequaat is. De reikwijdte van PSD2 voldoet mogelijk niet als er risico's ontstaan door niet-gereguleerde segmenten of diensten (i.e. segmenten of diensten buiten de reikwijdte). We behandelen deze twee vragen daarom in samenhang.

PSD2 kent het concept van technische dienstverleners ('technical service providers'): "indien de partij die de gegevens ophaalt géén zicht heeft of kan hebben op de persoonlijke beveiligingsgegevens of op een token van die gegevens. Deze partij maakt slechts de koppeling met de API van de rekening houdende betaaldienstverleners en fungeert als kanaal waarlangs de betaalgegevens van de rekening-houdende betaaldienstverlener naar de rekeninginformatiedienstverlener gaan. Zo'n partij kan niet eigenstandig toegang verkrijgen tot de betaalrekening en is dan een technische dienstverlener."[53] Dit zijn partijen die diensten verlenen aan PSD2-vergunninghouders, zoals de verwerking en opslag van gegevens of de beschikkingstelling van IT- en communicatie-infrastructuur. De rol van dergelijke technische dienstverleners is aan het groeien. Bij technische dienstverleners, waarbij een PSD2 vergunningsplichtige partij onderdelen van zijn bedrijfsvoering uitbesteedt, gelden uitbestedingsregels. Deze worden beschreven in artikel 19 van PSD2.

[53] Zie https://www.dnb.nl/voor-de-sector/open-boek-toezicht-wet-regelgeving/toezicht-wet-regelgeving/psd2/vergunningplicht-in-relatie-tot-samenwerking-en-uitbesteding-bij-rekeninginformatiedienstverlening/

Gerelateerd hieraan is de opkomst van *aggregators*. Dit zijn partijen die zelf een PSD2-vergunning voor dienst 7 en 8 hebben en voor een grote set aan banken API's hebben ontwikkeld. Derde partijen (dit kunnen zowel TPPs in de zin van PSD2 zijn als derde partijen die geen PSD2-vergunning hebben) maken vervolgens gebruik van die *aggregators*, zodat ze zelf geen API-koppelingen hoeven te ontwikkelen, of omdat ze dan zelf geen PSD2-vergunning hoeven aan te vragen. Met name over dat laatste bestaat in de markt in sommige gevallen onvrede. Sommige aanbieders hebben in de beginfase van PSD2 zelf een PSD2-vergunning aangevraagd, maar had dit achteraf niet gehoeven als zij een *aggregator* hadden gebruikt. Gesprekspartners stellen dat er hierdoor geen level playing *field* is. Zij zijn van mening dat bij het leveren van dezelfde diensten, aanbieders ook dezelfde compliancelast moeten hebben. Nu is dat niet zo voor derde partijen die gebruikmaken van een *aggregator*.

Door de combinatie van technische dienstverleners, *aggregators* en derde partijen nogmaals???: partijen (dit kunnen zowel TPPs in de zin van PSD2 zijn als derde partijen die geen PSD2-vergunning hebben) die consumenten diensten willen verlenen waar ergens een PSD2-toegang nodig is, kunnen lange ketens ontstaan. Een hypothetisch voorbeeld is een lange keten waarbij credit scoring op basis van transactiedata plaatsvindt, waarbij een partij het klantcontact heeft en een dienst verkoopt, deze partij een *aggregator* gebruikt voor de technische toegang tot de API van de bank, vervolgens diensten afneemt bij een technische dienstverlener om transacties te classificeren en op kredietwaardigheid te scoren, en gebruikmaakt van weer een andere partij om bijvoorbeeld AI-technieken toe te passen om op basis van die gegevens te besluiten of er al dan niet een lening verstrekt kan worden.

Door langere ketens ontstaat in de praktijk een gelaagdheid van activiteiten van verschillende partijen onderling waarbij het volgens gesprekspartners niet altijd duidelijk is wie de vergunningsplichtige is. Gesprekspartners stellen dat hierover verschillende standpunten zijn ingenomen door verschillende (Europese) toezichthouders. De dienstverleners in deze keten zijn bovengemiddeld vaak partijen die in meerdere Europese landen actief zijn. Er is dan ook meer Europese uniformering gewenst op dit punt. Tegelijkertijd hoeft de gelaagdheid van activiteiten in de keten niet per se een probleem te zijn. Zolang alle partijen in de keten maar heldere afspraken met elkaar maken is de velenging van de keten geen belemmering voor de veiligheid. Eén van de gesproken experts vindt dit zorgelijk, omdat de partijen die gebruikmaken van *aggregators* niet altijd een PSD2-vergunning hebben (en niet nodig hebben omdat de aggregator deze vergunning heeft) en in dat geval niet onder toezicht staan, maar wel toegang hebben tot de betaalgegevens. Zulke partijen vallen overigens wel onder de AVG en zullen daarmee ook alleen toegang hebben op basis van een AVG-geldige grondslag. De verplichtingen die horen bij toegang zijn verder ook contractueel geregeld, want de *aggregator* draagt alle risico's en vertaalt deze door naar de betrokkenen. Toch is er sprake van ongemak over de toegang tot de gegevens door partijen zonder vergunning.

Ten slotte is het belangrijk om op te merken dat de veiligheid van de betaaldienstverlening i) technisch hoog is en ii) geconcentreerd is bij banken. Het laten uitvoeren van een betaling vereist uiteindelijk een SCA via de bank en de daadwerkelijke betaling loopt vervolgens via een technisch zeer beveiligd digitaal netwerk. Voor zover uitbesteding van diensten naar niet-gereguleerde aanbieders risico's oplevert zit dit hem niet aan de 'betalingenkant' van PSD2, maar veel eerder aan de 'databeschermings- c.q. privacykant' van PSD2. Daar is behalve PSD2 de AVG een waarborg (zie hoofdstuk 5).

Conclusie

- Met betrekking tot betaaldienstverlening zijn er geen signalen dat de reikwijdte van PSD2 feitelijk voor problemen zorgt.
- Wel bestaan er zorgen op het gebied van rekeninginformatiediensten en de veiligheid van privacygevoelige betaaldata, met name daar waar deze data terechtkomen bij partijen die niet onder PSD2-toezicht staan.

Hier is de reikwijdte van PSD2 in onze ogen te beperkt. Verlenging van de keten en de groei van *aggregators* maakt het moeilijker om grip te houden op het gebruik van betaaldata, bijvoorbeeld als onduidelijk is hoe de verantwoordelijkheden voor databescherming of vergunningsplichten door de keten georganiseerd zijn. In beginsel is dit ook contractueel te borgen en biedt de AVG (en het toezicht daarop) in principe een waarborg voor gegevensbescherming. Hoofdstuk 5 gaat hier nader op in.

Zijn de vrijstellingen in PSD2 toereikend en moeten de prudentiële, operationele en consumenten-beschermingsvereisten worden gewijzigd?

PSD2 kent een aantal vrijstellingen voor het toepassen van SCA door betaal- of rekeninginformatiedienstverleners. Deze vrijstellingen moeten bezien worden tegen de achtergrond van het doel van de SCA-eis, namelijk een waarborg voor de veiligheid van betalingen en rekeninginformatiediensten. Het communicerende vat voor deze veiligheidswaarborg is gebruiksgemak. De vraag is dan in welke mate de vrijstellingen een voldoende veiligheidswaarborg bevatten zonder onnodig knellend te zijn. Bij betaalinitiatie is SCA nodig, behalve als er een vrijstelling van toepassing is. Vrijstellingen bestaan voor vertrouwde begunstigden, gedelegeerde autorisatie, bedrijfstransacties, op basis van een transactierisicoanalyse, of voor transacties onder een bepaalde drempel. In aanvulling hierop is er een aantal uitsluitingen waarop SCA geheel niet van toepassing is.

Met betrekking tot de vrijstellingsgrond voor laagrisicotransacties (de zogeheten Transaction Risk Analysis (TRA)) benoemen verschillende gesprekspartners dat deze vooralsnog niet veel gebruikt wordt, terwijl dit wel de mogelijkheid biedt voor een passende veiligheidswaarborg zonder de klantreis onnodig strikt te maken. Sommige betaaldienstverleners benoemen dat de praktijk nu soms mogelijk onnodig streng is doordat banken ook bij transacties die in de ogen van betaaldienstverleners laagrisico zijn een SCA toepassen. Banken geven in reactie hierop aan dat zij niet zonder meer kunnen vertrouwen op de risico-inschattingen van betaaldienstenverleners, des te meer daar banken ook de financiële kosten van eventuele fraude dragen.

Gesprekspartners geven verder aan dat de eisen voor TRA te stringent zijn omdat zijn voor alle transacties in een bepaalde klasse tezamen beneden een bepaalde fraudenorm moeten komen. Daarbij worden ook fraudevormen zoals spoofing meegenomen, die ongerelateerd zijn aan technische maatregelen om fraude te voorkomen. Fraude-eisen zijn gebaseerd op productgroepen, terwijl banken zeggen op meer detailniveau beter onderscheid te kunnen maken tussen categorieën transacties (frauduleus of niet). Een gesprekspartner benoemt wel dat er een afruil zit in het toepassen van een risicogedreven SCA: hoewel zo'n SCA het gebruiksgemak voor de consument kan verhogen, wordt de toepassing van SCA ook minder voorspelbaar voor de consument. Ook dat kan een frictie in de klantreis zijn.

Sommige gesprekspartners geven aan dat de handelsagentvrijstelling tot onduidelijkheid leidt omdat er in Europa geen uniforme interpretatie is van de handelsagent vrijstelling op sommige punten. Onder PSD1 gold de vrijstelling indien een handelsagent voor beide betrokken partijen optrad, maar onder PSD2 is er alleen een vrijstelling als de handelsagent voor één van de twee betrokken partijen (de betaler of de begunstigde) optreedt. In Duitsland geeft de Bafin aan dat een handelsagentvrijstelling niet mogelijk is in een online situatie. De Nederlandse toezichthouder heeft een andere interpretatie die een vrijstelling voor een online handelsplatform wel mogelijk maakt. Dat kan ertoe leiden dat grote platformen betalingen kunnen afhandelen zonder als betaalinstelling te classificeren.

Met betrekking tot de prudentiële, operationele en consumentenbeschermingsvereisten geldt dat zij vooralsnog een goede waarborg lijken voor consumentenveiligheid in het betalingsverkeer. De toename van fraudes in het betalingsverkeer zijn niet op het conto van PSD2 te schrijven, maar hangen samen met verdere digitalisering van de samenleving. Verder is PSD2 nog betrekkelijk jonge wetgeving, hebben zich er nog geen grootschalige incidenten

voorgedaan die manco's in de prudentiële, operationele en consumentenbeschermingsvereisten illustreren. Ook zijn in de gesprekken geen problemen met betrekking tot de vrijstellingen naar voren gekomen die aanpassingen van de prudentiële, operationele en consumentenbeschermingsvereisten op dit moment rechtvaardigen.

Conclusie

- De vrijstelling voor *transaction risk analysis* (TRA) wordt in de praktijk nauwelijks gebruikt, mede omdat deze lastig in te regelen is – zowel technisch als vanuit *compliance*. Marktpartijen benoemen dat zij graag de mogelijkheden voor *TRA* zouden verkennen, maar dat de regelgeving op dit punt te streng is.
- De uitwerking van de handelsagentvrijstelling lijkt in verschillende Europese landen verschillend te worden ingevuld. Het is de vraag of dit wenselijk is.
- De prudentiële, operationele en consumentenbeschermingsvereisten hoeven niet te worden gewijzigd.

5 Gegevensbescherming consumenten

Dit hoofdstuk bespreekt verschillende aspecten van gegevensbescherming, waarbij de relatie tussen PSD2 en de AVG een belangrijke rol speelt.

De implementatiewet PSD2 regelt hoe derde partijen toegang kunnen krijgen tot rekeninginformatie. Betaalgegevens zijn vaak echter ook persoonsgegevens, waarop de AVG van toepassing is.[54]

Betaalgegevens zijn gevoelig. Doordat het gedetailleerde informatie bevat over daadwerkelijke keuzes van consumenten (welk product is betaald, waar en wanneer een betaling is verricht, aan wie is betaald) kan er veel informatie uitgehaald worden over een persoon. Consumenten delen betaalgegevens dan ook het minst graag, na gegevens over de gezondheid (Bijlsma, Van der Cruisen & Jonker, 2021). Zowel PSD2 als de AVG stellen daarom ook eisen aan wat wel en niet mag met betaalgegevens.

Initiëring van betaalopdrachten mag alleen plaatsvinden met uitdrukkelijke instemming van de rekeninghouder voor de betaalopdracht of transactie.[55] Ook bij toegang tot de betaalrekening voor rekeninginformatie dienstverleners geldt dat uitdrukkelijke instemming van de rekeninghouder nodig is.[56] DNB houdt hier toezicht op. Om uitdrukkelijke instemming te geven, zal de gebruiker in ieder geval een wachtwoord, pincode en/of verificatiecode moeten intoetsen. De minister van Financiën zegt hierover:[57]

"*Toestemming voor de toegang tot de betaalrekening geeft de betaaldienstgebruiker via de afgifte van sterke cliëntauthenticatie, waarbij de rekeninghouder zich identificeert jegens de betaaldienstverlener. Met de afgifte van sterke cliëntauthenticatie is het voor de rekeninghoudende betaaldienstverlener (bank) duidelijk dat de betaaldienstgebruiker beseft dat hij gebruik maakt van de diensten van een betaaldienstverlener anders dan zijn eigen bank. De toestemming voor de toegang tot de betaalrekening kan door sterke cliëntauthenticatie niet onbewust plaatsvinden, aangezien de betaaldienstgebruiker in ieder geval een wachtwoord, pincode en/of verificatiecode (tancode) moet intoetsen. Dit moet voor elke betaling opnieuw gebeuren. Indien de begunstigde of het bedrag van de betaling verandert, moet opnieuw sterke cliëntauthenticatie worden afgegeven. Op deze manier draagt sterke cliëntauthenticatie bij aan de veiligheid*."

Bij betaalinitiatiediensten moet per transactie of reeks van transacties (bijvoorbeeld bij een abonnement) sprake zijn van uitdrukkelijke instemming. Bij rekeninginformatiediensten geldt dat de toestemming voor maximaal negentig dagen wordt gegeven.[58] Gedurende deze periode kan de rekeninginformatiedienstverlener maximaal vier keer per 24 uur toegang krijgen tot diens betaalrekening(en). Na deze negentig dagen moet de betaaldienstgebruiker opnieuw via SCA toestemming geven voor toegang tot zijn betaalrekening(en).

---

54 Als betaalgegevens B2B transacties zijn, betreft het geen persoonsgegevens. Transactiegegevens van ZZP'ers en eenmanszaken zijn ook persoonsgegevens.

55 Artikel 66 lid 2 PSD2

56 Artikel 67 lid 2 sub a PSD2

57 Verslag schriftelijk overleg Implementatiewet PSD2, Kamerstukken II 2018/19, 34813, 27, p. 7, https://www.eerstekamer.nl/behandeling/20181114/verslag_van_een_schriftelijk_3/document3/f=/vktgr30v3cz9.pdf

58 De EBA stelt voor deze termijn naar 180 dagen te verlengen om tegemoet te komen aan de behoeftes bij AISPs voor een langere termijn, zie https://www.eba.europa.eu/eba-consults-amendment-its-technical-standards-strong-customer-authentication-and-secure

Daarnaast moeten betaaldienstverleners uitdrukkelijke toestemming hebben van rekening-houdende betaaldienstgebruikers voor de toegang tot persoonsgegevens.[59] Artikel 94 van PSD2 is echter niet van toepassing als een betaaldienstverlener alleen rekeninginformatiediensten aanbiedt.[60] Ook eist PSD2 van een PISP dat zij informatie over de betalingsdienstgebruiker die is verkregen bij het verstrekken van betalingsinitiatiediensten, alleen aan de begunstigde en alleen met de uitdrukkelijke instemming van de betalingsdienstgebruiker verstrekt.[61] De AP houdt hier toezicht op.

Tabel 5.1 Vormen van toestemming in PSD2 en verwerkingsgrondslag AVG

Toestemming onder PSD2	PSD2	Dienst	Entiteit	Toezicht	Hoe PSD2-toestemming	Verwerkingsgrondslag onder de AVG
Uitdrukkelijke instemming met de betaalopdracht of transactie	66 lid 2	Initiëring van betalingsopdrachten	Van toepassing op PISP	DNB	SCA, per transactie	Het contract met de PISP creëert de AVG-grondslag
Uitdrukkelijke instemming met toegang tot de betaalrekening voor rekeninginformatie dienstverleners	67 lid 2 sub a	Informatiediensten op basis van toegang tot de betaalrekening	Van toepassing op AISP	DNB	SCA, voor negentig dagen of per keer	Meestal creëert het contract met de AISP de AVG-grondslag. Als informatie wordt opgehaald met als doel doorzenden naar een andere partij, is de AVG-grondslag toestemming. Conform de AVG moet toestemming expliciet en specifiek, vrijelijk, ondubbelzinnig, specifiek en intrekbaar zijn
Uitdrukkelijke toestemming voor de toegang van de betaaldienstverlener tot persoonsgegevens	94 lid 2	Toegang tot persoonsgegevens die betaaldata naar hun aard zijn	Niet van toepassing als een AISP alléén rekeninginformatiediensten aanbiedt (zie PSD2 33 lid 2)	AP	Toestemming moet vrij, ondubbelzinnig, geïnformeerd, specifiek, en intrekbaar zijn. In de EDPB guidelines staat intrekbaar niet. De AP geeft op haar website toelichting over hoe dit in de praktijk te doen	n.v.t.

De EDPB stelt "Uitdrukkelijke toestemming op grond van de PSD2 verschilt van de (uitdrukkelijke) toestemming op grond van de AVG". Uitdrukkelijke toestemming op grond van artikel 94, lid 2 is een aanvullend vereiste van contractuele aard.' Deze uitdrukkelijke toestemming is op vrijwel dezelfde wijze ingevuld als 'consent' in de AVG, namelijk dat deze moet plaatsvinden door middel van een duidelijke actieve handeling, op een vrijelijke, ondubbelzinnige, geïnformeerde en specifieke wijze.

Daarnaast zijn de eisen uit de AVG van toepassing indien er persoonsgegevens worden verwerkt. Dat betekent dat betaaldienstverleners naast uitdrukkelijke toestemming zoals vereist onder PSD2 ook een AVG-grondslag moeten hebben voor het verwerken van betaaldata voor zover het persoonsgegevens betreft. In geval van PISP en AISP-diensten vormt het contract met de klant de grondslag voor verwerking. Ook stelt de AVG eisen aan de verwerking

59 Artikel 94 lid 2 PSD2
60 Artikel 33 lid 2 PSD2
61 Artikel 66 lid 3 sub c

van persoonsgegevens, het proces van datadeling, de veiligheid van opslag, wijze van communicatie over verwerking van data, tijdperiode van opslag van data en de manier waarop data geanalyseerd mag worden. Tabel 5.1 geeft hier een samenvatting van.

In feite worden de voorwaarden en regels waaraan banken en betaaldienstverleners moeten voldoen met betrekking tot het verlenen van toegang voor betaalinitiatie en rekeninginformatiediensten, of de behandeling van data nadat consumenten toestemming hebben gegeven dus bepaald door het samenspel van PSD2 en de AVG. De AVG geeft daarbij een algemeen kader, terwijl PSD2 een sectorspecifieke uitwerking betreft. In beide wetten worden vergelijkbare begrippen gebruikt die niet hetzelfde zijn. Daarnaast is het zo dat waar met PSD2 data beschikbaar worden gemaakt, de AVG probeert te voorkomen dat data onnodig beschikbaar worden gemaakt. Hoe dit precies moet worden afgewogen is ingewikkeld, zowel voor toezichthouders als voor marktpartijen, en maakt het samenspel tussen PSD2 en de AVG complex.

Relevant is dat de EDPB-richtlijnen heeft gepubliceerd die zien op samenspel van PSD2 en de AVG. Het doel van de EDPB is het geven van '*guidance on data protection aspects in the context of the PSD2, in particular on the relationship between relevant provisions on the GDPR and the PSD2*.'

De punten die worden besproken in deze richtlijnen zijn:

- De juridische basis voor het verwerken van betaaldata;
- Wanneer er sprake is van explicit consent ('uitdrukkelijke toestemming');
- Hoe om te gaan met silent-party data;
- De behandeling van speciale categorieën van data;
- De toepasselijkheid van andere eisen vanuit de AVG, zoals:
    - Dataminimalisatie;
    - Transparantie en accountability;
    - Profiling.

Vanuit juridisch oogpunt zijn de twee wetten gelijkwaardig: de een betreft een Europese richtlijn die omgezet is in nationale wetgeving, de ander een verordening die directe geldigheid heeft op nationaal niveau. De relevante toezichthouders AP en DNB geven aan dat zij in de praktijk geen situaties zijn tegengekomen waarbij PSD2 en de AVG onverenigbaar zijn.

5.1 Waarborgen gegevensbescherming

Onderzoeksvragen

1. Zijn er voldoende waarborgen in de implementatiewet voor gegevensbescherming in combinatie met bestaande regelgeving?

Zijn er voldoende waarborgen in de implementatiewet voor gegevensbescherming in combinatie met bestaande regelgeving?

Een PISP beschikt, na toestemming van de cliënt, over informatie van een cliënt die een bank normaal rechtstreeks met de cliënt uitwisselt, zoals gegevens over overboekingen die de PISP heeft uitgevoerd. Een AISP beschikt, na

toestemming van een cliënt, over de saldo- en transactie-informatie die betrekking heeft op informatie van de client over diens betaalrekening bij de bank.[62]

Er zijn de volgende waarborgen voor gegevensbescherming opgenomen in PSD2:

- De PISP/AISP is op geen enkel moment in het bezit van geldmiddelen van de betaaldienstgebruiker, draagt zorg voor de beveiliging van de persoonlijke beveiligingsgegevens van de betaaldienstgebruiker, identificeert zich bij elke PIS/AIS, slaat geen gevoelige betalingsgegevens van de betaaldienstgebruiker op;[63]
- De PISP/AISP voert een beveiligingsbeleid gericht op de analyse en mitigatie van de beveiligingsrisico's inzake fraude en illegaal gebruik van persoonlijke betalingsgegevens van de betaaldienstgebruiker;[64]
- De PISP/AISP voldoet aan de vereiste procedure voor sterke cliëntauthenticatie; beveiligingsmaatregelen ter bescherming de persoonlijke beveiligingsgegevens van betaaldienstgebruikers; de voorschriften voor gemeenschappelijke en beveiligde open communicatienormen voor de identificatie, authenticatie, kennisgeving en informatieverstrekking;[65]
- De PISP/AISP voorziet in maatregelen en controlemechanismen ter beheersing van de operationele en beveiligingsrisico's met betrekking tot de aangeboden betaaldiensten; procedures voor detectie, classificatie en beheersing van incidenten; bedrijfscontinuïteitsregelingen;[66]
- De PISP/AISP verricht ten minste jaarlijks een eigen beoordeling van de operationele risico's en beveiligingsrisico's, en rapporteert daarover en over genomen risicobeheersingsmaatregelen, aan de toezichthouder en rapporteert ten minste jaarlijks aan de toezichthouder statistische data over fraude.[67]

Daarnaast moeten betaaldienstverleners zich niet alleen aan de PSD2-richtlijn houden, maar ook aan de AVG. Dat betekent dat zij naast de uitdrukkelijke toestemming van de consument zoals PSD2 die vereist, een AVG-grondslag nodig hebben om persoonsgegevens te mogen verwerken. Ook stelt de AVG eisen aan de manier waarop betaalgegevens gedeeld, bewerkt en bewaard worden. Dit staat ook expliciet in PSD2 vermeld.

Overweging 89 van PSD2 zegt over de relatie met de AVG "Het aanbieden van betalingsdiensten door de betalingsdienstaanbieders kan de verwerking van persoonsgegevens met zich meebrengen. Richtlijn 95/46/EG van het Europees Parlement en de Raad (1), de nationale voorschriften tot omzetting van Richtlijn 95/46/EG en Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad (2) zijn van toepassing op de verwerking van persoonsgegevens in het kader van deze richtlijn. Met name is het noodzakelijk, wanneer voor de toepassing van deze richtlijn persoonsgegevens worden verwerkt, dat het precieze doel wordt aangegeven, dat de desbetreffende rechtsgrondslag wordt vermeld, dat de relevante beveiligingsvoorschriften van Richtlijn 95/46/EG worden nageleefd, en dat de beginselen noodzaak, evenredigheid, doelbegrenzing en een niet-buitensporige gegevensbewaarperiode in acht worden genomen. Ook moeten in alle gegevensverwerkingssystemen die in het kader van deze richtlijn

62 Omdat in de praktijk toegang plaatsvindt door redirection, hebben AISP's geen beschikking over beveiligingsgegevens van de betaalrekening. PSD2 sluit het echter niet uit. DE AISP beschikt wel over een autorisatietoken voor toegang tot de rekening voor een periode van (nu nog) 90 dagen. Er zijn ook andere authenticatiemodellen mogelijk zoals embedded authenticatie zonder redirection naar de bank.

63 Artikel 66 & 67 PSD2

64 Artikel 5(1j) PSD2

65 Artikel 97 en 98 PSD2

66 Artikel 5(1h,j), 95 en 96 PSD2

67 Artikel 95 PSD2

worden ontwikkeld en gebruikt, de beginselen gegevensbescherming *by design* en gegevensbescherming *by default* in acht worden genomen."[68]

Artikel 26j (6). Van de implementatie wet stelt "Een rekeninginformatiedienstverlener gebruikt, verschaft zich toegang tot of slaat gegevens op uitsluitend ten behoeve van het uitvoeren van de door de betaaldienstgebruiker uitdrukkelijk gevraagde rekeninginformatiedienst, overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG en bij of krachtens de Uitvoeringswet AVG gestelde regels."

Voor derde partijen die betaaldata krijgen zonder dat zij zelf een PSD2-vergunning hebben, geldt dat PSD2 niet ziet op de bescherming van gegevens als deze eenmaal met expliciete toestemming van de consument ter beschikking zijn gesteld aan deze derde partijen. Deze derde partijen maken dan gebruik van de diensten van een *aggregator* die wel een vergunning heeft om betaaldata te kunnen ophalen. PSD2 stelt, voor zover wij weten, geen eisen aan de contractuele relatie tussen een *aggregator* en de derde partij. Als gegevens eenmaal zijn overgedragen aan een derde partij zonder PSD2-vergunning ziet de AVG toe op de verwerking en behandeling van gegevens. Voor consumenten kan dit verwarrend zijn omdat zij diensten afnemen van zo'n derde partij, terwijl het geven en intrekken van toestemming via de *aggregator* loopt.

Daarmee biedt de implementatiewet in combinatie met bestaande wetgeving (de AVG) een groot aantal waarborgen , zowel voor partijen die onder PSD2 vergunningsplichtig zijn als voor partijen die dat niet zijn. Als partijen de wetgeving naleven, dan zijn deze waarborgen in onze ogen adequaat. De vraag is uiteraard of partijen de eisen van PSD2 en de AVG daadwerkelijk naleven. Marktpartijen geven in de gesprekken die wij met ze hebben gehad aan dat zij de eisen op dit vlak naleven. In hoeverre de waarborgen in PSD2 en de AVG in de praktijk daadwerkelijk worden nageleefd, kunnen we niet beoordelen.

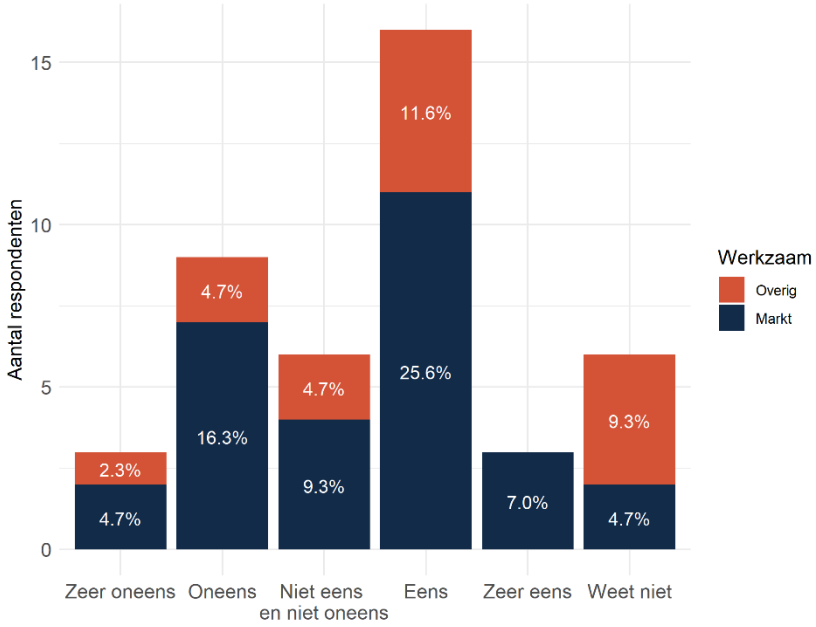
Bij DNB vindt in ieder geval een toets plaats op het moment van vergunningverlening. Daarnaast vindt er bij DNB doorlopend toezicht plaats op partijen met een vergunning. Dit geldt alleen voor partijen met een vergunning in Nederland en niet voor partijen die actief zijn op basis van *passporting*, waarbij een buitenlandse toezichthouder verantwoordelijk is. In dat geval is de buitenlandse toezichthouder verantwoordelijk voor de vergunningverlening en het doorlopend toezicht.

Daarnaast is er toezicht op naleving van de AVG door de AP. Dat toezicht moet waarborgen bieden voor gegevensbescherming van betaaldata, zowel bij partijen die onder PSD2 vallen als bij partijen die niet onder PSD2 vallen. In februari 2020 is de AP een onderzoek gestart naar bedrijven met een PSD2-vergunning met als doel 'te weten te komen of die bedrijven zich bewust zijn van de privacyrisico's die de verwerking van rekeninggegevens met zich meebrengt en of ze voldoen aan de privacyregelgeving.' De AP heeft met ons geen informatie gedeeld over eventuele bevindingen. Ook maakt de AP niet al haar sancties openbaar. Wel heeft de AP aangegeven dat haar acties richting banken met betrekking tot het incorporeren van dataminimalisatie in de API's die banken hebben ontwikkeld, uit dat onderzoek voortvloeien. Ook heeft de AP aan alle Nederlandse bedrijven met een nieuwe PSD2-vergunning een brief gestuurd met daarin de voor deze partijen relevante regels uit de AVG.

---

68 Omdat PSD2 tot stand kwam voordat de AVG er was, wordt gerefereerd naar Richtlijn 95/46/EG. Dit kan gelezen worden als AVG.

Figuur 5.1 Stelling: Gegevensbescherming is voldoende gewaarborgd in de huidige PSD2-regelgeving



Bron: SEO Economisch Onderzoek op basis van een mini-enquête onder 43 interviewpartners

De meerderheid van de gesprekspartners (42,2 procent) geeft in de online enquête aan eens of zeer eens te zijn dat er voldoende waarborgen zijn voor gegevensbescherming in de huidige PSD2-regelgeving (Figuur 5.1). Een deel van de gesprekspartners (25,7 procent) is het oneens of zeer oneens met de stelling dat gegevensbescherming voldoende is gewaarborgd in PSD2.

Voorbeelden in gesprekken die zien op gegevensbescherming benoemen het risico dat gegevensbescherming bij buitenlandse partijen die onder toezicht van andere lidstaten vallen minder goed is. Daarnaast benoemen ze het risico dat gegevensbescherming bij partijen die niet onder PSD2 vallen (maar wel over betaaldata beschikken) minder goed is. Deze partijen vallen immers niet onder het doorlopend toezicht van DNB. Wel vallen deze partijen onder de AVG. Het toezicht door de AP is echter minder intensief dan dat van een sectorale toezichthouder, die ex post toezicht houdt op basis van een vergunningstelsel, daardoor dichter op de markt staat en vaak over meer mensen en middelen beschikt. Wij hebben in gesprekken overigens geen concrete indicaties gekregen van dergelijke misstanden.

Een relevante waarborg voor gegevensbescherming is dataminimalisatie. De AP heeft banken middels een brief aan de NVB opgeroepen "om zorgvuldig na te gaan of de AVG-verplichtingen ten aanzien van dataminimalisatie worden nageleefd in alle gegevensverwerkingssystemen die in het kader van PSD2 zijn/worden ontwikkeld en gebruikt. Indien dit niet het geval is zullen de NVB-leden spoedig de nodige maatregelen moeten nemen." Marktpartijen geven aan dat zij behoefte hebben aan meer concrete *guidance* vanuit de AP over wat er nodig is om te voldoen aan deze oproep. Ze ervaren de huidige *guidance* van de AP als te beperkt. De AP controleert in principe alleen achteraf of er aan de eisen van de AVG voldaan is, maar vertelt niet vooraf hoe aan deze eisen te voldoen. De verplichting om de wet na te leven, rust immers op partijen zelf.[69]

[69] Overigens biedt AVG de mogelijkheid tot de goedkeuring van gedragscodes (art. 40/41 AVG), tot het certificeren van verwerkingen (art. 42/43 AVG), en tot het formeel vooraf raadplegen van de AP (art. 36 AVG).

Sommige gesprekspartners vragen zich daarbij af waarom banken en niet AISP's verantwoordelijk zijn voor dataminimalisatie. De EDPB en de AP geven op dit punt aan dat zowel de banken als de AISP/ PISP verantwoordelijk zijn voor dataminimalisatie. Ook geven banken aan dat het achteraf implementeren van de eisen die de AP stelt aan de API's kostbaar is. Daarbij versterkt volgens gesprekspartners het grote aantal ontwerpkeuzes dat gemaakt moet worden bij de implementatie van dataminimalisatie de tendens waarbij API's van verschillende banken van elkaar verschillen, zowel op nationaal als op internationaal niveau.

Tot slot geven meerdere gesprekspartners aan dat volgens hen de eisen van PSD2 op het punt van datadelen in strijd lijken met de eisen van de AVG: waar PSD2 zegt dat derde partijen volledige toegang moeten krijgen tot betaaldata als de cliënt daar toestemming voor geeft, geeft de AP aan dat banken die toegang op verzoek van de TPP moeten inperken. Deze respons van partijen laat zien dat de relatie van de AVG en PSD2 voor velen een uitdagend onderwerp blijft. Van dergelijke strijdigheid is immers geen sprake, omdat de AISP bepaalt welke gegevens hij nodig heeft gebaseerd op de uitdrukkelijke toestemming van de klant. De bank moet die vraag kunnen faciliteren en mag niet vooraf controleren of de door de klant gegeven toestemming aan de AISP overeenkomt met de gegevens die nodig zijn voor het verrichten van de betreffende betaaldienst door de AISP. Als de AISP gerechtvaardigde redenen heeft dat wel alle gegevens noodzakelijk zijn dan kan de AISP ook alle gegevens ophalen. Een open vraag die wij zien is of banken een toets mogen doen of al de gevraagde gegevens wel nodig zijn voor de betreffende dienst.

Conclusie

- De PSD2 en de AVG bieden gezamenlijk veel waarborgen voor gegevensbescherming en er zijn geen misstanden bekend. De implementatiewet biedt in combinatie met bestaande wetgeving (de AVG) in theorie voldoende adequate waarborgen voor gegevensbescherming.
- PSD2 eisen gelden alleen voor betaaldienstverleners (vergunningsplichtig of niet). DNB voert een toets uit bij vergunningverlening. Ook houdt DNB doorlopend toezicht.
- De eisen van de AVG gelden ook voor partijen zonder PSD2-vergunning die (bewerkte) persoonsgegevens krijgen via partijen zoals *aggregators* die wel een PSD2-vergunning hebben. Hier houdt de AP toezicht.
- In de praktijk is het toezicht voor derde partijen die via *aggregators* diensten verlenen, waarbij zij gebruikmaken van betaaldata, minder ingrijpend voor zover deze derde partijen niet onder PSD2 toezicht staan. AVG toezicht staat namelijk meer op afstand. Dit brengt risico's met zich mee.
- Kanttekening daarbij is dat wij behoudens de informatie uit gesprekken met partijen, geen feitelijk zicht hebben op hoe PSP's, PISP's en AISP's in de praktijk uitvoering geven aan de eisen rondom gegevensbescherming.
- Een ander risico betreft mogelijk buitenlandse partijen waar noch DNB noch de AP zicht op hebben. Hier is de mate van gegevensbescherming afhankelijk van de wijze waarop buitenlandse toezichthouders hun toezicht invullen. Die invulling kan immers verschillen, ook al zijn de kaders gelijk.
- Voor marktpartijen was en is onduidelijk hoe ze in de praktijk precies moeten voldoen aan de gecombineerde eisen uit PSD2 en de AVG. Er is behoefte aan een gezamenlijke visie of standpunt, wat zekerheid zou bieden.

5.2 Toegang tot gegevens

Onderzoeksvragen

1. Is voldoende geborgd dat er geen toegang is tot meer gegevens dan noodzakelijk?
2. Weten mensen voldoende waar ze ja tegen zeggen als ze toestemming geven voor toegang tot hun betaalgegevens?
3. Wordt de toestemming voldoende expliciet en specifiek gevraagd?

4. Geeft de consument bewust toestemming (i.e. is zich volledig bewust van de gevolgen van het geven van toestemming)?
5. Voelt de consument zich vrij om toestemming te weigeren?
6. Kunnen mensen eenvoudig terugkomen op een gegeven toestemming?
7. Hoe kunnen consumenten worden geholpen bij het bewaren van overzicht ten aanzien van de gegeven toestemmingen (dat kan d.m.v. het dashboard van banken, maar zijn er ook andere manieren)?

Is voldoende geborgd dat er geen toegang is tot meer gegevens dan noodzakelijk?

De drie belangrijkste vraagstukken die om dit kader spelen zijn: *silent party data*, bijzonder persoonsgegevens en dataminimalisatie. Al deze begrippen komen voort uit de AVG en worden besproken in de *guidelines* van de EDPB. PSD2 kent deze begrippen niet en stelt niet dat er vanuit de bank geen toegang mag zijn tot meer gegevens dan noodzakelijk. Wel stelt PSD2 dat een PISP geen gegevens vraagt van de betalingsdienstgebruiker die niet nodig zijn voor het verstrekken van de betalingsinitiatiedienst[70], terwijl een AISP zich geen toegang mag verschaffen tot gegevens voor andere doelstellingen dan het uitvoeren van de door de betalingsdienstgebruiker uitdrukkelijk gevraagde rekeninginformatiedienst.[71]

Silent party data betreft betaaldata van betaalrekeninghouders die geen toestemming hebben gegeven voor het delen van hun betaaldata, die toch zichtbaar worden voor derde partijen omdat iemand aan wie zij een betaling hebben gedaan of van wie zij een betaling hebben ontvangen, wel toestemming heeft gegeven voor het delen van hun betaaldata. Dit betreft in principe alle betaaldata die een AISP ophaalt van de betaalrekening van een klant, die geen betaaldata bevat over andere personen dan de klant zelf.

De vraag is op welke grond de AISP deze data mag verwerken en de bank deze mag verstrekken. De EDPB heeft in haar *guidelines* aangegeven dat verwerking mag, omdat de AISP en ASPSP hierbij een gerechtvaardigd belang kunnen hebben zoals bedoeld in de AVG.[72] De EDPB stelt wel dat dit gerechtvaardigd belang geen grond van verwerking is voor andere verwerking dan voor de rekeninginformatiedienst zoals bedoeld in PSD2. Dat betekent in de praktijk dat partijen dus ook geen toestemming kunnen vragen voor verdere verwerking, omdat het vragen van toestemming an sich al om verwerking van de data zou vragen.

In de AVG bestaat het onderscheid tussen gewone persoonsgegevens en bijzondere persoonsgegevens. In die laatste categorie vallen bijvoorbeeld gegevens over etnische afkomst, politieke opvattingen, levensovertuiging of vakbondslidmaatschap. Betaaltransacties kunnen hierover gegevens bevatten, denk aan een afschrift van een vakbond of politieke partij. Deze gegevens mogen pas worden verwerkt wanneer hiervoor uitdrukkelijke toestemming is verleend.[73] Deze toestemming is strikter dan de gewone toestemming voor persoonsgegevens. PSD2 kent dit onderscheid niet.

Tijdens het proces van vergunning verlening voor AISP's, PISP's of de beoordeling van API's, wordt niet gekeken naar de wijze waarop deze omgaan met bijzondere persoonsgegevens, omdat dit geen onderdeel vormt van de PSD2-vergunningsaanvraag. Binnen de AVG is verwerking van bijzondere categorieën persoonsgegevens alleen mogelijk met uitdrukkelijke toestemming of als de verwerking noodzakelijk is vanwege zwaarwegend algemeen

70 Artikel 66 lid 3 sub f PSD2
71 Artikel 67 lid 2 sub f PSD2
72 De gerechtvaardigd belang-toets bevat een case-by-case afweging van belangen die de AISP of PISP vooraf zelf moet uitvoeren.
73 Of een andere uitzonderingsgrond zoals opgesomd in art. 9 AVG.

belang op grond van EU- of nationale wetgeving. In de afwezigheid van een uitzonderingsgrond op het verwerkingsverbod moeten betalingsdienstaanbieders maatregelen nemen om de verwerking te voorkomen.[74] Aanbieders van betaalrekeningen zijn op grond van PSD2 echter wettelijk verplicht om verzoeken van derden in te willigen. Specifiek verplicht PSD2 betaaldienstaanbieders om dezelfde informatie aan AISP's te verstrekken als waartoe de betalingsdienstgebruiker online toegang heeft. Dat omvat bijzondere categorieën persoonsgegevens. Om vast te kunnen stellen of sprake is van bijzondere persoonsgegevens bij specifieke betaaldata zou een uitgebreide analyse nodig zijn van betaaldata door banken of AISP's dan wel PISP's. Al met al is onduidelijk hoe banken, AISPs en PISPs in de praktijk moeten omgaan met bijzondere categorieën persoonsgegevens, ondanks de *guidance* van de EDPB: hoe voorkom je in de praktijk dat je over gegevens beschikt die je niet mag hebben, of hoe vraag je op het juiste moment toestemming.

Het concept dataminimalisatie komt voort uit de AVG die bepalingen bevat die moeten borgen dat er geen toegang is tot meer persoonsgegevens dan noodzakelijk gegeven de grondslag. PSD2 kent het concept dataminimalisatie niet. Wel stelt PSD2 dat de destijds geldende privacyrichtlijn van toepassing is en daarmee dus nu de AVG. De API's die banken hebben ontwikkeld, zijn in eerste instantie niet gebouwd om dataminimalisatie te faciliteren. Omdat het geen PSD2-eis betreft, voorzien de richtlijnen omtrent de beoordeling waar DNB op toetste daarin ook niet. De meeste gesprekpartners geven aan dat de samenhang tussen PSD2 en de AVG onduidelijk was op het moment dat vanuit PSD2 deadlines gehaald moesten worden voor het ontwikkelen van API's. Het gevolg is dat op dit moment AISP's geen data-aanvraag kunnen doen bij een bank die erop gericht is om alleen een heel specifieke deelverzameling van gegevens op te vragen. De API-interface faciliteert dit immers niet.

Omdat banken op dit moment nog geen dataminimalisatie faciliteren, ligt de praktische verantwoordelijkheid voor dataminimalisatie bij algemene data-uitvragen op dit moment bij AISP's en PISP's. Gesprekspartners geven aan dat deze partijen soms belang hebben bij het minimaliseren van de data die ze krijgen, want 'wat je niet hebt, kun je ook niet kwijtraken'. Derde partijen minimaliseren zo de risico's die ze zelf lopen op datalekken. Uit gesprekken met marktpartijen komt naar voren dat AISPs en PISPs beperkt contact hebben met de AP. Wel is er een questionnaire geweest vanuit de AP naar een aantal partijen over de wijze waarop ze met de vereisten van de AVG omgaan. Wij hebben geen inzicht in deze questionnaire gehad noch in de bevindingen op basis van deze questionnaire.

De AP is volgens geïnterviewde partijen momenteel in gesprek met sommige banken over de implementatie van dataminimalisatie in de API's van banken. De AP toetst daarbij alleen achteraf of de wijze waarop dataminimalisatie is vormgegeven in overeenstemming is met de AVG.

Voor marktpartijen is het in de praktijk nog onduidelijk hoe ze dataminimalisatie precies moeten implementeren aangezien er veel dwarsdoorsnedes van data denkbaar zijn. Denk bijvoorbeeld aan specifieke typen betalingen, een specifiek tijdsinterval van de betaling, de hoogte van een betaling, de frequentie waarmee betalingen plaatsvinden, betalingen aan een bepaalde tegenpartij etc. Het aanpassen van de API's om dataminimalisatie mogelijk te maken zal extra kosten opleveren. Banken geven ook aan dat er in de praktijk wel eens weinig gebruikgemaakt zou kunnen worden van de mogelijkheden tot dataminimalisatie via de bankinterface, maar dat partijen liever achteraf dataminimalisatie doen.

Via marktpartijen hebben we inzage gekregen in de brief die de AP heeft gestuurd. Deze brief stelt 'In het geval dat niet alle betaalrekeninginformatie noodzakelijk is voor de uitvoering van de rekeninginformatiedienst, dient de AISP voorafgaand aan de verzameling van de betaalrekeninggegevens een selectie te maken van de gegevens die

74 Of een andere uitzonderingsgrond zoals opgesomd in art. 9 AVG.

noodzakelijk zijn en zal de AISP deze selectie in haar verzoek om toegang aan de bank kenbaar moeten maken.' Voor banken is onduidelijk hoe zij de API's vorm moeten geven zodat aan de principes van dataminimalisatie is voldaan. Zij hebben behoefte aan praktische guidance die uitstijgt boven abstracte voorbeelden hoe zij dergelijke zaken in de praktijk kunnen vormgeven, bijvoorbeeld door informele contacten over specifieke gevallen. De AP toetst alleen achteraf of een implementatie voldoet. Dit creëert risico voor marktpartijen.

De verantwoordelijkheid om te bepalen welke data een derde partij wil, ligt daarmee op dit moment feitelijk bij de AISP. Een in onze ogen relevante vraag is of banken een check mogen doen of een bepaalde selectie die een AISP aangeeft nodig te hebben bij een bepaalde uitvraag, ook daadwerkelijk nodig is. Banken kunnen immers niet zomaar toegang weigeren aan derde partijen tot bepaalde delen van de data die de cliënt wil delen, dat zou in strijd zijn met PSD2. Daarnaast zou dit ook vanuit mededingingsperspectief kwetsbaar zijn: op deze manier krijgen banken toch weer de zeggenschap over wie wel of niet toegang tot de betaaldata krijgt.

Marktpartijen die in meerdere landen actief zijn, geven aan dat de discussie over hoe dataminimalisatie in API's door te vertalen in andere Europese landen niet lijkt te spelen. Kennelijk zijn de maatschappelijke zorgen over het gebruik van betaaldata hier minder groot, of maken de APS van die landen zich er minder druk over. Het risico bestaat daarmee dat implementatie van dataminimalisatie vooralsnog alleen in Nederland plaatsvindt. Daarmee worden de verschillen tussen Nederlandse API's en API's in andere landen groter, terwijl juist mede het doel van de PSD2 is te komen tot meer harmonisatie binnen Europa.

Conclusie

- PSD2 bevat geen vereisten van dataminimalisatie of bepalingen die betaaldata classificeren als *silent party* data en bijzondere persoonsgegevens. Dit zijn bepalingen uit de AVG.
- Zowel dataminimalisatie als het omgaan met bijzondere persoonsgegevens is volgens gesprekspartners nog niet geïmplementeerd in de API's van banken.
- Een partij met een PSD2-vergunning die AISP-diensten biedt, krijgt op dit moment dus mogelijk meer toegang tot betaaldata dan strikt noodzakelijk voor de diensten die zo'n partij verleent. Er zijn echter ook AISP's die voor hun bedrijfsmodel wel toegang tot alle data nodig hebben.
- Op dit moment zijn banken in gesprek met de AP over hoe dataminimalisatie vorm te geven. Dat is complex omdat het aantal verschillende doorsnedes van data groot is en omdat banken van PSD2 niet a priori derde partijen mogen uitsluiten van toegang tot specifieke data. Partijen geven ook aan dat het kostbaar is om te implementeren.
- Er is vanuit de markt behoefte aan praktische *guidance*, bijvoorbeeld in de vorm van informele *guidance* of concrete gevallen, over welke implementatie AVG-proof is. De AP toetst alleen achteraf of een implementatie voldoet. Dit creëert risico voor marktpartijen.
- Een risico dat marktpartijen zien is dat de mogelijkheid om beperkte data uit te vragen maar beperkt gebruikt wordt en dat nationale en internationale verschillen in de API's van banken verder uiteenlopen. De discussie over dataminimalisatie speelt, voor zover wij hebben kunnen achterhalen, in andere landen niet, ondanks dat volgens gesprekspartners dataminimalisatie in die landen niet in de API's van banken is meegenomen.

Weten mensen voldoende waar ze ja tegen zeggen als ze toestemming geven aan toegang tot hun betaalgegevens?

De PSD2 bevat twee soorten eisen voor toegang tot betaalgegevens: uitdrukkelijke instemming en uitdrukkelijke toestemming. DNB houdt toezicht op uitdrukkelijke instemming, terwijl de AP heeft aangegeven wat zij onder uitdrukkelijke toestemming verstaat, zie ook Tabel 5.1. Gebruikers van AISP- en PISP-diensten geven dus altijd

uitdrukkelijke instemming en soms ook nog uitdrukkelijke toestemming. Uitdrukkelijke toestemming is daarbij alleen relevant voor PISP-diensten.

Mensen weten waar ze ja tegen zeggen, als ze voldoende zijn geïnformeerd. Het is dus van belang welke informatie ze krijgen. PSD2 kent een aantal informatieverplichtingen voor een betaaldienstverlener. Overweging (54) van de richtlijn stelt hierover dat deze informatieverplichtingen als doel hebben 'informatie verstrekken aan betalingsdienstgebruikers, die allen dezelfde, kwalitatief hoogwaardige en duidelijke informatie over betalingsdiensten dienen te ontvangen om overal in de Unie met kennis van zaken een vrije keuze te kunnen maken.' Artikel 52 PSD2 en bevat onder andere een verplichting voor de aanbieder om de gebruiker in te lichten over de voornaamste kenmerken van de aangeboden rekeninginformatiedienst.

De AVG stelt dat toestemming dient te worden gegeven door middel van een duidelijke actieve handeling, waaruit blijkt dat de betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens instemt.[75] De EDPB geeft ook aan hoe dit ingevuld moet worden in het kader van uitdrukkelijke toestemming in het kader van artikel 94 PSD.[76] Het vragen van uitdrukkelijke toestemming kan gebeuren in het proces dat de gebruiker doorloopt na het downloaden van de softwareapplicatie van een TPP – bijvoorbeeld door te klikken op een specifiek vakje.

Als betaaldienstverleners voldoen aan deze wettelijke verplichtingen van PSD2 en de AVG, worden gebruikers in ieder geval in staat gesteld om zich te informeren over waar ze ja tegen zeggen. De AFM houdt ex post toezicht op de informatieverstrekking door PISP's en AISP's. We hebben geen informatie over de handhavingsactiviteiten van de AFM op dit punt.

Het Maatschappelijk Overleg Betalingsverkeer (MOB) heeft *good practices*[77] opgesteld waarin zeven vragen zijn opgenomen aan rekeninginformatiedienstverleners om vooraf aan het moment dat de gebruiker toestemming geeft aan de aanbieder voor toegang tot zijn of haar rekening, bondig en begrijpelijk te beantwoorden. Bij de uitwerking van de *good practices* is overlegd met de ACM en AP over de mededingings- en privacyaspecten. De AFM maakt geen deel uit van het MOB, maar kan zich wel vinden in de lijn van de MOB.

Het MOB zou graag zien dat AISP's hun klanten een antwoord geven op de volgende vragen:
- Wie vraagt toegang tot mijn accountgegevens? Hoe is de dienst geregeld?
- Welke dienst die mijn gegevens nodig heeft, biedt de AISP aan?
- Welke gegevens van mijn betaalrekening gebruikt de AISP?
- Waarvoor gebruikt de AISP de gegevens nog meer?
- Welke gegevens deelt de AISP met welke derde partijen en met welk doel?
- Waar en hoe kan ik mijn eerder gegeven toestemming intrekken?
- Waar kan ik aanvullende informatie vinden?

De good practices zijn verspreid onder de leden van het MOB, die ze onder de aandacht van hun leden hebben gebracht. Onduidelijk is daarnaast of de *good practices* in de praktijk worden toegepast en wie verantwoordelijk is

75 Art. 4 onderdeel 11 AVG

76 Zie https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/financien/betaaldiensten#aan-welke-eisen-voor-uitdrukkelijke-toestemming-moet-ik-als-betaaldienstverlener-voldoen-6871. De AP schrijft 'In een digitale omgeving kan dat bijvoorbeeld in de vorm van een apart venster. Zoals een pop-up of een aan te vinken checkbox in een dialoog.'

77 Zie onder het kopje 'publicaties 2020' op https://www.dnb.nl/inclusieve-samenleving/maatschappelijk-overleg-betalingsverkeer/.

voor de controle of de *good-practices* ook worden nageleefd. In het MOB is afgesproken de toepassing van deze *good-practices* in 2022 te evalueren.

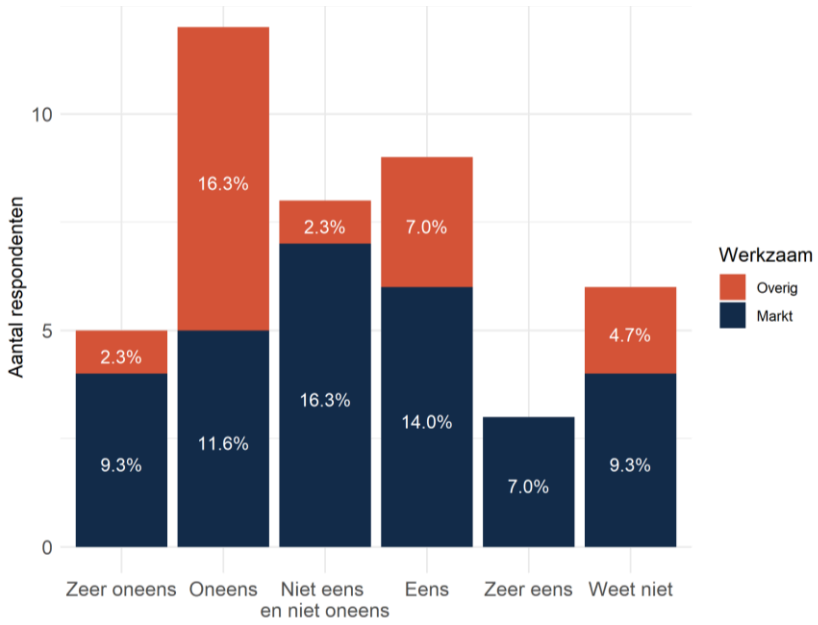
De AP heeft partijen met een nieuwe PSD2-vergunning een brief gestuurd waarin ze hen informeren over hun verplichtingen in het kader van de AVG en is van plan dit voorlopig bij alle nieuwe toetreders te doen. Hiermee bereikt de toezichthouder echter niet de partijen voor wie een PSD2-vergunning onderdeel is van andere vergunningen die deze partijen hebben en ook niet partijen die middels *passporting* actief zijn in Nederland en onder AVG-toezicht in een andere lidstaat vallen. Ook de *good-practices* van het MOB bereiken deze partijen niet. Daarmee bestaat het risico dat buitenlandse partijen minder goed op de hoogte zijn van de vereisten van de AVG en de good-*practices* van het MOB.

Voor een 5-tal aanbieders van AISP diensten aan consumenten[78] hebben we het proces van toestemming geven doorlopen en nagegaan welke informatie gebruikers allemaal krijgen gedurende het proces. Tijdens het proces waarin de gebruiker een contract aanging werd onder meer informatie gegeven over:

- Wat de app in kwestie voor diensten levert en met welk doel;
- Samenwerking met derde partijen en wat die partijen met de data doen;
- Wat er met de opgehaalde data gebeurt op het moment dat de gebruiker het contract opzegt;
- Wat de gebruiker moet doen om persoonsdata te verwijderen;
- De bewaartermijn voor wettelijk verplicht te bewaren data;
- Dat het contract beëindigd kon worden.

Deze informatie werd soms direct in het proces gegeven, soms moest daarvoor doorgeklikt worden naar een bijlage, zoals het privacy statement of de gebruiksvoorwaarden. De informatie wordt niet gegeven in de structuur van de *good-practices* die de MOB heeft opgesteld, maar biedt wel vrijwel dezelfde informatie.

Figuur 5.2 Stelling: Consumenten weten waar ze wel en geen toestemming voor geven als ze gebruikmaken van betaalinitiatiediensten en rekeninginformatiediensten



78 In totaal zijn er 7 aanbieders van B2C diensten met een vergunning van DNB voor diensten 7 of 8. Daarvan hebben we er 5 bekeken.

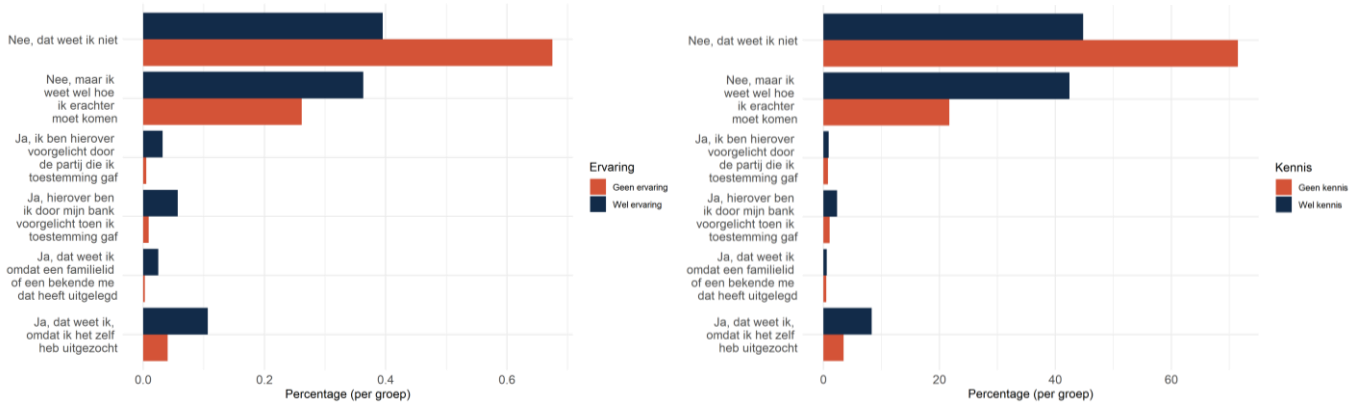
Bron: SEO Economisch Onderzoek op basis van een mini-enquête onder 43 interviewpartners

De online enquête (Figuur 5.2) geeft aan dat bijna 40 procent van de gesprekspartners het oneens is met de stelling 'consumenten weten waar ze wel en geen toestemming voor geven als ze gebruikmaken van betaalinitiatiediensten en rekeninginformatiediensten, terwijl ongeveer 28 procent aangeeft het eens of zeer eens te zijn met deze stelling. De antwoorden zijn relatief gespreid en gesprekspartners hebben dan ook uiteenlopende visies op deze vraag.

De uiteenlopende antwoorden op deze vraag zijn terug te voeren op het perspectief dat gesprekspartners hebben. Sommige gesprekspartners geven aan dat consumenten geen besef hebben van alles wat met hun betaaldata gedaan kan worden, als deze data eenmaal in handen zijn van derde partijen. Ook zijn er gesprekspartners die aangeven dat consumenten zich niet bewust zijn van alle privacyvoorwaarden die gesteld worden en daarom niet weten waar ze toestemming voor geven. Als illustratief wordt benoemd dat de privacy statements nauwelijks geopend worden.[79] Andere gesprekspartners geven aan dat consumenten die AISP-diensten gebruiken ook weten waarom ze deze diensten gebruiken en zich dus ook bewust zijn van waar ze toestemming voor geven.

We kunnen in de enquête onderscheid maken tussen consumenten die aangeven daadwerkelijk gebruik te maken van PSD2 en consumenten die aangeven kennis te hebben van PSD2. Deze groepen overlappen maar ten dele. Uit de consumentenenquête komt het beeld naar voren dat consumenten die aangeven gebruik te maken van PSD2 (en dus ervaring hebben) meer weten van *surcharging* en van twee-factor authenticatie (Figuur 5.3, 5.4 en 5.5). Ook laten de resultaten zien dat consumenten die aangeven kennis te hebben van PSD2 meer weten van *surcharging* en van twee-factor authenticatie. Tegelijkertijd wordt ook zichtbaar dat consumenten die kennis hebben van PSD2 of gebruikmaken van PSD2 beter weten waar ze terechtkunnen met hun klachten, of ervan overtuigd zijn dat ze erachter kunnen komen waar ze met een eventuele klacht terechtkunnen. Ook laten de resultaten zien dat kennis voor alle vragen uitmaakt, maar dat ervaring vooral uitmaakt voor vragen die direct gerelateerd zijn aan de diensten die AISP's aanbieden. Dit suggereert dat consumenten die gebruikmaken van PSD2 meer weten van relevante zaken rond PSD2 (zoals twee-factor authenticatie en het intrekken van hun toestemming) en dus ook beter weten waar ze ja tegen zeggen.

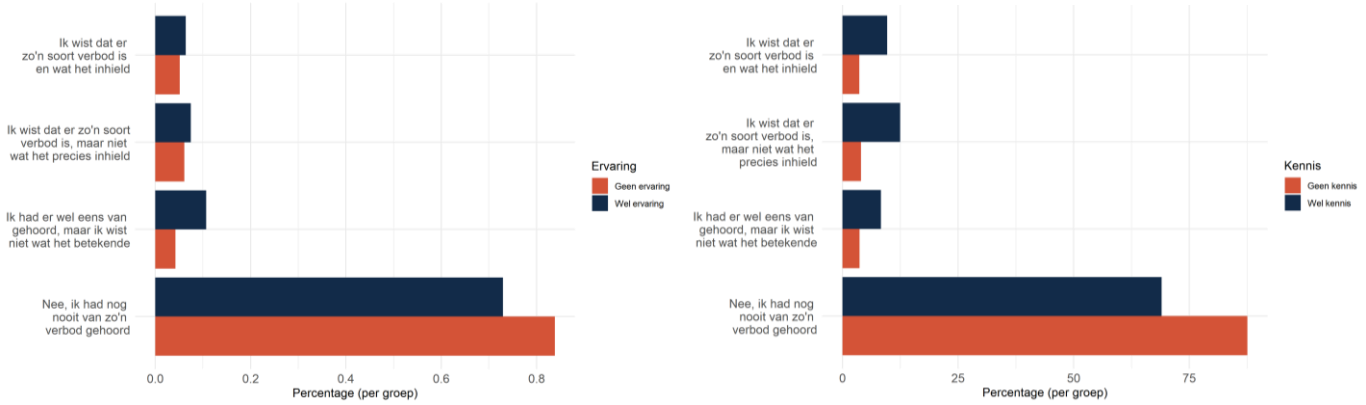
Figuur 5.3 Wist u hoe u toestemming voor toegang tot uw betaalgegevens kunt intrekken? (uitgesplitst naar kennis van en ervaring met PSD2)



Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2486

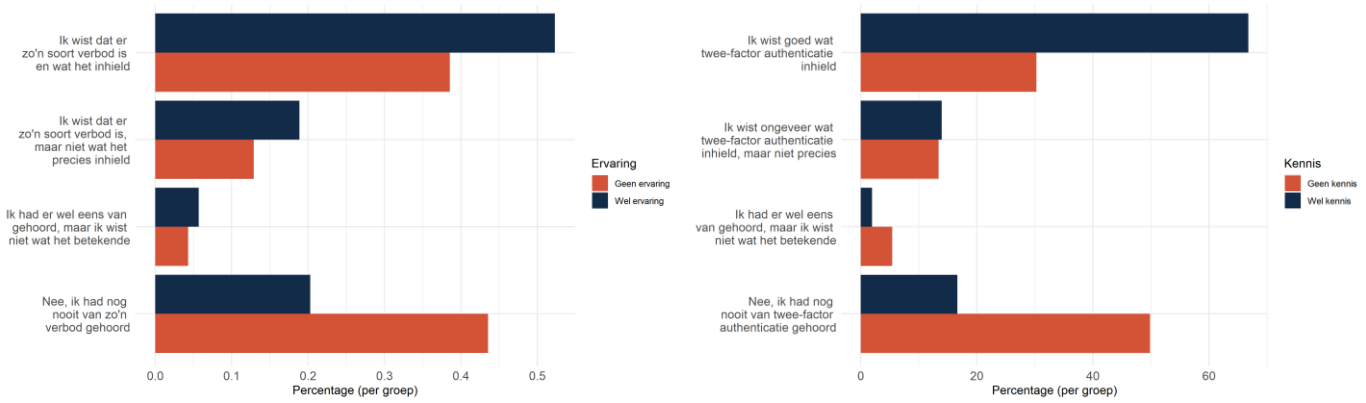
79 Hierin verschilt het gedrag van consumenten bij PSD2-diensten niet van andere typen diensten. Zie Steinfeld (2016)

Figuur 5.4 Wist u voor u deze vragenlijst invulde dat er een verbod op surcharging bestond? (uitgesplitst naar kennis van en ervaring met PSD2)



Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2484

Figuur 5.5 Wist u voor u deze vragenlijst invulde wat twee-factor authenticatie inhield? (uitgesplitst naar kennis van en ervaring met PSD2)



Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2483

De indruk op basis van de gesprekken met marktpartijen is dat consumenten die op dit moment gebruikmaken van PSD2 dat bewust doen, dat wil zeggen dat ze op zoek zijn naar een dienst en daarvoor een specifieke app uitproberen. Of consumenten zich volledig bewust zijn van het geven van toestemming is niet meetbaar, tenzij consumenten vlak na of op het moment van toestemming geven bevraagd worden, aangezien consumenten de context na verloop van tijd ook weer vergeten.

Bij meer voorkomende vormen van datadeling, denk bijvoorbeeld aan het geven van toestemming aan websites om cookies op te slaan, of de toestemming die consumenten aan Big Techs moeten gegeven voor het gebruik van hun diensten, blijkt dat consumenten relatief makkelijk toestemming geven en niet altijd stilstaan bij de gevolgen van het geven van toestemming. Er is sprake van een privacyparadox die breed in de economische literatuur wordt onderschreven: als je het ze vraagt, geven mensen aan dat ze hun persoonlijke data niet graag delen, maar in de praktijk delen ze data al voor relatief kleine bedragen of in ruil voor gratis diensten (zie bijvoorbeeld Athey, Catalini & Tucker, 2017, en Acquisti, Taylor & Wagman, 2016). Als de mogelijkheden van PSD2 om toegang te geven tot de betaalrekening een succes zou worden (wat het nu nog niet is), is er geen reden om aan te nemen dat dit gedrag van consumenten in het geval van PSD2 anders zou zijn dan in andere markten.

Conclusie

- Op het moment dat consumenten actief een handeling verrichten om toegang (zowel in het kader van instemming als toestemming) te geven tot hun betaalgegevens, zijn ze zich ervan bewust dat ze op dat moment ja zeggen tegen toegang tot hun betaalgegevens. Daarvan zijn consumenten zich dus voldoende bewust.
- Dat betekent niet dat consumenten volledig beseffen wat de potentiële gevolgen (of risico's) daarvan kunnen zijn, daarvoor moeten consumenten zich namelijk informeren.
- Als AISP's zich aan de eisen van PSD2 en de AVG houden, kunnen gebruikers zich in principe voldoende informeren over meerdere aspecten van de dienstverlening van de AISP of PISP waarmee ze een contract hebben. De PSD2 en de AVG bevatten immers voorschriften waar deze betaaldienstverleners zich aan moeten houden.
- Een nalevingsonderzoek met betrekken tot de informatieverstrekking door AISP's en PISP's vormt geen onderdeel van deze evaluatie. Op basis van de *onboarding* processen bij een 5-tal apps van AISP concluderen wij dat deze partijen voldoende informatie beschikbaar stellen aan de klant en dat AISP's in de praktijk proberen aan de eisen van de AVG te voldoen.
- Of consumenten ook gebruikmaken van deze mogelijkheid om zich te informeren en daardoor weten waar ze ja tegen zeggen, is op basis van de data die beschikbaar zijn niet meetbaar.
- Sommige gesprekspartners geven aan dat ze niet het idee hebben dat consumenten echt weten waar ze precies toestemming voor geven. In de praktijk is moeilijk vast te stellen in hoeverre dit klopt.
- De mate waarin consumenten zich bewust zijn van de gevolgen van het geven van toestemming is niet meetbaar op basis van de ingewonnen data.
- Uit het consumentenonderzoek blijkt wel dat consumenten die kennis hebben van PSD2 of die gebruikmaken van PSD2-diensten ook meer weten over PSD2, bijvoorbeeld over SCA, *surcharging*, of waar ze terechtkunnen met klachten. Dit suggereert dat die groep consumenten informatie beter kan plaatsen, omdat deze groep er al kennis van of ervaring mee heeft.

Wordt de toestemming voldoende expliciet en specifiek gevraagd?

Wij interpreteren deze vraag in het licht van artikel 94 lid 2 PSD2, het gaat hier om een onderdeel van hetgeen de EDPB verstaat onder uitdrukkelijke toestemming van de betaaldienstverlener tot persoonsgegevens.[80] Onder uitdrukkelijke toestemming valt volgens de AP dat toestemming specifiek en ondubbelzinnig is.[81] Specifiek betekent dat het voor de betrokkene duidelijk en begrijpelijk moet zijn om welke verwerking, van welke gegevens, door welke verwerkingsverantwoordelijke, voor welke doelen het gaat en, als daarvan sprake is, aan welke derde partijen persoonsgegevens worden verstrekt. Ondubbelzinnig betekent dat de toestemming moet worden gegeven via een *actieve* handeling of verklaring, zodat het duidelijk is dat de klant heeft ingestemd met de specifieke verwerking.

Over de precieze bewoording en wijze waarop betaaldienstverleners toestemming vragen zijn geen gegevens beschikbaar. In de gesprekken met betaaldienstverleners komt naar voren dat zij zich bewust zijn van de eisen die de AVG stelt. Ook hebben wij voor een 5-tal PSD2-apps het *onboarding* proces doorlopen.[82] Daaruit komt naar voren dat consumenten gedurende het proces eerst informatie krijgen over het doel van het contract dat ze met de AISP

80 Voor partijen die alleen AISP-diensten bieden, geldt de vereiste van uitdrukkelijke toestemming niet. De AP houdt daar ook geen toezicht op. Deze vraag is daar dus niet op van toepassing. Het contract met de AISP en PISP voor de te leveren dienst creëert de grondslag voor AVG-verwerking. Ook daar gaat deze vraag niet over.

81 De wijze waarop de AP het begrip uitdrukkelijke toestemming uit PSD2 art 94 invult, komt overeen met art. 4 onderdeel 11 AVG.

82 Omdat het AISPs betreft, is artikel 94 niet van toepassing op deze partijen. Desondanks geeft het *onboarding* proces een beeld van hoe dit in de praktijk verloopt.

aangaan. Deze informatie is vaak kort en in begrijpelijke taal weergegeven, met mogelijkheden voor de klant om vervolgens informatie verder uit te diepen, via links naar algemene voorwaarden en privacy statements.

Het proces van toegang verlenen tot de betaalrekening loopt in de praktijk via *redirection* in de bankomgeving, waar de klant eerst moet inloggen en vervolgens toestemming moet geven via een SCA-methode.[83] Dit is een garantie voor een meer expliciet gevraagde toestemming, want uit gesprekken met aanbieders komt verder naar voren dat er voor hen een afruil is tussen een zo soepel mogelijke klantreis, waarbij de klant zonder al te veel hobbels toestemming kan geven aan derde partijen voor toegang tot de betaalrekening, en het nagaan of klanten weten waar ze aan beginnen.

Als derde partijen via *aggregators* toegang krijgen tot de betaalrekening, kan dat volgens sommige gesprekspartners verwarrend zijn voor consumenten. Ze doen namelijk zaken met de ene partij om bepaalde diensten af te nemen, maar als ze toestemming moeten geven voor toegang tot de betaalrekening krijgen ze plotseling te maken met een heel andere partij, die ze mogelijk niet kennen. In het dashboard zien consumenten dan ook een andere naam dan de naam van de partij waarmee ze in eerste instantie zaken denken te doen, en dat kan verwarrend zijn voor consumenten, zo is de gedachte.

Conclusie

- Uit gesprekken en de eerdergenoemde proef met 5 apps van AISPs komt naar voren dat deze partijen zich aan de voorgeschreven manier van authenticatie in PSD2 houden. Dit suggereert dat toestemming voldoende expliciet en specifiek wordt gevraagd.
- Uit gesprekken komt ook naar voren dat betaaldienstverleners zich bewust zijn van de eisen die de AVG stelt.
- Of de praktische implementatie voldoet vanuit AVG-perspectief, is een handhavingsvraag voor de AP en daarmee geen onderdeel van deze evaluatie.
- Als derde partijen via *aggregators* toegang krijgen tot de betaalrekening, brengt dit een risico met zich mee omdat consumenten dergelijke partijen mogelijk niet herkennen in bijvoorbeeld het dashboard.

Voelt de consument zich vrij om toestemming te weigeren?

Wij interpreteren deze vraag in het licht van artikel 94 lid 2 PSD2, het gaat hier om een onderdeel van hetgeen de EDPB verstaat onder uitdrukkelijke toestemming van de betaaldienstverlener tot persoonsgegevens. De voorwaarde dat consumenten zich vrij moeten voelen om toestemming te weigeren, maakt geen onderdeel uit van PSD2. Artikel 94 is alleen van toepassing op PISP-diensten en niet op AISP-diensten. Daar geldt de eis van uitdrukkelijke toestemming niet en zijn dus ook de eisen die de AP daaraan stelt niet van toepassing.

De AVG geeft aan dat 'vrij' inhoudt dat een consument toestemming moet kunnen weigeren en daar geen nadeel van mag ondervinden. Hoe dit vereiste in de praktijk vormgegeven zou moeten worden is echter niet helder.[84] Het moge immers duidelijk zijn dat wanneer een commerciële partij aan een consument een product aanbiedt waarbij toegang tot de betaalrekening een rol speelt deze dienst niet meer of alleen tegen andere voorwaarden verleend kan worden als de consument die toegang weigert. Het standpunt van de AP lijkt nu te zijn dat dit niet mag.[85]

---

83 Volgens de RTS mag dit ook met andere methoden dan redirection.

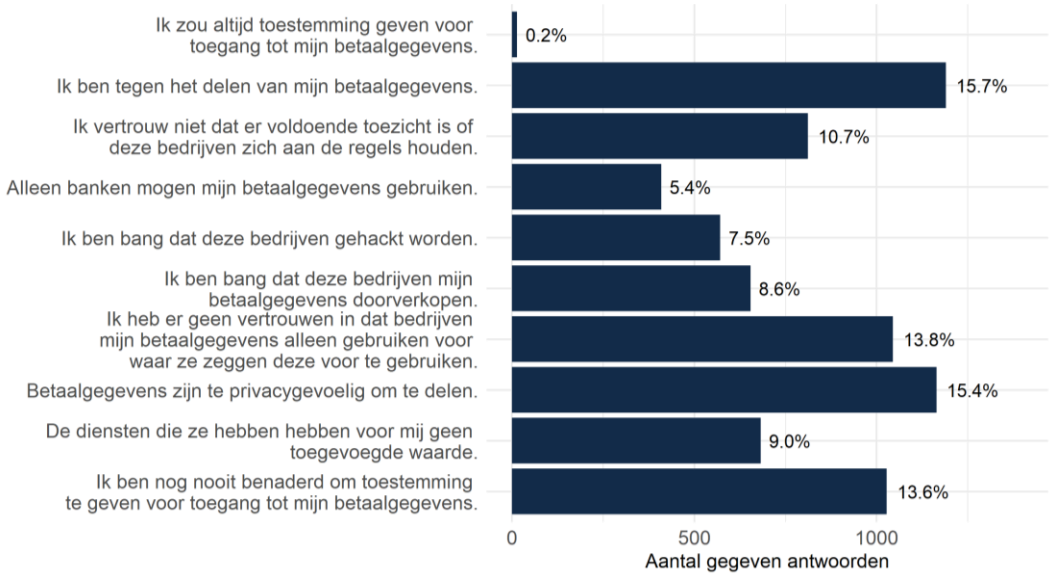
84 De EDPB zegt hierover in haar guidelines over het samenspel van PSD2 en de AVG: 'the payment service user must be able to choose whether or not to use the service and cannot be forced to do so'.

85 De EDPB zegt in voorbeeld 6 van haar guidelines 05/2020 on consent *'A bank asks customers for consent to allow third parties to use their payment details for direct marketing purposes. This processing activity is not necessary for the*

Concrete voorbeelden van situaties in de praktijk waarin dit speelt zouden hierbij behulpzaam zijn, ook om helder te krijgen hoe het juridische standpunt van de AP beleidsmatig uitpakt in de praktijk.

Zoals we al eerder zagen, zijn er relatief weinig consumenten die in de praktijk gebruikmaken van PSD2. Daarbij geeft een groot aandeel van de consumenten aan dat ze tegen het delen van betaalgegevens zijn of betaalgegevens te gevoelig vinden om te delen (Figuur 5.6). Consumenten zijn dus kritisch over PSD2 en gebruiken het dan ook niet. Dit suggereert dat in ieder geval een deel van de consumenten zich in de praktijk vrij voelt om toestemming te weigeren.

Figuur 5.6 Wat zijn voor u de belangrijkste redenen om bedrijven geen toestemming te geven voor toegang tot uw betaalgegevens voor betaalinitiatiediensten of rekeninginformatiediensten?



Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2486. Bij deze vraag konden respondenten meerdere antwoorden geven. Het percentage geeft daarom het aandeel antwoorden ten opzichte van het totaal aantal gegeven antwoorden (k = 7568) weer

Uit de gesprekken met marktpartijen komt niet het beeld naar voren dat consumenten zich niet vrij voelen om toestemming te weigeren. Bij de meeste voorbeelden van PSD2-diensten die we zijn tegengekomen, zijn dergelijke situaties ook moeilijk voorstelbaar, denk bijvoorbeeld aan een app waarmee consumenten een betaling willen verrichten bij een webwinkel. Consumenten gebruiken zo'n app uit eigen beweging. Daarbij is de dienst onmogelijk om te leveren als consumenten géén toestemming geven. Dit maakt ook moeilijk voorstelbaar hoe het concept van vrij voelen om toestemming te weigeren praktisch ingevuld zou moeten worden.

Sommige gesprekspartners zien het risico dat voor het krijgen van toegang tot bepaalde diensten het geven van toestemming tot de betaalrekening een vereiste zou kunnen worden. Een voorbeeld dat genoemd wordt, is kredietverstrekking. Een consument zou dan bij een kredietaanvraag toegang moeten geven tot de betaaldata, zodat de verstrekker op basis van die data een inschatting kan maken van het kredietrisico en op basis daarvan een aanbod kan doen.

---

performance of the contract with the customer and the delivery of ordinary bank account services. If the customer's refusal to consent to this processing purpose would lead to the denial of banking services, closure of the bank account, or, depending on the case, an increase of the fee, consent cannot be freely given.' Dit suggereert dat commerciële voorwaarden van een dienst niet mogen afhangen van het toegang krijgen tot de betaalrekening.

Het risico dat sommige gesprekspartners zien is dat het krediet niet verstrekt wordt als de toegang niet wordt gegeven, en dat consumenten daarom niet vrij zijn in hun keuze om toegang te geven. In de praktijk is er echter voldoende concurrentie in de markt voor kredietverstrekking, waardoor een consument ook andere keuzemogelijkheden heeft als hij of zij een krediet wil. Dat beperkt het risico dat een consument geen keuzevrijheid meer heeft en zich dus niet vrij voelt om toestemming te weigeren.

Een voorbeeld van een dergelijke partij (niet genoemd door gesprekspartners) is Lendex, een fintech die een volledige dochter is van NIBC.[86] Het bedrijf biedt krediet aan via een volledig digitaal proces, waarbij de consument inzage moet geven in de betaaldata van zijn of haar belangrijkste betaalrekening. Dit betreft waarschijnlijk een beperkt subsegment van een markt die op zichzelf al klein is. Initiatie van een kredietaanvraag loopt via een retailer. Consumenten kunnen Lendex niet zelf benaderen. Op basis van de betaaldata die via die toegang beschikbaar komen, beslist Lendex of krediet verstrekt kan worden.[87] We hebben geen informatie over wat Lendex precies doet op het moment dat een klant geen toegang geeft tot betaalgegevens.

Conclusie

- Wij hebben in de interviews met marktpartijen geen aanwijzingen gekregen dat consumenten zich niet vrij voelen om toestemming te weigeren.
- Voor veel rekeninginformatie- of betaalinitiatiediensten is toegang tot de betaalrekening een vereiste om de dienst te kunnen leveren. Het valt moeilijk in te zien hoe de voorwaarde dan een consument geen nadeel mag ondervinden van het weigeren van toegang in de praktijk moet worden vormgegeven voor dergelijke diensten.
- Het grote aantal consumenten dat aangeeft betaaldata niet te willen delen, vormt een aanwijzing dat consumenten zich vrij voelen om toestemming te weigeren.
- Er zijn partijen in de markt die betaalinformatie gebruiken in het proces van kredietverstrekking. Dit is echter beperkt, voor zover wij dat kunnen beoordelen, en consumenten hebben ook andere kanalen om krediet aan te vragen waar dergelijke toegang niet gevraagd wordt.

Kunnen mensen eenvoudig terugkomen op een gegeven toestemming?

Wij interpreteren deze vraag in het licht van artikel 94 lid 2 PSD2, het gaat hier om uitdrukkelijke toestemming en niet instemming van de betaaldienstverlener tot persoonsgegevens. PSD2 bevat geen voorwaarden met betrekking tot het intrekken van een eenmaal gegeven toestemming.

De AP schrijft op haar website 'Uw betaaldienstverlener moet u duidelijk hebben geïnformeerd over het feit dat u uw toestemming weer kunt intrekken. En ook hoe u dat kunt doen. De betaaldienstverlener moet u die informatie vóór het afsluiten van de overeenkomst hebben gegeven.' PSD2 bevat geen bepalingen die iets zeggen over het kunnen terugkomen op een gegeven toestemming. Dit is een invulling die de AP heeft gegeven aan het concept uitdrukkelijke toestemming onder artikel 94, waarmee de AP aansluit bij de AVG die bepaalt dat de verwerkingsverantwoordelijke (in dit geval de TPP) ervoor moet zorgen dat het intrekken van toestemming door de gebruiker even eenvoudig moet zijn als het geven ervan.[88]

---

86 NIBC heeft Lendex in 2019 gekocht.

87 Lendex werkt samen met Salt Edge Limited om toegang te krijgen tot betaalrekeningen. Lendex heeft zelf een PSD2-vergunning. Salt Edge is partij uit de UK die technische implementatie van PSD2 compliant software biedt, zowel aan banken als aan fintechs.

88 Artikel 7, lid 3 van de AVG

Voor betaalinitiatiediensten geldt dat de toestemming meestal per betaling plaatsvindt. Intrekken van de toestemming is daarmee geen issue, de toestemming wordt immers éénmalig verleend, waarna de betaling plaatsvindt. Ex post intrekken van de toestemming heeft dan weinig betekenis. Bij rekeninginformatiediensten zou het terug willen komen op toestemming wel kunnen spelen. Daar geldt dat toestemming voor een periode van negentig dagen wordt verleend (het kan ook eenmalig), waarna opnieuw expliciete toestemming gevraagd en gegeven moet worden. Artikel 94 is echter niet op AISP's van toepassing.

Voordat PSD2 van start ging was er veel discussie over de manier waarop klanten terug kunnen komen op een toestemming. Op verzoek van consumentenorganisaties hebben banken een dashboard ingevoerd waarbij ze consumenten inzicht geven aan welke partijen zij toegang hebben verleend tot hun betaalrekening. Sommige banken hebben consumenten daarbij ook de mogelijkheid gegeven om de toegang voor specifieke partijen op te heffen of om de mogelijkheid te bieden om toegang tot de betaalrekening helemaal uit te zetten.

De meeste banken hebben aan deze oproep gehoor gegeven. DNB geeft aan dat banken een dashboard mogen aanbieden en dat een bank de klant de mogelijkheid mag geven om de gegeven toestemming in te trekken.[89]Er is discussie in Europa over wat in dit opzicht wel en niet mag.[90] Deze dashboards zijn echter niet altijd terug te vinden in de mobiel bankieren app, blijkt uit een steekproef onder 4 banken.[91] In de online bankierenomgeving is het dashboard wel altijd terug te vinden. Het is ook mogelijk om de toegang voor een specifieke partij dicht te zetten in het dashboard. Banken geven in de informatie die betrekking heeft op PSD2 aan dat intrekken van de toestemming moet gebeuren via de derde partij. [92]

Er zijn volgens gesprekspartners op dit moment ook banken die kiezen voor een algemene knop waarmee toegang tot PSD2-diensten geblokkeerd wordt. Andere banken stellen zich op het standpunt dat dit wettelijk niet mogelijk is. De EBA *opinion on obstacles* stelt hierover: *'a general, ex-ante consent required by the ASPSP in order for PSUs to be able to use the AISP's/PISP's' services is an obstacle under Article 32(3) RTS'*.[93]

Hier speelt de balans van mededinging versus privacy. Te veel obstakels in de vorm van informatie die klanten tot zich moeten nemen, zorgen voor een minder aantrekkelijke klantreis en maakt het moeilijker om concurrentie op gang te brengen. Aan de andere kant geeft een makkelijke manier om toegang te blokkeren of in te trekken additionele zekerheid aan klanten dat ze 'in control' zijn. Dat zou kunnen helpen om de acceptatie van PSD2 te vergroten, volgens sommige gesprekspartners.

---

89 Zie https://www.dnb.nl/voor-de-sector/open-boek-toezicht-wet-regelgeving/toezicht-wet-regelgeving/psd2/mogen-account-servicing-payment-service-providers-aspsps-hun-klanten-een-dashboard-aanbieden/

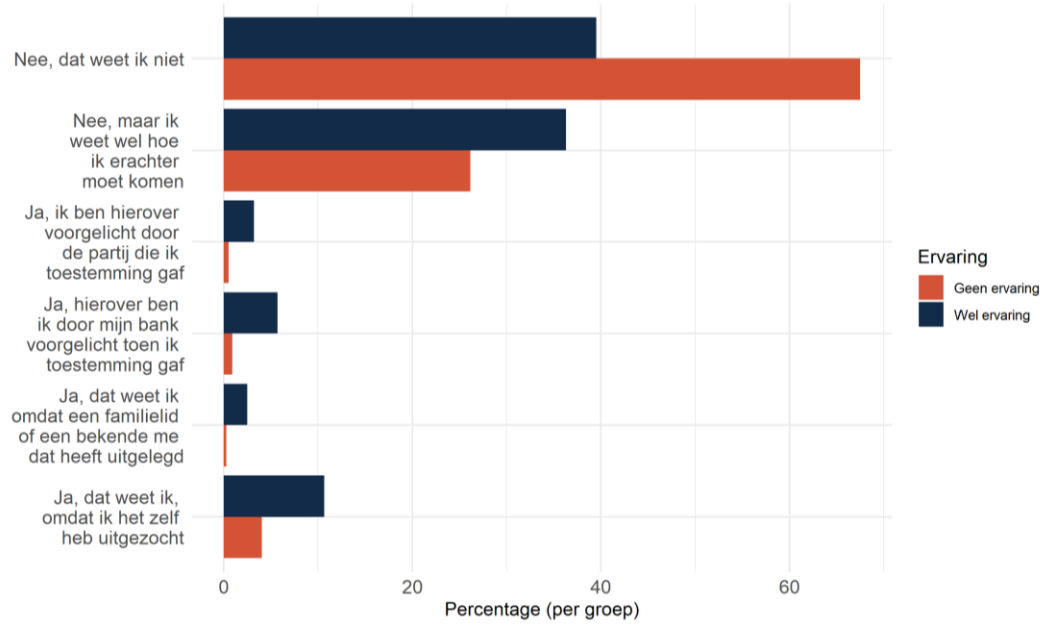
90 Zie ook EBA Q&A 2018-4309, zie https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4309. Deze EBA-Q&A verbiedt 2 dingen. Ten eerste dat banken de toegang dicht zetten en ten tweede dat banken de mogelijkheid bieden voor een 'general opt out', dus de mogelijkheid om vooraf de toegang bij de bank voor alle derde partijen dicht te zetten.

91 We hebben niet voor alle Nederlandse banken onderzoek welke banken wel en welke banken niet een dashboard bieden.

92 Het intrekken van de autorisatie via een bankendashboard is juridisch niet hetzelfde als het intrekken van toestemming, maar komt materieel wel op hetzelfde neer.

93 Zie https://www.eba.europa.eu/eba-publishes-opinion-obstacles-provision-third-party-provider-services-under-payment-services

Figuur 5.7 Weet u hoe u toestemming voor toegang tot uw betaalgegevens kunt intrekken?



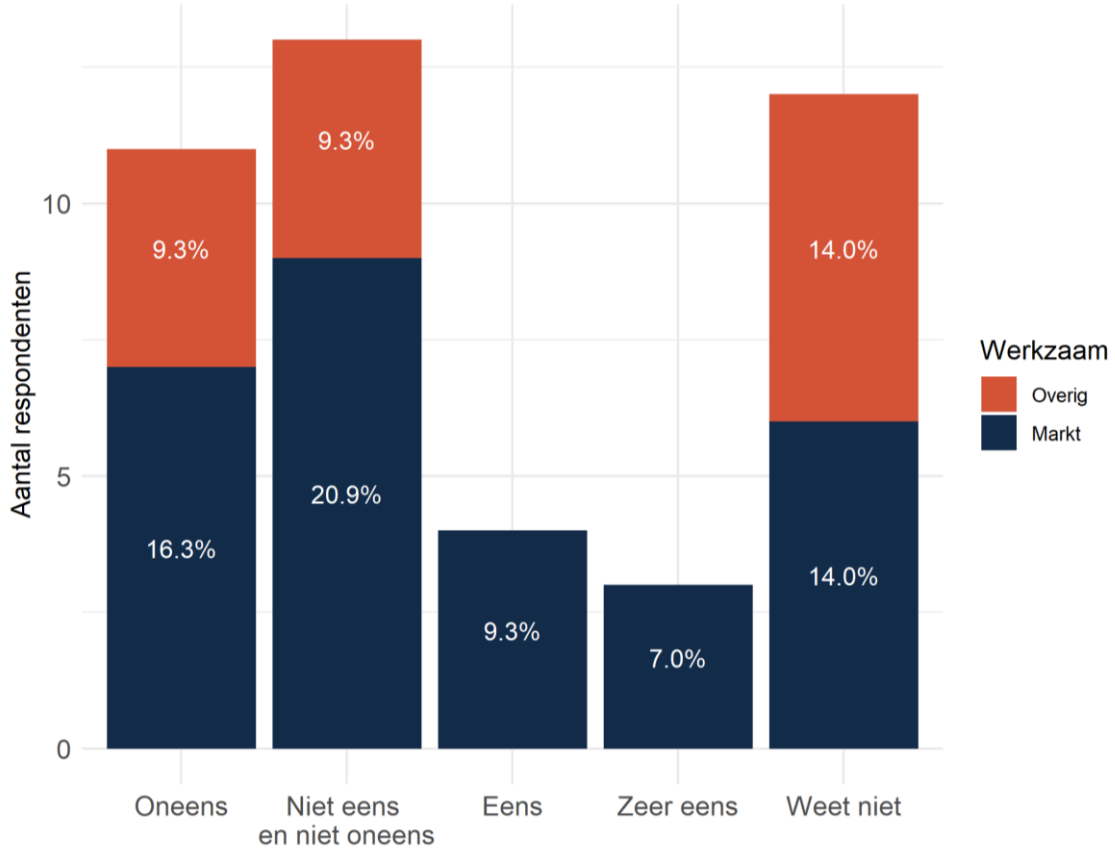
Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2486

De consumentenenquête laat zien dat van mensen die ervaring hebben met PSD2 een meerderheid weet hoe ze toestemming kunnen intrekken of weet hoe ze erachter kunnen komen hoe ze toestemming moeten intrekken. Het verschil met de mensen die geen ervaring hebben met PSD2 is daarbij opmerkelijk. Dit suggereert dat consumenten die ervaring hebben met PSD2 zich ook informeren over zaken die daarmee te maken hebben.

De online enquête onder gesprekspartners laat zien dat 25,6 procent het oneens of zeer oneens is met de stelling dat consumenten weten hoe ze hun toestemming kunnen intrekken, terwijl 16,3 procent het eens of zeer eens is met de stelling (Figuur 5.8). Een groot deel, 31.2 procent, is het noch eens, noch oneens. In de praktijk lijkt opzeggen van een contract met een AISP relatief eenvoudig als het contract voor de dienst in een app wordt afgesloten. De optie om het contract te beëindigen maakt in de gevallen die wij hebben bekeken onderdeel uit van de app.

Een groot deel van gesprekspartners geven aan dat het relevant is om onderscheid te maken tussen bedrijven die derden toegang geven tot hun rekening voor betaalinitiatiediensten en rekeninginformatiediensten en consumenten. Voor bedrijven geldt immers dat de vraag of toestemming gemakkelijk ingetrokken kan worden minder relevant is omdat bedrijven meer dan individuele consumenten geacht worden om rationele weloverwogen beslissingen te nemen die in het bedrijfsbelang zijn. Daarnaast betreft het soms geen persoonsgegevens van individuele consumenten, maar betalingen aan andere bedrijven.

Figuur 5.8 Stelling: Consumenten weten hoe ze toestemming voor toegang tot hun betaalrekening kunnen intrekken



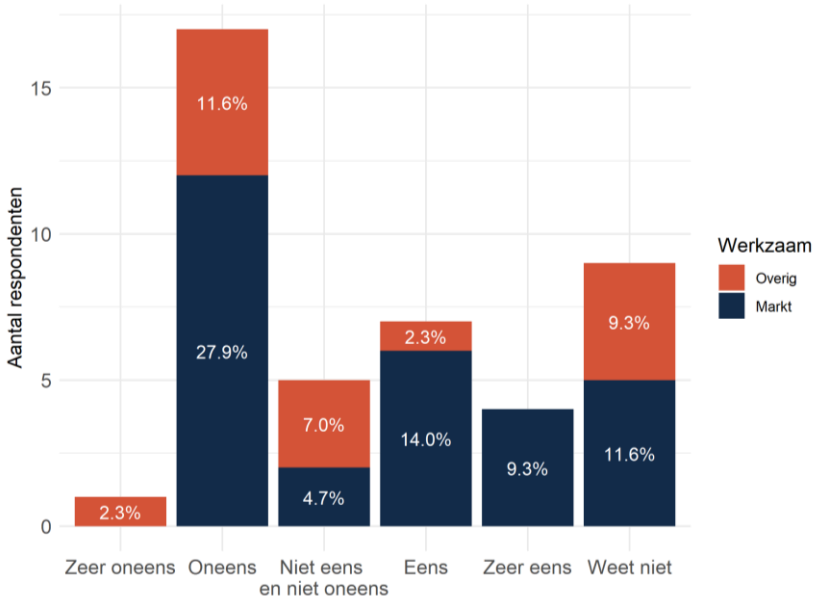
Bron: SEO Economisch Onderzoek op basis van een mini-enquête onder 43 interviewpartners

Conclusie

- PSD2 bevat geen bepaling over intrekken van toestemming, dit is een bepaling uit de AVG.
- Banken bieden in hun dashboard veelal de mogelijkheid om toegang voor individuele partijen waaraan de klant toestemming heeft gegeven te blokkeren, hetgeen feitelijk hetzelfde effect heeft als het intrekken van toestemming.
- De AISP's waarvoor wij het *onboarding* proces hebben doorlopen geven tijdens dit proces aan hoe klanten het contract met hen kunnen beëindigen.
- Klanten kunnen in de praktijk dan ook terugkomen op een gegeven toestemming door een contract te beëindigen of de toegang voor individuele partijen in hun bank-app te blokkeren.

Hoe kunnen consumenten worden geholpen bij het bewaren van overzicht ten aanzien van de gegeven toestemmingen (dat kan d.m.v. het dashboard van banken, maar zijn er ook andere manieren)?

Figuur 5.9 Stelling: Consumenten kunnen eenvoudig achterhalen aan welke partijen ze toestemming hebben gegeven voor betaalinitiatiediensten en rekeninginformatiediensten



Bron: SEO Economisch Onderzoek op basis van een mini-enquête onder 43 interviewpartners

Een groot aantal gesprekspartners (41,5 procent) geeft aan dat consumenten niet eenvoudig kunnen achterhalen aan wie zij toestemming hebben gegeven (Figuur 5.). Dit is opmerkelijk, aangezien de testen bij een 4-tal banken leren dat gegeven toestemming in de online bankomgeving op overzichtelijke wijze terug is te vinden.

Banken bieden een dashboard in de betaalapp dat een overzicht biedt van de partijen waaraan toestemming is gegeven voor PSD2-diensten. Gesprekspartners geven aan dat de dit dashboard voor consumenten niet altijd eenvoudig te vinden is. Ervaringen op basis van eigen testen bij een 4-tal banken bevestigen dit beeld niet. Als een dashboard onderdeel uitmaakt van de app is deze in onze beleving relatief makkelijk te vinden. Het blijkt echter dat niet alle banken een dergelijke functionaliteit in de betaalapp bieden. In de online bankomgeving is het dashboard wel altijd te vinden bij de door ons bekeken banken.

Het is moeilijk in te zien hoe consumenten anders geholpen zouden kunnen worden om te achterhalen aan welke partijen ze toestemming hebben verleend dan met een dashboard omdat alleen de bank inzicht heeft in welke PSD2-vergunninghouders toegang hebben gevraagd. Dit is geen informatie die op een centrale plek wordt geregistreerd, alleen de bank weet welke partijen zijn klant toegang heeft gegeven tot zijn of haar betaalrekening. Banken mogelijk dergelijke data niet met derden delen. Oplossing via marktwerking zijn daarmee niet aan de orde. Opties die een centrale registratie vragen, brengen veel extra administratieve kosten met zich mee. Daarnaast brengt dit ook de vraag met zich mee wie een dergelijke database moet beheren, nog los van de privacyrisico's die dit met zich mee kan brengen (single point of failure).

Afhankelijk van de consumentenbehoefte zouden banken kunnen onderzoeken of het haalbaar is een dergelijk instrument te creëren. Hier kunnen mededingingsrechtelijke aspecten spelen. Daarnaast zou onderzocht moeten worden of dit op bezwaren vanuit de AVG stuit. Gezien het beperkte succes van PSD2 in Nederland is het echter de vraag of dit op dit moment nodig is. Daarnaast is het de vraag welke toegevoegde waarde een dergelijke centrale

registratie heeft ten opzichte van het dashboard dat banken bieden en wat daarvan de kosten zijn. Wel zou een optie kunnen zijn dat een klant een jaarlijks bericht krijgt van zijn bank met een overzicht.

Conclusie

- Banken bieden een dashboard en daarmee een mogelijkheid voor consumenten om eenvoudig te achterhalen aan welke partijen ze toegang hebben gegeven.
- Als toegang via een *aggregator* loopt, zien consumenten in het dashboard dat ze deze partij toegang hebben gegeven. Dat kan verwarrend werken.
- Hierbij zijn er soms kleine belemmeringen. Zo is het dashboard soms niet toegankelijk via de bank app, maar wel via de online omgeving.
- Het valt moeilijk in te zien hoe een overzicht anders of beter dan via een dashboard bij de bank kan worden geimplementeerd. Een alternatief lijkt op het moment ook niet echt nodig, mede omdat het gebruik van PSD2 laag is.
- Als het PSD2 gebruik zou toenemen, neemt het belang dat alle banken een overzichtelijk en makkelijk toegankelijk dashboard bieden toe. Een optie zou kunnen zijn dat een klant een jaarlijks bericht krijgt van zijn bank met een overzicht van partijen met toegang.

5.3 Gebruik van gegevens

Onderzoeksvragen

1. Leveren de bepalingen in de implementatiewet in verhouding tot de AVG in de praktijk uitdagingen/problemen op (met inachtneming van de verduidelijking die de EDPB heeft geboden)?
2. Hoe worden betaalgegevens gebruikt (doelbinding)?
3. Worden betaalgegevens ook gebruikt voor maatschappelijk onaantrekkelijke doelen?

Leveren de bepalingen in de implementatiewet in verhouding tot de AVG in de praktijk uitdagingen/problemen op (met inachtneming van de verduidelijking die de EDPB heeft geboden)?

PSD2 is in Europa in 2015 vastgesteld, de AVG in 2016. Dit heeft er mogelijk toe geleid dat bij de vormgeving van PSD2 onvoldoende rekening is gehouden met de AVG. Er is ook een inherente spanning tussen de twee wetten: waar PSD2 stuurt op het beschikbaar maken van betaaldata voor derde partijen, streeft de AVG rechtmatige en zorgvuldige omgang met persoonsgegevens na en stelt daarmee grenzen aan de beschikbaarheid van betaaldata voor zover het persoonsgegevens betreft. In de initiële fase van PSD2, waarin partijen bezig waren met het verkrijgen van een vergunning, was er dan ook veel onduidelijkheid over de relatie tussen de AVG en PSD2. Partijen wisten niet hoe ze API's of interne processen zo vorm moesten geven dat deze zowel aan de eisen van PSD2 als aan de eisen van de AVG voldeden. Denk hierbij aan de vereisten van dataminimalisatie, of de precieze invulling in de praktijk van de verschillende vormen van consent.

De bepalingen leveren ook nu nog uitdagingen op voor marktpartijen. De problemen zijn veelal praktisch van aard en hebben te maken met interactie tussen de eisen die PSD2 stelt en de eisen die de AVG stelt zoals de EDPB die in haar guideline bespreekt. PSD2 legt niet vast hoe om te gaan met de vereisten die de AVG stelt. De eisen die de AVG stelt aan de API's van PSD2-vergunningshouders kennen dan ook geen plek in het vergunningsproces van DNB. Marktpartijen hebben behoefte aan praktische *guidance* door toezichthouders over de manier waarop partijen in de praktijk hun processen en implementaties moeten vormgeven om te voldoen aan de AVG-vereisten.

Uitdagingen die nog spelen op het gebied van de AVG zijn:

1. De behandeling van speciale categorieën van data, met name bijzondere persoonsgegevens. Vragen die hier spelen zijn: moet een AISP apart toestemming vragen om dergelijke data op te halen? Zo ja, hoe zouden ze dat dan moeten doen en op welk punt in het proces? Hoe moet een bank hiermee omgaan? Mag de bank controleren of de uitdrukkelijke toestemming die de AVG vereist is gegeven voordat het data die in deze categorie vallen deelt met derde partijen?
2. De praktische implementatie van dataminimalisatie. Betaaldata kennen veel dimensies waardoor het technisch lastig is om alle mogelijke doorsnedes van de data te faciliteren. Hier speelt dat marktpartijen behoefte hebben aan praktische *guidance* over hoe dit in specifieke gevallen in de praktijk vorm te geven.

In het kader van PSD2 ligt het volgende vraagstuk er:

3. Internationale divergentie in de aanpak van de wijze waarop partijen in de vormgeving van API's moeten omgaan met de vereisten uit de AVG. In de meeste landen speelt de discussie over dataminimalisatie voor zover wij hebben kunnen achterhalen niet (terwijl net als in Nederland de mogelijkheid in API's voor dataminimalisaties ontbreekt) en zijn banken ook niet bezig met het aanpassen van hun API's op dit punt. Dit kan de reeds bestaande verschillen in API's tussen landen verder vergroten.

Conclusie

- De interactie van PSD2 met de AVG levert in de praktijk uitdagingen op voor marktpartijen.
- Deels komt dit doordat de eisen van de AVG tijdens het implementatieproces bij betaaldienstverleners onvoldoende in beeld waren.
- Deels komt dit doordat niet altijd duidelijk is wat marktpartijen moeten doen om de eisen van de AVG in de praktijk te verenigen met die van PSD2.
- Er is vanuit marktpartijen veel behoefte aan praktische *guidance* over hoe de eisen die voortvloeien uit het samenspel tussen PSD2 en de AVG in praktijk vorm te geven.
- Het gebrek daaraan creëert onzekerheid en onduidelijkheid bij marktpartijen.
- Verschillende landen gaan ook verschillend om met de interactie van PSD2 met de AVG, bijvoorbeeld op het punt van dataminimalisatie.. Dit creëert het risico van verdere fragmentatie van het API-landschap.

Hoe worden betaalgegevens gebruikt (doelbinding)?

PSD2 schrijft voor dat een AISP niet overgaat 'tot het gebruiken, zich toegang verschaffen tot of opslaan van gegevens voor andere doelstellingen dan het uitvoeren van de door de betalingsdienstgebruiker uitdrukkelijk gevraagde rekeninginformatiedienst, overeenkomstig de voorschriften inzake gegevensbescherming.'[94] Voor PISP geldt dat deze niet mag overgaan 'tot het gebruiken, zich toegang verschaffen tot of opslaan van gegevens voor andere doelstellingen dan het verstrekken van de door de betaler uitdrukkelijk gevraagde betalingsinitiatiedienst'.[95] Toezicht hierop valt onder DNB.

De AVG schrijft doelbinding voor bij het verwerken van persoonsgegevens. Dat doel is gekoppeld aan een grondslag. Data mogen alleen met het van tevoren bepaalde doel verwerkt worden op basis van de bijbehorende verwerkingsgrondslag. De basis voor de verwerkingsgrondslag is het contract dat de betaaldienstverlener heeft met de klant. PISP's, AISP's en derde partijen moeten zich aan de AVG houden die doelbinding voorschrijft.

94 PSD2 artikel 67 lid f
95 PSD2 artikel 66 lid g

Uit de inventarisatie van het register met vergunningen komen de volgende typen gebruikers naar voren: huishoudboekje, hulp bij beleggen, financiële planning, krediet aanvragen, budgetbeheer en het koppelen van betaalrekeningen. Deze manieren waarop betaaldata gebruikt worden, waren grotendeels voorzien op het moment dat PSD2 in werking trad, wellicht op het gebruiken van betaaldata om gestructureerd kleine bedragen te beleggen na.

In deze evaluatie hebben wij voornamelijk in gesprekken inzicht gekregen in de wijze waarop betaalgegevens in de praktijk daadwerkelijk gebruikt worden door vergunninghouders. Wij hebben geen daadwerkelijk zicht gehad op hoe data in systemen worden opgeslagen, gebruikt en gedeeld. Gesprekspartners met een PSD2-vergunning geven desgevraagd aan dat ze betaalgegevens alleen gebruiken voor doelen waarvan in het contract met de klant sprake is. Sommige gesprekspartners geven aan dat ze vermoeden dat er partijen zijn die dat niet doen, maar geven geen concrete voorbeelden hiervan.

Daarnaast blijkt uit de privacy statements van enkele AISP's dat bij het verwerken van de betaalgegevens gebruikgemaakt wordt van de diensten van derde partijen, die bijvoorbeeld betaaldata classificeren of softwareapplicaties hebben die op basis van betaaldata kredietwaardigheid kunnen inschatten, maar zelf geen PSD2-vergunning hebben en buiten de reikwijdte van PSD2 vallen. [96]De privacy statements bevatten ook beschrijvingen van de wijze waarop betaaldata gebruikt worden. Dit geeft een rudimentair beeld van de wijze waarop betaalgegevens in de praktijk gebruikt worden.

Conclusie

- Betaaldata worden gebruikt op manieren en voor doelen die grotendeels waren voorzien. Bij de partijen die vergunningen hebben gekregen zitten geen onverwachte, nieuwe diensten.
- De evaluatie heeft vooral via gesprekken een beeld gevormd over hoe betaalgegevens gebruikt worden.
- Daarnaast geven privacy statements van partijen zicht op hoe data gebruikt worden.
- Wij hebben geen aanwijzingen dat partijen data gebruiken op manieren of voor doelen die niet in lijn zijn met de doelen waarvoor die data zijn verkregen.

Worden betaalgegevens ook gebruikt voor maatschappelijk onaantrekkelijke doelen?

Deze evaluatie heeft geen zicht gegeven op de precieze wijze waarop betaalgegevens gebruikt worden nadat de gebruiker toestemming heeft gegeven. Een precieze analyse van de wijze waarop AISP's betaaldata gebruiken vergt een meer gedetailleerd en diepgravend onderzoek waarbij de bedrijfsprocessen van AISP's in kaart en ge-audit zouden moeten worden.

Partijen die toegang vragen hebben een vergunning van ofwel DNB ofwel een buitenlandse toezichthouder als ze op basis van *passporting* actief zijn in Nederland. Als partijen zich aan de vereisten in PSD2 en de AVG houden is het gebruik daarmee in juridische zin geoorloofd. Op partijen van buiten Nederland met een *passporting* vergunning houdt DNB geen toezicht. Toezichthouders in andere EU-landen kunnen het toezicht anders vormgeven dan in Nederland, hoewel de EBA harmonisatie nastreeft van de wijze waarop PSD2 geïmplementeerd is in verschillende EU-landen.

Desondanks kunnen activiteiten maatschappelijk gezien onaantrekkelijk zijn. Het is daarbij wel de vraag wanneer activiteiten maatschappelijk gezien onaantrekkelijk zijn. Dit hangt af van de maatschappelijke voorkeuren die beleidsmakers hebben. Daarbij kan het antwoord op de vraag of een activiteit maatschappelijk gezien onaantrekkelijk

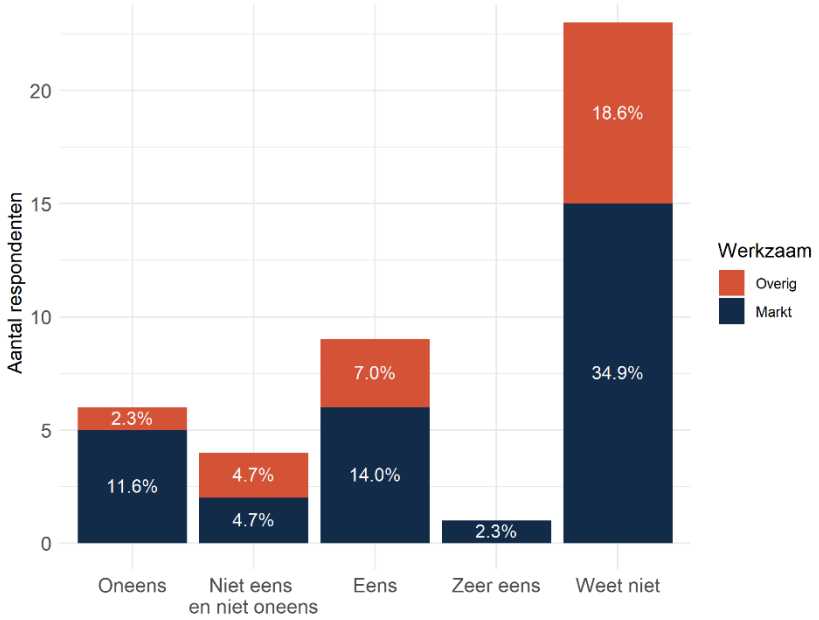
[96] Dergelijke outsourcing is gebruikelijk in financiele markten en mag ook onder PSD2.

is, ook in detail afhangen van de wijze waarop de activiteit vormgegeven is.[97] Wij hebben over de maatschappelijke onaantrekkelijkheid van specifieke diensten in het kader van deze evaluatie geen mening of oordeel.

Duidelijk is dat de ongeoorloofde doorverkoop van betaalgegevens aan derde partijen of het gebruiken van de data voor andere doelen dan aangegeven op het moment van overeenkomst met de gebruiker maatschappelijk gezien ongewenst en dus onaantrekkelijk gebruik inhoudt. In principe houdt DNB hier toezicht op, conform artikel 66 PSD2 en 67 PSD2. Wij zijn van dergelijke ongeoorloofde doorverkoop tijdens onze gesprekken geen feitelijke voorbeelden tegengekomen.

Ongeoorloofd gebruik zou ook kunnen plaatsvinden door derde partijen die geen PSD2-vergunning hebben, maar wel diensten verlenen waarbij betaaldata gebruikt wordt aan partijen met een PSD2-vergunning. In de praktijk bestaat het toezicht op de wijze waarop deze data gebruikt en verwerkt worden door derde partijen zonder PSD2-vergunning uit de algemene handhavingsactiviteiten van de AP in het kader van de AVG op dit vlak. De middelen van de AP voor dergelijk toezicht zijn echter beperkt, vergeleken met de middelen van DNB die het sectorspecifieke toezicht uitoefent.

Figuur 5.10 Stelling: Er bestaan marktpartijen die betaalgegevens gebruiken voor maatschappelijk ongewenste doeleinden



Bron: SEO Economisch Onderzoek op basis van een mini-enquête onder 43 interviewpartners

Hoewel 20 procent van de respondenten het eens is met de stelling dat er marktpartijen bestaan die betaalgegevens gebruiken voor maatschappelijk onwenselijke doelen, kwamen hier tijdens de gesprekken geen praktijkvoorbeelden van naar boven, ook niet als hier expliciet op werd doorgevraagd (Figuur 5.10). Voorbeelden die werden

97 Neem het voorbeeld van verwerking ten behoeve van kredietverstrekking. Dit kan maatschappelijk gezien positief zijn als door betere informatie personen die eerst onterecht geen krediet kregen om bijvoorbeeld scholing te financieren, alsnog een krediet krijgen. Denk aan personen waarbij op basis van oppervlakkige informatie de indruk zou kunnen bestaan dat zij niet kredietwaardig zijn, maar waar een analyse van inkomende en uitgaande bedragen op betaalrekeningen blijkt dat hun kredietwaardigheid hoger is. Het kan echter ook negatief uitpakken, als door slimmere risicobeheersing personen die eerst terecht geen krediet kregen alsnog een krediet krijgen waardoor ze meer risico lopen. Zonder een gedetailleerde analyse van de precieze besluitvorming binnen zo'n bedrijf en de situatie van de klant is een uitspraak over de maatschappelijke effecten en daarmee over de wenselijkheid van gebruik van betaalgegevens niet mogelijk.

genoemd waren speculatief en verwezen niet naar daadwerkelijk bestaande partijen. Een speculatief voorbeeld dat genoemd werd, was het niet verstrekken van een hypotheek als een klant geen inzage geeft via PSD2 in zijn of haar betaalrekening. Een ander voorbeeld was het ongeoorloofd doorverkopen van betaaldata aan derde partijen. Dit zou een overtreding zijn van zowel PSD2 en de AVG. Sommige gesprekspartners riepen de vraag op of DNB dan wel de AP zicht hebben op het gebruik van betaaldata. Opvallend is vooral het grote percentage dat aangaf het niet te weten. Dit suggereert dat ook onze gesprekspartners maar een beperkt beeld hebben van de wijze waarop betaalgegevens gebruikt worden nadat deze eenmaal zijn opgehaald door een derde partij.

Conclusie

- Of betaaldata gebruikt worden voor maatschappelijk onaantrekkelijke doelen, is uit te splitsen in twee vragen.
- Ten eerste kan sprake zijn van geoorloofd gebruik van betaaldata door vergunninghouders. Of dit in principe geoorloofde gebruik maatschappelijk onaantrekkelijke doelen nastreeft, is een maatschappelijk vraagstuk. Wij hebben daar in het kader van deze evaluatie geen mening over.
- Ten tweede kan sprake zijn van ongeoorloofd gebruik van betaaldata. Dit kan zowel door partijen met als zonder PSD2-vergunning gebeuren. Wij hebben in onze interviews geen aanwijzingen gekregen dat er ongeoorloofd gebruik plaatsvindt.
- DNB kan nagaan of voor partijen met vergunning sprake is van ongeoorloofd gebruik van betaaldata. Of derde partijen zonder PSD2-vergunning zich aan de AVG houden is iets waar de AP toezicht op houdt.

6 Regelgeving en toezicht

Dit hoofdstuk beschrijft de ontwikkeling van de regelgeving en het toezicht. De beschrijving van regelgeving is beperkt, omdat belangrijke aspecten van regelgeving al in eerdere hoofdstukken zijn behandeld. Op het gebied van toezicht richt dit hoofdstuk zich op de samenwerking tussen de toezichthouders.

6.1 Ontwikkeling regelgeving

Onderzoeksvragen

1. Zijn de gesignaleerde problemen van PSD1 verholpen?
2. Toepasselijkheid van PSD2 op one-leg-in-one-leg-out betalingen waarvan een deel in de EU plaatsvindt (108 lid b)

Zijn de gesignaleerde problemen van PSD1 verholpen?

PSD2 is geïntroduceerd om de gesignaleerde problemen van PSD1, zoals het gebruik van achterhaalde of vage begrippen, te verhelpen. Dit is één van de doelstellingen zoals genoemd in de memorie van toelichting.[98] Deze vraag richt zich op de mate waarin dat is gelukt.

De belangrijkste veranderingen onder PSD2 zijn in de voorgaande hoofdstukken besproken. Deze kernbepalingen van PSD2 zijn het verlenen van toegang tot betaalgegevens aan vergunninghoudende partijen, regulering van rekeninginformatiedienstverleners en betaalinitatiedienstverleners en verhoogde bescherming met SCA. Dit hoofdstuk bespreekt deze onderwerpen niet, tenzij ze raken aan andere bevindingen.

Deze paragraaf richt zich op de verandering in de geografische reikwijdte van PSD2 en andere wijzigingen in de regelgeving. De onderzoeksvraag over de 'one-leg-in-one-leg-out' bepaling richt zich op de geografische reikwijdte, die vraag bespreken wij verderop in deze sectie. Eerst bespreekt de paragraaf de 'substance-eis', het aanwijzen van een Central Point of Contact voor betaaldienstagenten en de meldingssystemen voor operationele en beveiligingsincidenten. De paragraaf eindigt met een weergave van de opvattingen van de gesprekspartners over de PSD1 en PSD2.

Voor het aanvragen van een PSD2-vergunning, geldt een 'substance-eis'.[99] Deze houdt in dat als een betaaldienstverlener een vergunning in een land aanvraagt, zij ook een deel van haar betaaldienstverlening in dat land moet verrichten. Dit is ook van toepassing op betaaldienstverleners die al een vergunning hadden op grond van PSD1. De gedachte hierachter is dat anders een dienstverlener een vergunning kan aanvragen in het land met de laagste toegangseis, om vervolgens in een ander land actief te worden. Door de bevoegdheden van nationale toezichthouders, bestaat er een verschil in interpretatie en de compliancelast om een vergunning te krijgen tussen verschillende landen. Daarbij schaart men de Nederlandse toezichthouders onder een van de strengere. Litouwen staat bekend als een land waarbij de toezichthouder niet streng is. Zonder substance-eis kan een betaaldienstverlener een vergunning aanvragen in Litouwen om vervolgens alleen in Nederland actief te zijn. Met de substance-eis moet die dienstverlener een deel van haar diensten in Litouwen aanbieden. Als zij alleen in Nederland actief wil zijn, zal zij

98 Kamerstukken II 2017-2018, 34813, nr. 3.
99 PSD2, Art. 11.

dus ook in Nederland een vergunning aan moeten vragen. Dit zorgt voor een gelijk speelveld met andere Nederlandse dienstverleners.

Sommige buitenlandse betaaldienstverleners zijn in een ander land gevestigd, maar zijn in bijv. Nederland actief middels agenten, de zogenaamde betaaldienstagenten. De toezichthouder kan deze dienstverleners verplichten om Central Point of Contact (CCP) aan te wijzen. [100] De host toezichthouder heeft verdergaande bevoegdheden om bij de genotificeerde entiteit informatie op te vragen. Zo kan de toezichthouder toezien op de activiteiten van buitenlandse dienstverleners die in het land van de toezichthouder actief zijn. De regels voor betaaldienstagenten zijn onder PSD2 aangescherpt met extra informatievereisten. Zo dient een betaalinstelling (i) elke materiële wijziging in het Wwft-beleid van de betaaldienstagent onverwijld te melden; (ii) van bestuurders en managers van een niet gereguleerde betaaldienstagent aan te tonen dat deze betrouwbaar en deskundig zijn; en (iii) te melden voor welke betaaldiensten de betaaldienstagent wordt gemachtigd.[101] Hiermee kan de nationale toezichthouder nog beter toezicht houden op de activiteiten die binnen haar jurisdictie plaatsvinden.

PSD2 regelt ook dat betaalinstellingen een systeem voor classificatie en melding van operationele en beveiligingsincidenten moeten hebben.[102] In dat systeem moet ook een proces aanwezig zijn om majeure incidenten te melden aan de relevante toezichthouder, in Nederland is dat DNB. Het is dan aan DNB om dit te rapporteren aan de ECB en aan de EBA. Ook moeten betaalinstellingen periodiek en minstens jaarlijks statistische gegevens over fraude verstrekken aan de toezichthouder. Dit is niet uniek voor betaaldienstverleners, maar dit geldt ook voor banken in het algemeen. Het unieke is dat alle betaaldienstverleners onder PSD2 deze regeling moeten toepassen.

Gesprekspartners zijn van mening dat de markt voor betaaldiensten is verbeterd door de invoering van PSD2 en dat de problemen van PSD1 die één van de aanleidingen vormden voor de invoering van PSD2 zijn geadresseerd . De memorie van toelichting noemt toepassingsgebied van PSD1 en de uitzonderingen hierop, die te vaag of te algemeen geformuleerd of gelet op de evolutie van de markt achterhaald waren. De invoering van PSD2 heeft dit verholpen. Gesprekspartners uit de markt en van belangenorganisaties geven aan dat er met PSD2 nieuwe kansen zijn ontstaan. Er is meer concurrentie doordat banken data en toegang met derde partijen moeten delen. De gesprekspartners zien het lage aantal observaties en de beperkte innovatie in de markt niet direct als een teken dat PSD2 niet heeft gewerkt. Ze stellen dat de markt de tijd moet krijgen en dat het mogelijk over een aantal jaar anders is. Ook geeft een aantal gesprekpartners aan dat er qua regelgeving al meer harmonisatie is dan onder PSD1. De meeste gesprekspartners stellen dat de aandacht voor PSD2 vele malen groter is dan de aandacht voor PSD1.

Conclusie

- Met PSD2 zijn enkele problemen van PSD1 verholpen. De regelgeving is nu eenduidiger en zorgt ook meer voor een gelijk speelveld. Door de substance-eis is er een gelijker speelveld bij het aanvragen van een vergunning, met de bepalingen rondom betaaldienstagenten is er meer toezicht op en communicatie met buitenlandse betaaldienstverleners die in een land actief zijn.

Toepasselijkheid van PSD2 op *one-leg-in-one-leg-out* betalingen waarvan een deel in de EU plaatsvindt (108 lid b)

De reikwijdte van PSD2 is groter dan de reikwijdte van PSD1, omdat PSD2 ook transacties reguleert waarbij slechts één van de betrokken betaaldienstverleners in de EU gevestigd is. Dit zijn zogenaamde 'one-leg-in-one-leg out'

100 PSD2, Art. 15.
101 PSD2, Art. 19.
102 PSD2, Art. 96.

transacties. PSD1 was alleen van toepassing op transacties waarbij beide betrokken betaaldienstverleners in de EU gevestigd waren.[103] De uitbreiding van de reikwijdte dient om de consument beter te beschermen bij het verrichten van betalingen. Onder PSD1 vielen betalingen aan bijvoorbeeld een Amerikaans bedrijf niet volledig onder de regelgeving. Onder PSD2 is de Europese consument ervan verzekerd dat alle transacties onder dezelfde regelgeving vallen, als de transactie deels binnen de Europese Unie plaatsvindt. Transacties die volledig buiten de Europese Unie plaatsvinden, vallen niet onder PSD2.

De *one-leg-in-one-leg-out* bepaling legt ook vast dat PSD2 van toepassing is op betalingen in valuta anders dan EU-valuta, wanneer de betrokken betaaldienstverlener(s) in de EU gevestigd is (zijn). Voorheen vielen betalingen in dollars dus niet onder de Europese regelgeving. Onder PSD2 is dat wel zo, indien een van de partijen een in de EU gevestigde betaaldienstverlener is.

Tijdens de evaluatie zijn geen signalen ontvangen dat betaaldienstverleners problemen hebben met de werking van de *one-leg-in-one-leg-out* bepaling. Wel is het zo dat transacties met een niet-EU partij of met niet-EU valuta minder vaak voorkomen dan transacties tussen twee EU-partijen in EU-valuta.

Conclusie

- Met PSD2 is de geografische reikwijdte uitgebreid, door de *one-leg-in-one-leg-out* bepaling. Dit zorgt voor een gelijker speelveld qua regelgeving en toezicht bij betalingen met niet-EU partijen. Ook is de regelgeving gelijkgetrokken bij betalingen in andere valuta.

6.2 Toezicht

Onderzoeksvraag

1. Hoe verlopen de onderlinge afstemming en communicatie tussen de toezichthouders DNB, AFM, ACM en AP?

Hoe verlopen de onderlinge afstemming en communicatie tussen de toezichthouders DNB, AFM, ACM en AP?

Er zijn vier Nederlandse toezichthouders betrokken bij het toezicht op de bepalingen uit PSD2, namelijk: DNB, AFM, ACM en AP. Deze vier hebben alle afzonderlijke toezichtstaken zoals uiteengezet in sectie 2.1, maar het is van belang dat zij goed samenwerken. Zo zijn er onderwerpen die de afzonderlijke toezicht terreinen overstijgen, waarbij samenwerking en afstemming dus van belang zijn. De onderzoeksvraag richt zich op de onderlinge afstemming en communicatie tussen toezichthouders, dus niet op communicatie van toezichthouders met andere marktpartijen. Marktpartijen hebben uiteraard geen direct zicht op hoe het overleg tussen toezichthouders functioneert. Wel vatten zij enkele signalen samen over de communicatie tussen toezichthouders.

Fout! Verwijzingsbron niet gevonden.1 laat zien dat bijna de helft van de gesprekspartners denkt dat marktpartijen weten bij welke toezichthouder ze moeten zijn met vragen. Tegelijkertijd denkt ruim een kwart dat het onduidelijk is. In lijn hiermee geven sommige marktpartijen in gesprekken aan niet altijd zicht te hebben op welke toezichthouder welke verantwoordelijkheid heeft rond PSD2. Marktpartijen hebben het meeste contact met DNB, andere toezichthouders spreken ze sporadisch. Het komt voor dat ze met een probleem bij de ene toezichthouder aankloppen en dat die de aanbieder naar een andere toezichthouder doorverwijst, die vervolgens weer naar een

[103] Kamerstukken II 2017-2018, 34813, nr. 3, p.3.

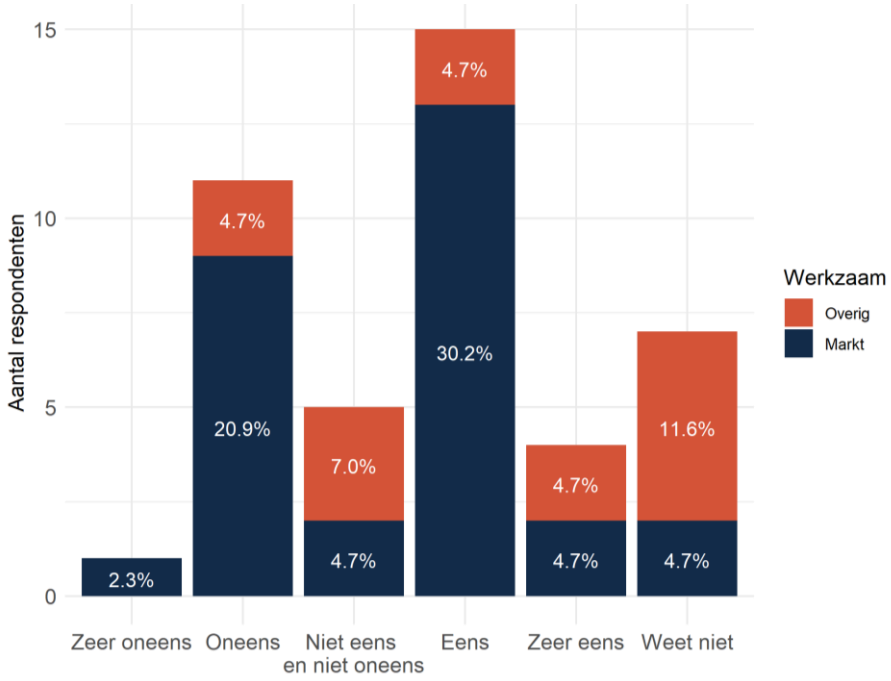
andere toezichthouder doorverwijst. In die gevallen hebben marktpartijen soms een kastje-naar-de-muur gevoel, wat overigens niet alle marktpartijen delen. Volgens sommige gesprekspartners hadden de PSD2-teams bij sommige toezichthouders bij de start van PSD2 nog weinig verstand hadden van betalingsverkeer. Marktpartijen waren dan soms bezig met uitleggen hoe betalingsverkeer werkt.

De informatievoorziening over PSD2 is ook verdeeld over de verschillende toezichthouders. Elke website van een toezichthouder heeft weer zijn eigen informatie over PSD2, waarbij op de website van DNB sommige links naar verdiepende informatie niet meer werken na de overgang naar een nieuwe website. Consumentenorganisaties gaven aan dat er weinig informatie voor consumenten beschikbaar is. De informatie die er is, is niet centraal beschikbaar en bevat veel jargon.

Over contact met DNB zijn de meeste marktpartijen te spreken. Ze ervaren een constructieve houding die informatie goed weet te brengen. Vragen die marktpartijen hebben, stellen ze vaak aan DNB en die zet eventueel vragen door. Dit gaat echter nog niet met de gewenste snelheid, soms moeten marktpartijen lang wachten op een antwoord, omdat de vraag via vele kanalen gaat. Sommige marktpartijen geven aan dat niet elke toezichthouder even goed op de hoogte was van de verschillende terreinen, zo zou DNB weinig aandacht hebben voor de AVG, en de AP zou weinig oog hebben voor betaaldiensten. Dit is verbeterd door de continue dialoog tussen de toezichthouders onderling.

Toezichthouders geven zelf aan dat partijen hen weten te vinden met de relevante vragen. Ook geven ze aan dat ze zelf naar buiten treden, bijvoorbeeld bij het jaarlijkse 'Fintech meets the regulator'-evenement. Wel herkennen ze dat DNB voor de meeste partijen de gesprekspartner is, omdat de meeste onderwerpen ook bij DNB horen.

Figuur 6.1 Stelling: Marktpartijen weten bij welke toezichthouder ze moeten zijn als ze vragen rondom PSD2 hebben



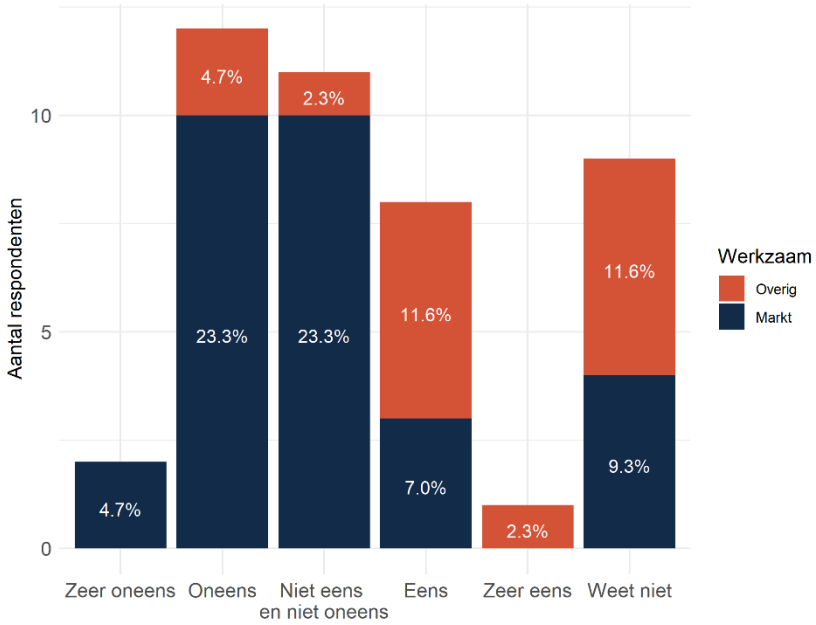
Bron: SEO Economisch Onderzoek op basis van een mini-enquête onder 43 interviewpartners

Marktpartijen, experts en belangenorganisaties vragen zich af of de toezichthouders wel goed met elkaar samenwerken. Uit de online enquête onder gesprekspartners komt naar voren dat het merendeel van de gesprekspartners, 32,7 procent, denkt dat de toezichthouders niet goed samenwerken, terwijl ongeveer 21 procent denkt dat dit wel zo is (Figuur 6.2). Een kwart geeft het aan niet eens en niet oneens te zijn met de stelling, ruim 20 procent weet het niet. Dit geeft aan dat bijna de helft van de gesprekspartners geen goed zicht heeft op de samenwerking. Dat is logisch, want de meeste zijn niet bij de samenwerking betrokken.

Als redenen noemen gesprekspartners de verschillen in cultuur en de verschillende focusgebieden die de organisaties hebben bij PSD2, waarbij ze benoemen dat volgens hen de verschillende toezichthouders elkaar niet altijd goed lijken te begrijpen. Dit is mogelijk een uitvloeisel van de verschillende mandaten die de toezichthouders hebben, waarbij is gekozen voor een verdeling van bevoegdheden die het meest aansluiten bij de bestaande expertise en toezichtsmandaat. Zo merken betrokkenen op dat DNB meer oog heeft voor de uitvoerende en technische aspecten van het betalingsverkeer en dat de AP meer oog heeft voor de juridische aspecten van gegevensbescherming, terwijl de ACM zich vooral focust op een goed functionerende marktwerking.

Overigens bestaat ook het beeld dat de samenwerking nu veel beter is dan in het begin bij de introductie van PSD2 en dat de expertise op het vlak van betalingsverkeer bij de andere toezichthouders is toegenomen door de onderlinge communicatie. DNB wordt gezien als centraal aanspreekpunt voor marktpartijen en coördinator in het overleg met andere toezichthouders.

Figuur 6.2 Stelling: De vier toezichthouders (ACM, AFM, AP en DNB) werken goed samen bij het toezicht op PSD2



Bron: SEO Economisch Onderzoek op basis van een mini-enquête onder 43 interviewpartners

Toezichthouders stellen zelf dat zij uitstekend samenwerken, onder andere in de gezamenlijk opgerichte taskforce. Daarin bespreken zij wie welke vraag oppakt en wisselen zij bevindingen uit. Een kanttekening is dat de toezichthouders stellen dat zij nog vaker de verbinding met de praktijk kunnen leggen, bijvoorbeeld door contact met marktpartijen te zoeken. Het samenspel tussen vier toezichthouders met eigen focusgebieden bleek complexer dan bij aanvang was gedacht. Zo bleek de vormgeving van het toezicht en de rolverdeling, met inachtneming van de verschillende mandaten, complex. De balans tussen het toezicht op gegevensbescherming en het toezicht op de

financiële dienstverlening was lastig te maken, stelt een betrokkene van de beleidsmakers en toezichthouders. Daarbij speelde mee dat sommige bewoordingen (bijv. *consent* of *explicit consent*) niet helemaal overeenkwamen, wat kon leiden tot verschillende interpretaties. Begin 2019 hebben DNB en de AP een samenwerkingsprotocol ondertekend om het toezicht op PSD2 te verbeteren en onderlinge uitwisseling te bevorderen.[104]

Betrokkenen zien verschillen tussen toezichthouders over de grondhouding waarmee ze PSD2 benaderen. Deze verschillen in grondhouding volgen mogelijk uit de verschillende taken en achtergronden van de toezichthouders. Ze merken dat DNB meer oog heeft voor het faciliteren of in ieder geval niet belemmeren van innovatie, terwijl bij de AP de focus ligt op borgen van rechtmatige en veilige persoonsgegevensverwerkingen. De AVG heeft als doel het onnodig delen van data tegen te gaan, terwijl PSD2 juist het delen van betaalgegevens mogelijk maakt om innovatie en concurrentie te bevorderen. Deze wisselwerking tussen PSD2 en AVG leidt tot onduidelijkheid over hoe bedrijven hun dienstverlening moeten inrichten, welke gegevens wel of niet gedeeld mogen worden en hoelang die bewaard moeten blijven. Ten slotte merken sommige marktpartijen en experts op dat de AP wel een bevoegdheid heeft bij PSD2, maar te weinig beschikbaar personeel heeft om die bevoegdheid goed vorm te geven, bijvoorbeeld door *guidance* over de inrichting van privacy en goed zicht op wat marktpartijen met de data doen. Dit kan ook een rem op innovatie zijn, als door deze onduidelijkheden marktpartijen geen nieuwe producten ontwikkelen.

Een voorbeeld van het verschil in interpretatie speelde bij de aanvraag van een PSD2-vergunning van een marktpartij. De marktpartij wilde weten of de dienstverlening conform AVG was ingericht, en vroeg dat aan DNB in het vergunningsproces. De DNB kon dat niet beantwoorden en zette de vraag door naar de AP. De AP wilde echter alleen achteraf controleren, terwijl deze casus ging om controle vooraf, wat aansluit bij de vormgeving van de AVG waarin eigen verantwoordelijkheid voor gegevensbescherming het uitgangspunt is. Dit maakt het echter moeilijker om aan de AVG te voldoen, als er vooraf geen duidelijkheid is, stelt de marktpartij. Andere toezichthouders, die ook met open normen te maken hebben, geven in de beleving van gesprekspartners meer informele *guidance* in één-op-één gesprekken met marktpartijen. Overigens biedt de AVG wel instrumenten om de AP vooraf te raadplegen.

Wisselwerking PSD2 en AVG

Gesprekspartners geven aan dat de wisselwerking tussen verschillende wetten van tevoren niet goed is doordacht en niet goed is omgezet in praktische handvatten voor de markt. Experts geven aan dat beleidsmakers en toezichthouders hier beter over na hadden moeten denken. Er was nog veel discussie over de relatie met de AVG tijdens de implementatie van PSD2, wat de adoptie van PSD2 mogelijk heeft gehinderd. Uit de online enquête onder gesprekspartners blijkt dan ook dat slechts 16 procent van mening is dat de relatie tussen PSD2 en AVG duidelijk is, ongeveer 65 procent vindt deze relatie onduidelijk. Toezichthouders AP en DNB zouden beter kunnen samenwerken bij het geven van *guidance* hoe marktpartijen moeten omgaan met het samenspel van PSD2 en de AVG. Verduidelijking van het samenspel is ook een belangrijke verantwoordelijkheid van de (Europese) wetgever.

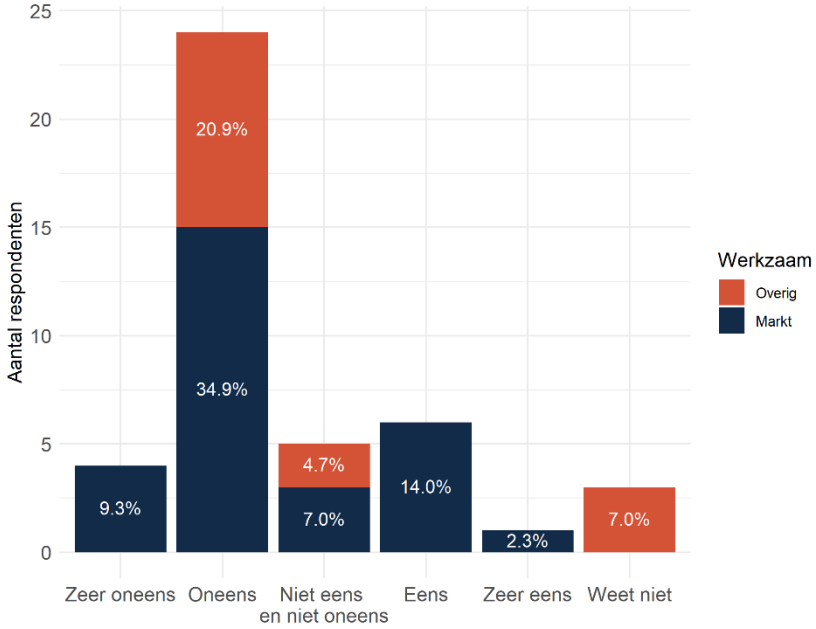
Illustratief is dat banken meer dan twee jaar na inwerkingtreding van PSD2 bezig zijn om hun API's aan te passen aan de eisen die de AVG stelt, terwijl deze goedgekeurd waren tijdens het ontheffingsproces bij DNB. Dit leidt tot extra kosten die voorkomen hadden kunnen worden als dit in een eerder stadium was meegenomen in het proces, waarbij moet worden opgemerkt dat partijen hier ook een eigen verantwoordelijkheid bij hebben. Daarnaast ontbreekt op dit punt ook de Europese coördinatie. In andere landen roept de autoriteit persoonsgegevens voor zover wij dat hebben kunnen achterhalen banken niet op om de interfaces aan te passen, hoewel ook daar de API's van

104 https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/dnb-en-ap-bezegelen-samenwerking-toezicht-op-psd2 (Benaderd op 22-11-2021).

banken dataminimalisatie niet faciliteren. en de EDPB-*guidelines* door alle gegevensbeschermingstoezichthouders worden onderschreven. Meer Europese coördinatie in de keuzes met betrekking tot handhaving van de door alle AP's onderschreven *guidelines* is dan ook gewenst, temeer daar marktpartijen meer en meer zaken over de nationale grenzen heen verrichten. Zonder Europese duidelijkheid brengt dat onzekerheid bij marktpartijen met zich mee.

Het vrijkomen van betaaldata zorgt er ook voor dat het belang van toezicht op gegevensbescherming toeneemt, doordat het toepassingsbereik van betaaldata in de economie groter wordt: er zijn meer datastromen. In de huidige vormgeving van PSD2, waarbij borging van de privacyaspecten van betaalgegevens door de AVG wordt gedekt, komt er ook een grotere verantwoordelijkheid bij de privacy toezichthouders te liggen om ervoor te zorgen dat de AVG wordt nageleefd. De toezichthouder moet daarvoor wel voldoende kennis hebben van een specifieke sector en over voldoende de mensen en middelen beschikken om actief toezicht te houden.

Figuur 6.1 Stelling: De relatie tussen de AVG en PSD2 is duidelijk



Bron: SEO Economisch Onderzoek op basis van een mini-enquête onder 43 interviewpartners

Verschillen tussen landen

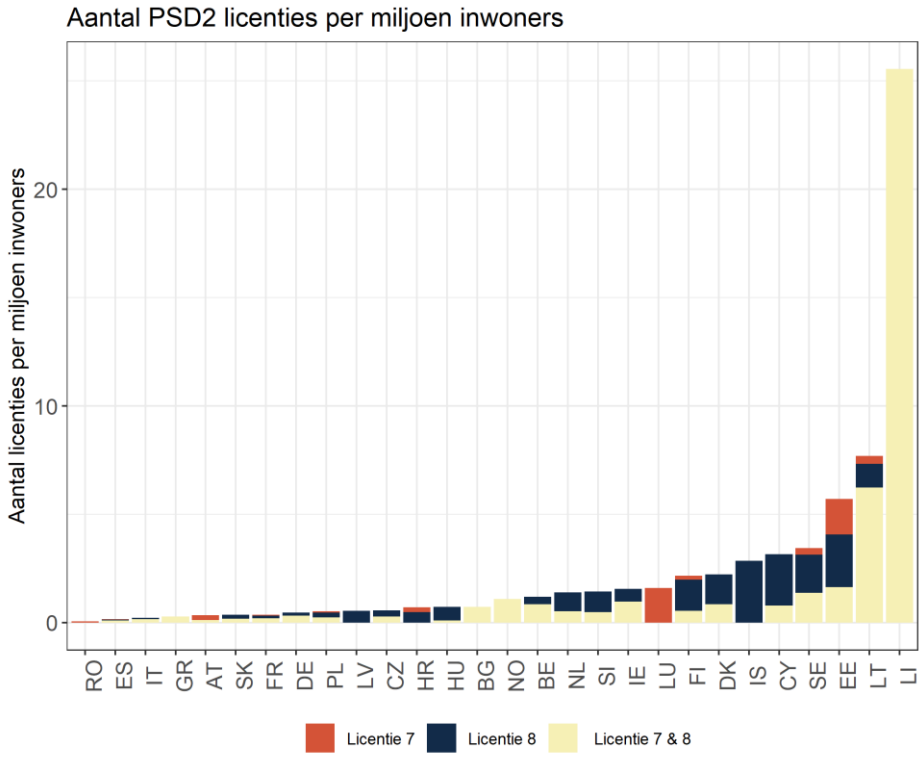
PSD2 is nu een Richtlijn (Directive) van de Europese Commissie. Een Richtlijn is "een rechtshandeling die een bepaald doel vastlegt dat alle EU-landen moeten bereiken. Maar zij mogen zelf de wetgeving vaststellen om dat doel te bereiken."[105] Een aantal gesprekspartners geeft aan dat het beter zou zijn geweest als het een Verordening (*Regulation*) was geweest. Een Verordening is "een bindende rechtshandeling die in de hele EU van toepassing is"[106], daarmee zou PSD2 in elk land hetzelfde zijn geweest. Bij een *Regulation* is er meer harmonisatie en minder fragmentatie binnen de EU, omdat elke lidstaat een Directive vertaalt in eigen wetgeving, die op punten kan verschillen van elkaar.

105 https://european-union.europa.eu/institutions-law-budget/law/types-legislation_nl (Benaderd op 18-1-2021)
106 https://european-union.europa.eu/institutions-law-budget/law/types-legislation_nl (Benaderd op 18-1-2021)

Ondanks de rol van de EBA in het harmoniseren van wetgeving in verschillende landen, hebben vrijheden in interpretatie geleid tot verschillen in de nationale wetgeving. Zo is er een marktpartij die met de handelsagentvrijstelling opereert, maar omdat de verschillende Europese toezichthouders die vrijstelling anders interpreteren, is het niet eenvoudig om daarmee in het buitenland actief te zijn. Daarnaast speelt de vraag dat het niet altijd duidelijk is welke toezichthouder in welke situatie relevant is. Het openen van een bijkantoor in het buitenland is daarom lastig.

Naast de verschillen in de nationale wetgeving die ontstonden door een andere interpretatie en invulling, handhaven toezichthouders in verschillende lidstaten ook verschillend. Uit de EBA-data komt naar voren dat sommige kleine landen in verhouding naar het aantal inwoners veel vergunningen verlenen (Figuur 6.2). Dit suggereert dat het voor betaaldienstverleners aantrekkelijk is om vanuit die landen te opereren, bijvoorbeeld vanwege lage vergunningskosten of minder streng toezicht. Ook gesprekspartners geven aan dat het toezicht in sommige andere landen minder streng is dan in Nederland.

Figuur 6.2 Het aantal licenties er miljoen inwoners is disproportioneel groot in sommige EU-lidstaten



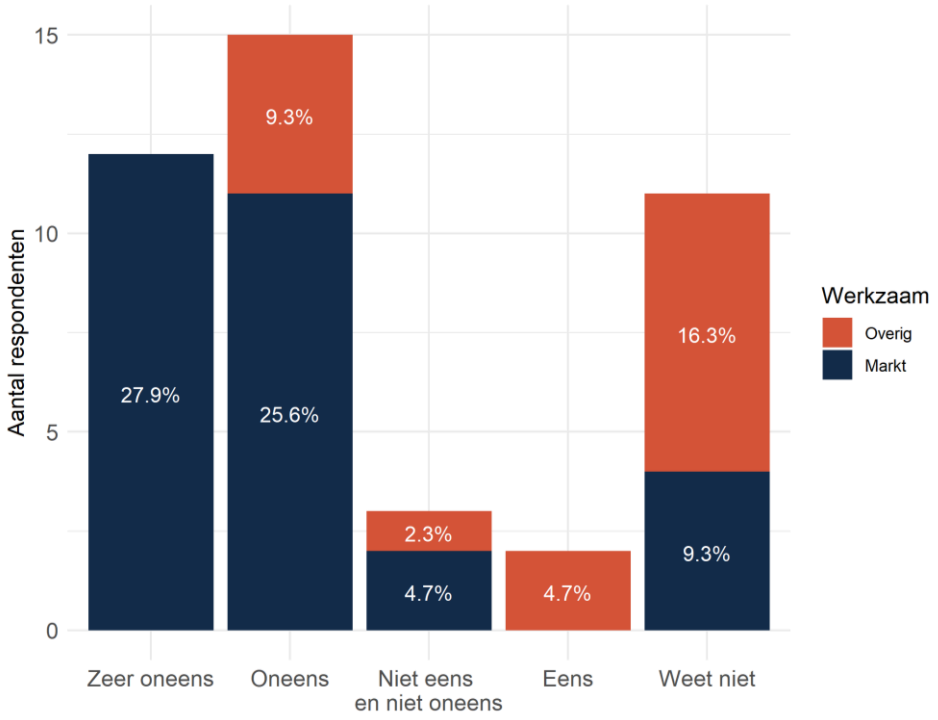
Bron: EBA (2021), o.b.v. analyse EBA-register

Ook de manier waarop toezichthouders omgaan met de interactie tussen PSD2 en de AVG verschilt per land. Nederland is bijvoorbeeld een van de weinige landen waar de AP een rol heeft gespeeld bij de vormgeving van de implementatiewet. Gezien de maatschappelijke zorgen over privacy in Nederland is dit ook een belangrijke rol die de AP vervult. Ook de discussie over dataminimalisatie speelt voor zover wij hebben kunnen achterhalen in andere landen niet of in veel mindere mate dan in Nederland. Illustratief is dat de AP op haar website veruit de meeste informatie over PSD2 geeft, vergeleken met andere leden van de EDPB. De zoekterm "PSD2" levert bij de AP 37 resultaten op, bij de Finse toezichthouder 19 resultaten, bij de Italiaanse toezichthouder 10 resultaten en bij 9

andere toezichthouders 5 of minder resultaten.[107] 15 toezichthouders verwijzen in het geheel niet naar PSD2 op hun website. Dit is een indicatie dat de AP, in vergelijking met haar buitenlandse evenknieën, zeer actief betrokken is bij PSD2.

Uit de online enquête met onze gesprekspartners komt dan ook naar voren dat slechts 5 procent van de ondervraagden vindt dat lidstaten PSD2 op dezelfde manier implementeren in verschillende landen (Figuur 6.3). Bijna twee derde van de ondervraagden geeft aan dat de implementatie verschilt tussen landen.

Figuur 6.3 Stelling: PSD2 wordt in Europa op dezelfde manier geïmplementeerd in verschillende landen



Bron: SEO Economisch Onderzoek op basis van een mini-enquête onder 43 interviewpartners

Conclusie

- De interactie tussen PSD2 en AVG is complex. De grootste noodzaak tot samenwerking en communicatie ligt dan ook bij DNB en de AP over de interactie van PSD2 met de AVG. Over die interactie was zowel voor als na het in werking treden van PSD2 veel onduidelijk.
- Dit vloeit mede voort uit de beperkte aandacht die de Europese wetgever bij het opstellen van PSD2 aan het samenspel met wetgeving rondom persoonsgegevens heeft gegeven.
- Het algemene beeld over de samenwerking tussen toezichthouders is diffuus. Een deel van de betrokkenen geeft aan dat de toezichthouders goed samenwerken, maar een deel denkt dat dit niet goed genoeg gebeurt.
- Met de taskforce PSD2 zoeken toezichthouders toenadering tot elkaar en hebben zij een structuur georganiseerd om beter samen te werken.

107 Deze zoekopdracht is op 16 december 2021 uitgevoerd.

- Een risico is dat EU-landen verschillen in hun interpretatie van PSD2 en uitvoering van toezicht op PSD2. Doordat er sprake is van een Richtlijn en geen Verordening is hiervoor ook meer ruimte. Dat kan ertoe leiden dat het toezicht in sommige landen minder streng is dan in Nederland.
- Betaaldienstverleners met een passportinglicentie komen disproportioneel veel uit een beperkt aantal landen. Mogelijk hangt dit samen met de intensiteit van het toezicht.

7 Conclusie

De evaluatie richt zich op drie hoofdvragen

1. In hoeverre zijn de normen in de implementatiewet doeltreffend en doelmatig in NL, gelet op de in de memorie van toelichting beschreven doelstellingen?
2. Wat zijn de belangrijkste effecten van de implementatiewet in de praktijk?
3. Zijn de waarborgen in de implementatiewet voor de gegevensbescherming in combinatie met bestaande regelgeving adequaat?

Met daarbij een aantal aandachtspunten:

- de bescherming van persoonsgegevens;
- de gevolgen van de invoering van PSD2 voor de marktverhoudingen;
- is de reikwijdte van PSD2 adequaat in het licht van een meer gefragmenteerde betaalketen;
- is voldoende duidelijk welke betaalmiddelen onder het verbod op *surcharging* vallen.

De onderstaande paragrafen geven de conclusies op deze punten weer.

7.1 Doeltreffendheid en doelmatigheid normen implementatiewet

7.1.1 Doeltreffendheid

Toetsstenen voor doeltreffendheid

De memorie van toelichting van het implementatiewetvoorstel PSD2 onderscheidt drie doelen van PSD2, namelijk:

1. Het versterken van interne markt voor kaartbetalingen, internetbetalingen en mobiele betalingen;
2. Problemen van PSD1 zoals gebruik van achterhaalde of vage begrippen verhelpen; en
3. Het stimuleren en faciliteren van innovaties onder meer door het reguleren van nieuwe betaalproducten en -diensten.

Onderliggend hieraan zijn vijf pijlers te onderscheiden die wij zullen hanteren als toetsstenen voor doeltreffendheid, namelijk:

- De mate waarin PSD2 concurrentie bevordert;
- De mate waarin PSD2 innovaties in het betalingsverkeer mogelijk maakt;
- De mate waarin PSD2 de veiligheid van betalingsverkeer vergroot;
- De mate waarin PSD2 bescherming biedt aan deelnemers aan het betalingsverkeer; en
- De mate waarin PSD2 bijdraagt aan het vormen van één Europese betaalmarkt.

Doeltreffendheid betreft de vraag of de normen waaruit PSD2 bestaat doel treffen. Met andere woorden, zijn de doelen van PSD2 gehaald (doelbereik) als gevolg van de implementatie van PSD2?

Doelbereik en causaliteit

Sinds de invoering van PSD2 is sprake van ontwikkelingen op de betaalmarkt die doelbereik suggereren. Dit vormt een indicatie voor de doeltreffendheid van de PSD2-regelgeving.

Concurrentie

PSD2 heeft het mogelijk gemaakt dat nieuwe spelers tot de markt toetreden door het introduceren van de nieuwe diensten 7 (betaalinitiatiediensten) en 8 (rekeninginformatiediensten). Dit heeft ertoe geleid dat diverse nieuwe spelers actief zijn geworden in Nederland. Het gaat hier om zowel partijen die bij DNB onder toezicht staan, als om partijen die gebruikmaken van de mogelijkheid om met een *passport* in Nederland actief te zijn.[108] De producten die deze nieuwe spelers aanbieden zijn vaak niet nieuw en bestonden ook al voor de introductie van PSD2. Wel nieuw is dat de spelers en producten nu gereguleerd zijn. Een toename van het aantal spelers dat dingt om de gunsten van consumenten en bedrijven is in de regel een gunstige ontwikkeling voor de concurrentieverhoudingen op de betaalmarkt. Verschillende gesprekspartners geven dan ook aan dat de concurrentie op de betaalmarkt is toegenomen.

De marktontwikkelingen verschillen per type dienst. Als het gaat om betaalinitiatiediensten hebben bestaande spelers op de betaalmarkt met het betaalproduct iDEAL een groot marktaandeel en is het marktaandeel van nieuwe betaalinitiatiedienstverleners verwaarloosbaar. Als het gaat om rekeninginformatiediensten is er meer concurrentie, hoewel de traditionele banken ook hier belangrijke spelers in zijn.

Ook verschilt de mate waarin nieuwe partijen consumentenmarkt (B2C) dan wel zakelijke markt (B2B) diensten aanbieden. Het gebruik van PSD2-diensten op de B2C is nog beperkt. Het marktaandeel van toetreders op de consumentenmarkt is hiermee klein, maar hier gaat wel concurrentiedruk vanuit waardoor banken meer zijn gaan innoveren (zie Innovatie hieronder). Partijen op de B2B concurreren actiever, bijvoorbeeld aanbieders van boekhoudpakketten. Dit zijn bestaande aanbieders die gebruikmaken van de nieuwe mogelijkheden die PSD2 hen biedt (zie Innovatie hieronder), maar ook kleinere aanbieders die nu ook koppelingen met betaalrekeningen kunnen opnemen in hun administratieve pakketten. Deze partijen zijn minder afhankelijk geworden van bilaterale contracten met banken en praktische belemmeringen die banken in het verleden opwierpen.

We concluderen dat de concurrentie is toegenomen, met meer actieve partijen die minder afhankelijk zijn van bestaande aanbieders. Hoewel de toegenomen concurrentie nog niet is terug te zien in marktaandelen, is wel sprake van potentiële concurrentie, dat wil zeggen dat bestaande partijen de druk van potentiële toetreders voelen. Daarbij bevindt de markt zich nog in een vroeg stadium van ontwikkeling. Er kan dus nog veel veranderen.

Innovatie

De meeste soorten diensten of producten die partijen met een vergunning om betaalinitiatie- en rekeninginformatiediensten, bestonden al voordat PSD2 van kracht was. Nieuwe aanbieders geven deze diensten wel op andere manieren vorm of combineren ze met andere diensten die banken niet aanbieden (denk bijvoorbeeld aan het ophalen van formele documenten uit meerdere bronnen). Op de consumentenmarkt hebben met name bestaande spelers (i.e. de banken) hun productaanbod verbeterd door gebruik te gaan maken van API's. Daarnaast is er sprake van beperkt nieuw aanbod op de consumentenmarkt, maar consumenten maken van deze productinnovaties nog weinig gebruik.

---

108 We hebben geen beeld van de verhouding tussen actieve passporting partijen en partijen met een vergunning onder Nederlands toezicht.

De zakelijke markt maakt meer gebruik van diensten die aangeboden worden onder een PSD2-vergunning. Dit betreft met name boekhoudpakketten. De spelers die zulke pakketten aanbieden maakten pre-PDS2 gebruik van FTP-koppelingen als dat door de banken werd gefaciliteerd. Sinds PSD2 moeten banken een koppeling aanbieden aan eenieder en kiezen deze aanbieders -maar ook nieuwe kleinere aanbieders van boekhoudpakketten- er veelal voor om gebruik te maken van de API's die banken sinds PSD2 verplicht zijn om aan te bieden. Dit is ook innovatie.

Tussen zakelijke of particuliere eindgebruikers en de banken bij wie de betaaldata of de uitvoering van betalingen na initiatie primair ligt zijn ten slotte in toenemende mate nieuwe tussenpartijen actief geworden die fricties in de keten verminderen (*aggregators*). Die fricties zijn het gevolg van twee factoren. Ten eerste, een gebrek aan standaardisering van API's, wat ervoor zorgt dat het voor individuele (potentiële) aanbieders van betaalinitiatie- of rekeninginformatiedienstverlening kostbaar is om (grensoverschrijdend) een dekkend netwerk van API-koppelingen op te bouwen. Ten tweede, de compliancekosten die partijen moeten maken om een PSD2-vergunning te krijgen en te behouden. Gespecialiseerde *aggregators* zijn in dit gat gesprongen door van het aan elkaar knopen van (niet-gestandaardiseerde) API's hun product of dienst te maken die zij zowel aan de bank als de derde partij aanbieden. Een deel van de interviewpartners duidt dit als de grootste (proces)innovatie sinds de invoering van PSD2, hoewel dit ook risico's met zich meebrengt, waar we in sectie 7.1.2 onder het kopje *aggregators* op ingaan .

We concluderen dat als gevolg van PSD2 de innovatie is toegenomen doordat nieuwe partijen reeds bestaande diensten anders zijn gaan vormgeven en combineren, doordat bestaande partijen andere technische oplossingen zijn gaan inzetten (API's) en doordat nieuwe vormen van dienstverlening zijn opgekomen om fricties in de betaalketen te verminderen. Ook hier geldt dat de markt zich nog in een vroeg stadium van ontwikkeling bevindt en er dus nog veel kan veranderen.

Veiligheid

Voordat PSD2 van kracht was, was het merendeel van de huidige betaalinitiatiedienstverleners al actief op de Nederlandse betaalmarkt, waarbij ze toegang tot de betaalrekening middels screenscraping verrichten. Als gevolg van PSD2 zijn deze partijen nu actief op basis van de API-interfaces. Omdat aan screenscraping meer veiligheidsrisico's verbonden zijn, vergroot deze verschuiving de veiligheid van betaaldiensten 7 en 8. Daarnaast zijn deze nieuwe betaaldienstverleners actief op basis van een vergunningsstelsel, waarbij er eisen gesteld worden aan de bedrijfsvoering. Daarbij vindt ook doorlopend toezicht plaats om na te gaan of de vergunningsplichtige dienstverleners aan de toezichteisen blijven voldoen. Ook dit heeft de veiligheid van betaaldiensten vergroot.

Tot slot is als gevolg van PSD2 SCA marktbreed ingevoerd. Gesprekspartners benoemen dat de SCA-eis een technisch passend middel is om de veiligheid te vergroten, maar dat voor de Nederlandse markt het effect van deze eis beperkt is. Dit heeft twee redenen. Ten eerste werd reeds vóór PSD2 bij het leeuwendeel van de betalingen in Nederland SCA toegepast, onder andere doordat iDEAL reeds vóór de invoering van PDS2 SCA-compliant was. Het effect van de introductie van de SCA-eis is daardoor beperkt. Wel zijn er enkele inlogprocedures door banken aangepast en is bij (online) betalingen met creditcards sprake van een (veiligheidsverhogende) verandering van de klantreis, maar het aandeel van zulke betalingen in het totaal is in Nederland relatief klein. De tweede reden is het feit dat fraude verschuift van technische fraude naar fraude op basis *social engineering* waarbij klanten verleid worden om zelf 'de deur van het slot te doen' en toegang te verlenen. Tegen directe misleiding van de consumenten door *spoofing* of *phishing* bieden de technische beschermingsmaatregelen in PSD2 zoals SCA geen bescherming.

We concluderen dat de invoering van PSD2 de veiligheid van betaaldiensten op verschillende manieren heeft vergroot, hoewel het effect van SCA in Nederland beperkt is geweest.

Bescherming van deelnemers aan het betalingsverkeer[109]
Door het onder toezicht brengen van niet-gereguleerde activiteiten als betaalinitiatiediensten en rekeninginformatiediensten en de eisen die toezichthouders vervolgens aan deze partijen stellen, die zien op de bescherming van hun klanten, zijn stappen gemaakt om de deelnemers aan het betalingsverkeer te beschermen. Technische waarborgen zoals SCA en toezichtrechtelijke waarborgen zoals operationele vereisten helpen eveneens om risico's voor consumenten wat betreft betalingen te beperken en de veiligheid van het betalingsverkeer beter te waarborgen.

De regels voor onbedoelde en niet-toegestane overboekingen leggen de verantwoordelijkheid voor het terugbetalen bij de betaaldienstverlener. Consumenten lopen daardoor nauwelijks risico's. Het is de vraag of het niet wenselijk is om enig eigen risico bij consumenten te leggen, aangezien een dergelijk eigen risico consumenten ook een prikkel geeft om zelf actief onbedoelde en niet-toegestane overboekingen te voorkomen. Een dergelijk eigen risico zien we bijvoorbeeld ook in de zorgmarkt.

Door de invoering van PSD2 is de bescherming van deelnemers aan het betalingsverkeer voor zover het betalingen betreft dan ook toegenomen en is deze in onze ogen adequaat.

Bijdragen aan één Europese betaalmarkt
PSD2 komt voort uit de beleidsmatige wens om tot één Europese betaalmarkt te komen, door één Europees regime te creëren voor nieuwe betaaldiensten in heel Europa. Hiernaast biedt PSD2 marktpartijen direct de mogelijkheid om Europa-breed actief te worden via de *passporting*-rechten voor vergunningen om betaalinitiatiediensten en betaalinformatiediensten aan te bieden. Een groeiend aantal spelers maakt gebruik van deze mogelijkheid, bijvoorbeeld door een vergunning in hubs zoals Litouwen aan te vragen en vervolgens over een groot deel van de Europese markt actief te zijn.

Er is volgens marktpartijen heterogeniteit in de interpretatie en de uitvoering van het PSD2-regime, wat het ontstaan van een Europese betaalmarkt remt.[110] Dit is een proces in ontwikkeling. Harmonisatie via EBA-guidelines, Q&A's en andere overleggremia (zoals de ERPB) helpen om fricties in *cross-border* toetreding, aanbod of dienstverlening voor marktpartijen te verminderen. Heterogeniteit in de uitvoering kan ertoe leiden dat het vergunningsverleningsproces en toezichtregime in sommige Europese landen minder strikt is dan in Nederland. Dit is een risico vanuit Nederlands perspectief.

We concluderen dat de invoering van PSD2 bijdraagt aan het ontstaan van één Europese betaalmarkt, waarbij heterogeniteit in de omzetting van de richtlijn zelf en uitvoering van het toezicht een aandachtspunt vormt.

7.1.2 Doelmatigheid normen implementatiewet

Toetsstenen voor doelmatigheid

Doelmatigheid gaat over de wijze waarop de doelen gehaald wordt. Dit valt uiteen in twee onderdelen:
1. Worden de doelen op een efficiënte wijze bereikt; en
2. In welke mate heeft het beleid schadelijke neveneffecten?

We bespreken hier kort de indicaties voor de kosten en lasten waartoe PSD2 leidt en de factoren waardoor deze hoger of lager uitvallen.

[109] Bescherming van persoonsgegevens wordt apart besproken.
[110] Uiteraard is PSD2 een vooruitgang ten opzichte van een volledig nationaal regime.

Implementatiekosten en administratieve lasten

Er zijn geen concrete cijfers beschikbaar over de kosten die gemaakt zijn om PSD2 te implementeren, de administratieve lasten voor partijen van een vergunningaanvraag en de doorlopende compliance kosten die partijen maken. In kwalitatieve zin geven marktpartijen aan kosten gemaakt te hebben voor o.a. vergunningsaanvragen, het aanpassen van processen en het bouwen en technisch inregelen van bijvoorbeeld de onder PSD2-vereiste API's. Hoewel kwantitatieve cijfers ontbreken, is duidelijk dat dit een significante inspanning is geweest voor marktpartijen en toezichthouders. Een aantal kleinere spelers geeft aan dat de kosten voor het verkrijgen en behouden van een vergunning voor een startende speler aanzienlijk zijn.

Marktpartijen geven aan dat het aanvragen van een vergunning lang duurde. Het was voor aanbieders niet altijd duidelijk aan welke eisen ze allemaal aan moesten voldoen en hoe deze eisen te implementeren. Dit leidde volgens hen tot onzekerheid en hogere implementatiekosten. Enkele aanbieders gaven aan dat zij snel een vergunning hebben aangevraagd, maar dat achteraf niet hadden hoeven doen, aangezien zij van een *aggregator* gebruik konden maken. Dit zou kosten hebben gescheeld. Ook kwam het gesprek tussen aanbieders van AISP- en PISP-diensten en banken, wat bijvoorbeeld nodig was bij de vormgeving van API's, moeizaam op gang. Uiteindelijk wisten partijen elkaar in het overleg tussen marktpartijen in het NISP-NL gremium van de Betaalvereniging wel te vinden.

De publiekscampagne die DNB in opdracht van het MOB heeft gehouden, bracht ook kosten met zich mee. Hoewel deze kosten niet onder toezichtkosten vallen, zijn het maatschappelijk gezien wel algemene implementatiekosten. Naast administratieve lasten zijn er ook de handhavingskosten bij de toezichthouders. De bulk van de handhavingskosten ligt daarvan bij DNB, die zij voor het toezicht op PSD2 volledig doorbelast aan de sector.

Het algemeen gedeelde beeld onder marktpartijen is dat Nederlandse toezichthouders strenger zijn dan buitenlandse toezichthouders. De toezichthouders in Duitsland en Frankrijk zijn volgens gesprekspartners ook relatief strikt. Dit heeft als voordeel dat in de markt Nederlandse vergunningen gelden als een kwaliteitswaarborg. Een mogelijk nadeel is dat de kosten van het toezicht en de compliancelasten als gevolg van het strikte toezicht in Nederland hoger zijn dan in sommige andere Europese landen. Het minimaliseren van dergelijke kosten kan een prikkel zijn voor betaaldienstverleners om vanuit landen waar de compliancekosten lager zijn op basis van *passporting* actief te zijn in heel Europa. Uit onze analyse van EBA-data blijkt dat sommige landen disproportioneel veel vergunningen verlenen. Dat kan betekenen dat dergelijke landen bijzonder efficiënte vergunningsprocessen hebben, maar kan ook betekenen dat toezicht er minder ingrijpend is.

Hoewel we geen data hebben die ons in staat stellen deze kosten kwantitatief in kaart te brengen, kunnen we wel een aantal factoren benoemen die de doelmatigheid in negatieve of positieve zin hebben beïnvloed.

Factoren die de doelmatigheid beïnvloeden

Een aantal keuzes in de vormgeving van PSD2 en ontwikkelingen in de markt hebben gevolgen voor de doelmatigheid van PSD2. Hieronder bespreken we deze factoren.

Gebrek aan standaardisering API's

PSD2 biedt geen uniforme standaard voor API's. Het gevolg is dat verschillende banken allemaal verschillende API's hebben ontwikkeld en elke bank opnieuw het wiel moest uitvinden, hoewel enige mate van standaardisering plaatsvond via de RTS van EBA en werk binnen de Berlin Group. Op macroniveau resulteren daarmee extra implementatiekosten. Ook leidt dit tot extra kosten voor betaaldienstverleners die via meerdere banken diensten willen verlenen. Zij moeten immers koppelingen met API's, die in de praktijk vaak net verschillend werken, zien te maken en te onderhouden.

Standaardisatie van API's kan tot lagere kosten leiden en het gebruik van PSD2-diensten een impuls geven, ook door betere Europese schaalbaarheid van innovaties. In de UK biedt de *Open Banking Implementation Entity* (OBIE) wel een standaard voor API's en open banking heeft daar ook een grotere vlucht genomen. Het ontwikkelen van een uniforme standaard leidt tot snellere acceptatie in de markt, minder discussie met de toezichthouder en minder discussie tussen banken en betaaldienstverleners. Veel gesprekspartners geven aan dat PSD2 niet ver genoeg gaat op het gebied van standaardisering. Marktpartijen noemen vaak dat een standaard voor API's wenselijk is, al is daar niet iedereen het mee eens. Marktpartijen noemen vaak dat een standaard voor API's wenselijk is, al is daar niet iedereen het mee eens. Voorstanders stellen dat een standaard toegang tot de betaalgegevens vereenvoudigt en concurrentie bevordert. Tegenstanders benoemen dat een standaard is dat het innovatie kan belemmeren als deze niet technologisch neutraal is of dat het risico bestaat dat de verkeerde API-standaard wordt gekozen.

Gemandateerde standaardisering van API had er ook toe geleid dat de discussie over wat de eisen in de AVG en PSD2 betekenen voor de vormgeving van API's eerder plaats had gevonden. Dat had Europese wetgevers en toezichthouders mogelijk aangezet om over het samenspel van de twee wetten na te denken voordat de wet in de praktijk geïmplementeerd werd. In de UK neemt de OBIE, een onafhankelijke organisatie die op aanwijzing van de *Competition and Markets Authority* (CMA) in 2017 is opgericht door de 9 grootste retailbanken in de UK om Open Banking te implementeren, aspecten zoals consent management of dataminimalisatie mee in haar API-standaarden. Het vermindert zo compliance- en ontwikkelkosten voor banken omdat bepaalde vraagstukken gecentraliseerd geadresseerd worden.

Anderzijds kunnen er ook nadelen zitten aan (verdere) standaardisering van API's. Zo kunnen banken samenwerken en afspraken maken over de vormgeving van API's, wat mogelijk de TPP's benadeelt. Ook kunnen er nadelen zitten aan het via API's vastleggen van bepaalde vormgevingsaspecten die achteraf bezien niet handig blijken. De markt zit er dan immers aan vast. Daarnaast kan het een rem zijn op innovatie als marktpartijen nieuwe ontwikkelingen vertraagd kunnen inbedden doordat de *regulatory* standaard eerst moet worden aangepast.

In de praktijk hebben de verschillen tussen banken geleid tot de opkomst van *aggregators*. Dit is in principe een werkbaar model dat een brug slaat tussen flexibiliteit in de vormgeving en het drukken van kosten door het benutten van schaalvoordelen en vermindert de toegevoegde waarde van een standaard vanuit het perspectief van het verminderen van transactiekosten. Het is dan wel belangrijk dat het toezicht op het ecosysteem dat zo ontstaat, waarbij onder PSD2 gereguleerde *aggregators* data doorgeven aan niet-gereguleerde dienstverleners, wat onder PSD2 is toegestaan, passend is.

We concluderen dat een API-standaard nog steeds veel zou toevoegen, ook al zijn er inmiddels *aggregators*, omdat het ook de discussie over wat wel en niet nodig is om compliant te zijn met wetgeving centraliseert en structureert. Als er een standaard was opgesteld, had dit bijvoorbeeld een belangrijke bijdrage kunnen leveren aan helderheid voor de markt over hoe de eisen van de AVG en de PSD2 met elkaar te verenigen.

Gratis toegang en efficiëntieprikkels

PSD2 mandateert gratis toegang tot de betaalinfrastructuur van banken. In geval van toegang tot betaaldata speelt hier het argument dat de klant moet kunnen beschikken over zijn eigen data. Dit argument speelt niet bij betaalinitiatiediensten. Banken maken kosten om de betaalinfrastructuur te onderhouden, terwijl zij niet alle baten hiervan kunnen internaliseren doordat derden hier gratis toegang toe krijgen. Dit vermindert aan de marge de prikkel voor banken om te investeren in die infrastructuur, zeker op het moment dat een steeds groter deel van de baten die de infrastructuur genereert 'weglekt' naar niet-bancaire aanbieders. Vooralsnog speelt dit in Nederland maar in zeer

beperkte mate omdat PSD2-diensten hier niet veel voet aan de grond hebben gekregen. Vanuit concurrentie- en innovatieoogpunt is de keuze voor gratis toegang op dit moment te rechtvaardigen, maar naarmate het gebruik van PSD2-diensten toeneemt, wordt het belangrijker oog te hebben voor dit nadeel.

Een vergelijkbaar punt betreft het verbod op *surcharging*. Voor marktpartijen zoals banken en toonbankinstellingen is voldoende duidelijk welke betaalmiddelen onder het verbod op *surcharging* vallen. De gedachte achter het verbod is dat PSD2 een gelijk speelveld creëert voor verschillende betaalinstrumenten en de consumenten beschermt. Voor consumenten is het prettig dat zij niet voor verrassingen komen te staan of niet zichtbaar meer hoeven te betalen voor het gebruik van bepaalde betaalproducten, hoewel zij veelal niet weten wat *surcharging* is.[111] Ook voorkomt het dat een partij met marktmacht een specifieke betaalaanbieder bevoordeelt ten koste van andere. Voor het betaalsysteem kan het verbod op *surcharging* echter nadelige gevolgen hebben als dit de mogelijkheid wegneemt om consumenten te prikkelen efficiënte betaalproducten te gebruiken, wat ertoe kan leiden dat relatief dure betaalmethoden algemeen gangbaar worden. Als genoeg consumenten dergelijke betaalmethoden gebruiken, hebben toonbankinstellingen immers geen andere keuze dat de betaalmethode te faciliteren.

Wij concluderen dat deze elementen van PSD2 de doelmatigheid mogelijk negatief kunnen beïnvloeden. Hoewel dit momenteel niet speelt, kan dit wel in de toekomst een aandachtspunt worden naarmate PSD2 succesvoller wordt.

Opkomst van aggregators

Een gerelateerd punt is dat met de opkomst van *aggregators* derde partijen via dergelijke *aggregators* diensten op basis van betaaldata kunnen verlenen zonder dat zij onder PSD2-toezicht vallen.[112] Op de *aggregators* zelf is PSD2-toezicht van toepassing. Daarmee zijn er adequate waarborgen voor veiligheid en gegevensbescherming. Op de derde partijen die een *aggregator* gebruiken is PSD2 niet van toepassing. Een toezichthouder als DNB heeft daarom geen zicht op het datagebruik van dergelijke partijen die wel gebruikmaken van betaaldata. Het ontbreken van zicht bij de toezichthouder op wat dergelijke derde partijen precies doen, leidt tot ongemak bij veel gesprekspartners, hoewel er geen feitelijke voorbeelden van misstanden zijn.

Met betrekking tot gegevensbescherming ligt de verantwoordelijkheid om dergelijke derde partijen te monitoren daarmee bij de AP. De AVG is immers ook van toepassing in gevallen dat dienstverleners niet PSD2-vergunningplichtig zijn. Een nadeel van deze situatie is wel dat de intensiteit van het toezicht waarschijnlijk lager is dan onder een vergunningsplicht. Bij een vergunningsplicht voert de toezichthouder een ex-ante toets uit en is sprake van een doorlopende bewaking van de mate waarin partijen voldoen aan de in de vergunning gestelde voorwaarden. Bij 'generiek' AVG-toezicht op basis van de eigen verantwoordelijkheid van de organisatie is hier geen sprake van en is ook de doelgroep niet structureel in kaart. Dit is overigens inherent aan de wijze waarop binnen de Europese kaders het AVG-toezicht is vormgegeven.

Voorts hoeven dienstverleners niet noodzakelijkerwijs binnenlands te zijn. Voor buitenlandse partijen die in Nederland actief zijn, moet vertrouwd worden op buitenlandse toezichthouders. Dit creëert de noodzaak van verregaande afstemming en communicatie tussen toezichthouders in verschillende landen. Hoewel de EBA en de EDPB streven naar een uniforme interpretatie en uitvoering van wetgeving in Europa, zijn er in de praktijk volgens marktpartijen

111 Nu expliciete tarifering niet mogelijk is, slaan de kosten van het betalingsverkeer neer in de kosten (en prijs) van de aangekochte producten.

112 Daarnaast kunnen AISP's en PISP ook veel diensten uitbesteden die bewerkingen van betaaldata vereisen. De uitbesteding met betrekking tot dataopslag, beveiligingssoftware en databewerking is standaard praktijk in de financiële sector, waarbij de financiële instelling onder toezicht staat voor deze uitbestede taken.

verschillen tussen landen in toezichtsintensiteit en interpretatie, maar ook in prioritering.[113] DNB en de AP hebben geen zicht en geen grip op *aggregators* die op basis van buitenlandse *passporting* in Nederland opereren. Uiteraard is er wel buitenlands toezicht. Arbitragemogelijkheden in het toezicht zijn in een Europese markt met meerdere bevoegde autoriteiten en *passporting* een generiek aandachtspunt, temeer als er onduidelijkheid bestaat over hoe de verantwoordelijkheden binnen een verlengende keten georganiseerd zijn.

We concluderen dat het regulerend kader adequaat is voor toezicht op aggregators. Desondanks zijn wel risico's spelen bij de niet-gereguleerde dienstverleners omdat deze partijen niet onder PSD2-toezicht vallen. De reikwijdte van PSD2 is niet adequaat om op dergelijke partijen toezicht te houden. Ook wordt het extra belangrijk dat de toezichtstandaarden in andere EU-landen vergelijkbaar zijn met die in Nederland.

Complexiteit samenhang PSD2 en de AVG

De interactie tussen de twee wetten is complex. Als het bijvoorbeeld gaat om consent, speelt DNB een rol als het gaat om uitdrukkelijke instemming en stelt expliciet vast hoe hieraan te voldoen. De AP houdt hierbij onder meer toezicht op uitdrukkelijke toestemming op basis van open normen. Het toezicht op de informatieverstrekking, die de basis vormt waarop consumenten zich kunnen informeren om consent te geven, ligt bij de AFM. Er zijn dus drie toezichthouders op dit ene aspect betrokken, waarbij elke toezichthouder zijn eigen rol vervult vanuit zijn eigen verantwoordelijkheid, maar waar het eindresultaat voor marktpartijen en gebruikers afhangt van het samenspel van het toezicht uit de verschillende hoeken. Hoewel de interactie tussen de toezichthouder inmiddels goed verloopt, ontstaat daarbij complexiteit doordat verschillende toezichtmandaten, dezelfde terreinen raken.

De complexiteit in de interactie tussen de twee wetten zorgt voor kosten bij marktpartijen, bijvoorbeeld omdat zij na moeten gaan hoe hun bedrijfsvoering aansluit bij verschillende toezichtkaders. Ook zijn er de kosten van onzekerheid: als ex ante niet duidelijk is hoe de toezichtspraktijk zal uitvallen, zullen marktpartijen minder geneigd zijn om nieuwe activiteiten te gaan ontplooien. Dit is een mogelijke rem op het succes van PSD2.[114]

Een aanzienlijk deel van de gesproken partijen vindt de samenhang tussen de AVG en PSD2 onduidelijk, hoewel er met de EDPB-*guidelines* een belangrijke stap is genomen. Deze vermeende onduidelijkheid hoeft niet noodzakelijkerwijs overeen te komen met de toezichtrechtelijke realiteit die verantwoordelijkheden juridisch regelt. Echter is dit wel een signaal dat toezichthouders beter met elkaar en de buitenwereld kunnen communiceren over deze samenhang. Een groot deel van de gesprekspartners geeft dan ook aan dat ze behoefte hebben aan praktische *guidance* in specifieke gevallen. Alternatief was geweest dat de Europese wetgever deze verhouding anders had kunnen regelen, bijvoorbeeld door sommige AVG-vereisten direct te incorporeren in PSD2. De AVG maakt het ook mogelijk dat gegevensbescherming in sectorale wetgeving wordt uitgewerkt. PSD2 zou dan meer invulling geven aan bepaalde AVG-beginselen zoals dataminimalisatie. Dat zou bij sommige partijen een deel van de privacy-zorgen mogelijk hebben kunnen wegnemen, wat de adoptie van PSD2 ten goede zou zijn gekomen.

Verschillen tussen landen

Ook is relevant dat toezichthouders in verschillende landen in de praktijk volgens gesprekspartners verschillen in interpretatie van PSD2, terwijl ook de implementatie per land kan verschillen. Daarbij verschilt ook de manier waarop landen omgaan met de interactie tussen de AVG en PSD2. Dit kan leiden tot toezichtarbitrage tussen landen, en tot verschillen in toezichtintensiteit tussen toezichthouders binnen landen en reikwijdtebepalingen in

113 Verschillen tussen landen concreet in beeld brengen valt buiten de scope van dit onderzoek.
114 In een bredere context is bewust gekozen voor open normen in de AVG om innovatie niet in de weg te zitten.

verschillende stukken wet- en regelgeving die al dan niet van toepassing zijn op bepaalde aanbieders. Activiteiten van de EBA en de EDPB om tot meer harmonisatie te komen blijven daarom belangrijk.

7.2 Belangrijkste effecten in de praktijk

De inschatting van doeltreffendheid en doelmatigheid bespreekt een aantal neveneffecten van PSD2 die gevolgen hebben voor doeltreffendheid en doelmatigheid. Niet alle effecten zijn even groot, of van even groot belang voor de Nederlandse markt. Hieronder bespreken we de belangrijkste effecten van PSD2. Sommige effecten overlappen met de eerder in het kader van doelmatigheid besproken neveneffecten.

Geharmoniseerd Europees regime
Wel heeft PSD2 een geharmoniseerd Europees regime voor nieuwe betaaldiensten gecreëerd, wat ertoe geleid heeft dat er meer aanbieders van betaalinitiatie- en rekeninginformatiediensten op de markt zijn gekomen, zowel voor consumenten als voor bedrijven. Een groot deel van die partijen heeft via *passporting* een vergunning om PISP- of AISP-diensten aan te bieden in Nederland. Dat heeft tot gevolg dat de kwaliteit van toezicht op PSD2 en de AVG in andere EU-landen belangrijker wordt voor de veiligheid en gegevensbescherming in Nederland.

Nog geen nieuwe diensten, wel meer aanbieders
Gesprekspartners benoemen dat PSD2 nog niet heeft geleid tot diensten die heel anders of veel efficiënter zijn dan reeds bestaande diensten. Veel van de diensten die PISP of AISP aanbieden waren voor PSD2 ook al op de markt. Bij rekeninginformatiediensten zijn er wel enkele nieuwe diensten ontstaan. Wel zijn er meer aanbieders.

Gebruik van PSD2-diensten nog beperkt
Hoewel er wel meer aanbieders actief zijn geworden op de Nederlandse markt, is het beeld in de markt, bij consumentenorganisaties en bij toezichthouders dat het gebruik van PSD2-diensten nog beperkt is, vooral bij consumenten (B2C-diensten). Een reden hiervoor is dat iDEAL in Nederland al erg sterk is en het -qua kosten- lastig is om hiermee te concurreren. Daarnaast zijn consumenten ook terughoudend als het gaat om delen van betaalgegevens of derde partijen toegang geven tot de betaalrekening. Er is echter geen concreet cijfermateriaal over gebruik in publieke bron beschikbaar. Hoewel er bij B2B-diensten meer succes is, is ook daar het gebruik nog beperkt.

Wel innovatie zichtbaar
Ondanks het beperkte gebruik, is er op onderdelen wel innovatie zichtbaar. Zo kunnen kleine partijen op de markt voor administratieve software nu ook directe koppelingen met de betaalrekening van banken aanbieden. Een onverwachte ontwikkeling is de opkomst van PSD2-aggregators, die fricties in de markt verminderen, door compliancekosten en ontwikkelkosten te centraliseren. Innovatie komt daarnaast uit de hoek van bestaande aanbieders: zij voelden druk om te innoveren na de komst van PSD2. Ook heeft PSD2 ervoor gezorgd dat banken API's zijn gaan gebruiken voor hun betalingsverkeer. Dit maakt nieuwe diensten mogelijk.

Te vroeg om een effect van PSD2 te zien op de marktstructuur
De wet bestaat echter nog maar kort. Dit voorlopige beeld van de belangrijkste effecten in de praktijk moet dus ook in dat licht bezien worden. Het is goed mogelijk dat er nieuwe producten of diensten op de markt komen of meer aanbieders op de markt toetreden waardoor PSD2 alsnog een succes wordt in Nederland. Het is dan ook te vroeg om een effect van PSD2 te zien op de marktstructuur voor betalen (dienst 7) en betaaldata gedreven diensten (dienst 8) in Nederland. Ook is de situatie in andere EU-landen anders dan in Nederland. In sommige landen lijkt meer ruimte te zijn voor innovatie in de betaalmarkt, Nederland loopt immers voorop op het vlak van efficiëntie en

innovativiteit van betaaldiensten. Naar verwachting zal PSD2 daar ook grotere effecten hebben. De Europese evaluatie van PSD2 zou hier meer zicht op kunnen geven.

Zorg over risico's voor kwetsbare groepen ongegrond
Belangenorganisaties maakten zich bij de invoering zorgen dat met name kwetsbaardere groepen zoals ouderen en visueel beperkten last zouden ondervinden van PSD2, bijvoorbeeld doordat diensten te veel digitale kennis vragen of omdat ze het risico zagen op nieuwe vormen van fraude. Er zijn echter weinig klachten hierover gekomen en de zorgen over PSD2 zijn in de praktijk tot nu toe ongegrond gebleken. Een reden daarvoor is dat deze kwetsbare groepen (en consumenten in het algemeen) op dit moment nog nauwelijks gebruikmaken van PSD2. Toezichthouders zien een vergelijkbaar beeld. In het algemeen heeft PSD2 de veiligheid van betalingen vergroot door het verplicht stellen van SCA-authenticatie en het onder toezicht brengen van nieuwe betaaldiensten.

7.3 Toereikendheid waarborgen gegevensbescherming

PSD2 heeft tot doel om betaalgegevens, met uitdrukkelijke instemming van de consument, beschikbaar te maken aan derde partijen. Voor zover dit persoonsgegevens betreffen, heeft PSD2 daarmee tot gevolg dat, afhankelijk van het succes van nieuwe betaalinformatiediensten, de datastromen van persoonsgegevens toenemen. Hiermee nemen ook risico's voor de privacy toe, tenzij deze risico's door adequate maatregelen ingeperkt worden.

PSD2 en AVG bieden gezamenlijk adequate waarborging voor gegevensbescherming. Het toezicht van DNB omvat een ex ante vergunningstraject, actief toezicht op basis van concrete normen en jaarlijks terugkerende rapportages garanties op naleving omvat. Het toezicht vanuit de AVG is ex post, controle op basis van open normen, vooral gebaseerd op gewaarworden van de normen van de AVG. In februari 2020 is de AP bijvoorbeeld een onderzoek gestart naar bedrijven met een PSD2-vergunning met als doel 'te weten te komen of die bedrijven zich bewust zijn van de privacyrisico's die de verwerking van rekeninggegevens met zich meebrengt en of ze voldoen aan de privacyregelgeving.' De AP heeft met ons geen informatie gedeeld over eventuele bevindingen, maar van dergelijk onderzoek gaat naar verwachting een disciplinerende werking uit richting de markt.

De vervolgvraag is uiteraard of partijen de eisen van PSD2 en de AVG daadwerkelijk naleven. In hoeverre de waarborgen in PSD2 in de praktijk feitelijk worden nageleefd, kunnen we in deze evaluatie niet beoordelen. Toezichthouders hebben hierover geen informatie met ons gedeeld. Beide toezichthouders hebben volgens marktpartijen echter beperkt zicht op wat er feitelijk met data gedaan wordt, waarbij DNB vanwege rapportageverplichtingen en vergunningstrajecten waarschijnlijk meer zicht heeft op feitelijk gebruik dan de AP. Dat is ook niet vreemd gezien de beperkte omvang en het brede werkveld van de AP. Wel is ons beeld dat de wettelijke waarborgen voldoende zijn om een zorgvuldige omgang met betaalgegevens te borgen.

Door langer wordende betaalketens en de opkomst van *aggregators* vallen sommige partijen die wel werken met betaaldata niet onder toezicht van PSD2. Zij zijn of technische dienstverleners en om die reden uitgesloten van de reikwijdte van PSD2 of maken gebruik van de PSD2-vergunningen van *aggregators*. Dat betekent dat voor dergelijke partijen alleen AVG-toezicht en de contractuele overeenkomsten met partijen die wel onder toezicht staan het gebruik van betaalgegevens reguleert. Gezien de gevoeligheid van betaalgegevens lijkt ons dit onwenselijk. Het gebrek aan zicht op het feitelijke gebruik van betaaldata is een risico. Tegelijkertijd is dit vooral een compliance

vraag. Als alle partijen, zowel degene die binnen als degene die buiten het bereik van PSD2 vallen, zich aan de gecombineerde normen van PSD2 en de AVG houden, is gegevensbescherming toereikend gewaarborgd.[115]

Partijen kunnen ook via *passporting* actief zijn. Dat betekent dat zij niet onder Nederlands toezicht vallen. In dat geval hebben Nederlandse toezichthouders geen zicht op compliance. Daarbij kunnen toezichthouders uit andere EU-landen het toezicht anders invullen, hoewel het toezicht moet voldoen aan de Europese kaders van PSD2. De mogelijkheid dat toezichthouders in andere landen minder streng toezien op de eisen uit PSD2 zien sommige gesprekspartners ook als een risico.

[115] Dit raakt ook aan de algemene figuur van uitbesteden in de Wft.

Literatuur

ACM (2020). Big Techs in het betalingsverkeer, Den Haag: Autoriteit Consument & Markt.

Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. (2016). The Economics of Privacy. Journal of Economic Literature, 54 (2), 442-92.

Athey, S., Catalini, C., & Tucker, C. (2017). The digital privacy paradox: small money, small costs, small talk. *NBER Working Paper 23488*, NBER, Cambridge, MA.

Bijlsma, M., Bolt, W., Jonker, N. (2021). Regulering toegang betaalinfrastructuur vergt nadere analyse, *Economische Statistische Berichten, 102*(47), 43-47.

Bijlsma, M.J., Van der Cruijsen, C., & Jonker, N. (2021). Not All Data are Created Equal - Data Sharing and Privacy, 2021, *De Nederlandsche Bank Working Paper No. 728*.

DNB (2020). MOB-rapportage, Amsterdam: De Nederlandsche Bank.

ERPB (2021). Report from the ERPB working group on transparency for retail payment end-users. *ERPB Report 2021/006*.

Steinfeld, N (2016). "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment, Computers in Human Behavior, Volume 55, Part B, 2016, Pages 992-1000, ISSN 0747-5632, https://doi.org/10.1016/j.chb.2015.09.038.

Van Praag, E.J. (2020). PSD2: naar open banking en bankieren in een ecosysteem. *Preadvies voor de Vereniging voor Financieel Recht 2020*.

Bijlage A Onderzoeksvragen

Thema	Subthema	Onderzoeksvraag	Bespreking in rapport
Markt voor betaaldiensten	Concurrentie	Is het aanbod van betaaldiensten veranderd in Nederland door PSD2 en wat heeft dat voor effect gehad op de concurrentie?	
Markt voor betaaldiensten	Concurrentie	Verloopt toegang tot de betaalrekening en transactiedata op objectieve, evenredige en niet-discriminerende wijze?	
Markt voor betaaldiensten	Concurrentie	Hoe verloopt toegang tot betalingssystemen, met name rekening houdend met de mate van concurrentie (108 lid c)**?	
Markt voor betaaldiensten	Concurrentie	Wat zijn de gevolgen voor de marktverhoudingen (concurrentie, diversiteit, monopolies, markt-macht)?	
Markt voor betaaldiensten	Concurrentie	Is het voldoende duidelijk welke betaalinstrumenten er wel en niet onder het verbod op surcharging vallen?	
Markt voor betaaldiensten	Innovatie	In welke mate faciliteert en stimuleert PSD2 innovaties?	
Markt voor betaaldiensten	Innovatie	Zijn nieuwe spelers en nieuwe producten op de markt gekomen?	
Markt voor betaaldiensten	EU-betaalmarkt	Is grensoverschrijdend betalen voor consumenten en bedrijven gemakkelijker en goedkoper geworden?	
Markt voor betaaldiensten	Consumentenzijde	Zijn er kwetsbare groepen voor wie dit wetsvoorstel tot problemen heeft geleid? Zo ja, voor welke groepen en tegen welke problemen lopen zij aan?	
Veiligheid borgen	Bescherming toegang	Wat zijn de effecten van strong customer authentication?	
Veiligheid borgen	Bescherming toegang	Wat is de impact van SCA op de omvang van de betalingsfraude en moeten aanvullende maatregelen worden overwogen?*	
Veiligheid borgen	Bescherming toegang	Wat zijn oplossingen die gebruikers in staat stellen hun transacties makkelijker te monitoren, rekening houdend met aanbevelingen ERPB?*	
Veiligheid borgen	Bescherming betalingen	Voldoen de regels over niet-toegestane en onbedoelde overboekingen?	
Veiligheid borgen	Bescherming betalingen	Zijn additionele maatregelen nodig om het hoge beschermingsniveau van andere betaalinstrumenten voor consumenten ter realiseren bij instantbetalingen?*	
Veiligheid borgen	Bescherming betalingen	Bieden de wettelijke grenzen voor uitzonderingen bij contactloze betalingen voldoende evenwicht gemak en frauderisico?*	
Veiligheid borgen	Bescherming betalingen	Wenselijkheid van maximumbedragen bij betalingen waarbij autorisatie vooraf gegeven wordt (108 lid f)?**	

Thema	Subthema	Onderzoeksvraag	Bespreking in rapport
Veiligheid borgen	Bescherming dienstverleners	Is de huidige reikwijdte van PSD2 adequaat met het oog op technische dienstverleners bij betaaldiensten en fragmentatie in de keten van betaaldienstverleners (mede gelet op regels voor uitbesteding in PSD2)?	
Veiligheid borgen	Bescherming dienstverleners	Welke nieuwe risico's vloeien voort uit niet-gereglementeerde diensten?*	
Veiligheid borgen	Bescherming dienstverleners	Zijn de vrijstellingen in PSD2 toereikend en moeten de prudentiële, operationele en consumentenbeschermingsvereisten worden gewijzigd?*	
Gegevensbescherming consumenten	Waarborgen gegevensbescherming	Zijn er voldoende waarborgen in de implementatiewet voor gegevensbescherming in combinatie met bestaande regelgeving?	
Gegevensbescherming consumenten	Toegang tot gegevens	Is voldoende geborgd dat er geen toegang is tot meer gegevens dan noodzakelijk?	
Gegevensbescherming consumenten	Toegang tot gegevens	Weten mensen voldoende waar ze ja tegen zeggen als ze toestemming geven aan toegang tot hun betaalgegevens?	
Gegevensbescherming consumenten	Toegang tot gegevens	Wordt de toestemming voldoende expliciet en specifiek gevraagd?	
Gegevensbescherming consumenten	Toegang tot gegevens	Geeft de consument bewust toestemming (i.e. volledig bewust van de gevolgen van het geven van toestemming)?	
Gegevensbescherming consumenten	Toegang tot gegevens	Voelt de consument zich vrij om toestemming te weigeren?	
Gegevensbescherming consumenten	Toegang tot gegevens	Kunnen mensen eenvoudig terug komen op een gegeven toestemming?	
Gegevensbescherming consumenten	Toegang tot gegevens	Hoe kunnen consumenten worden geholpen bij het bewaren van overzicht ten aanzien van de gegeven toestemmingen (dat kan d.m.v. het dashboard van banken, maar zijn er ook andere manieren)?	
Gegevensbescherming consumenten	Gebruik van gegevens	Leveren de bepalingen in de implementatiewet in verhouding tot de AVG in de praktijk uitdagingen/problemen op (met inachtneming van de verduidelijking die de EDPB heeft geboden)?	
Gegevensbescherming consumenten	Gebruik van gegevens	Hoe worden betaalgegevens gebruikt (doelbinding)?	
Gegevensbescherming consumenten	Gebruik van gegevens	Worden betaalgegevens ook gebruikt voor maatschappelijk onaantrekkelijke doelen?	
Regelgeving en toezicht	Ontwikkeling regelgeving	Zijn de gesignaleerde problemen van PSD1 verholpen?	
Regelgeving en toezicht	Ontwikkeling regelgeving	Toepasselijkheid van PSD2 op one-leg-in-one-leg-out betalingen waarvan een deel in de EU plaatsvindt (108 lid b)**	

Thema	Subthema	Onderzoeksvraag	Bespreking in rapport
Regelgeving en toezicht	Ontwikkeling regelgeving	Toepassing en effect van bepalingen rondom drempelwaardes en vrijstellingen (108 lid e)**	
Regelgeving en toezicht	Toezicht	Hoe verlopen de onderlinge afstemming en communicatie tussen de toezichthouders DNB, AFM, ACM, en AP?	

Bijlage B Interviewpartners

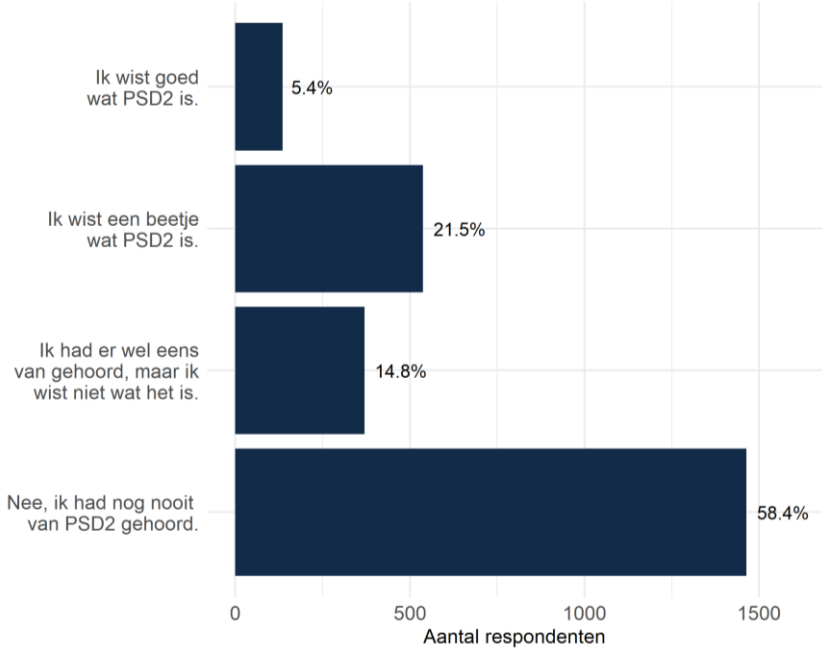
Voor dit onderzoek hebben wij 51 partijen geïnterviewd.

Groep	Organisatie
Banken	ABN AMRO
Banken	ING
Banken	Rabobank
Banken	Volksbank
Beleidsmaker	Europese Commissie DG FISMA
Beleidsmaker	Europese Commissie DG COMP
Beleidsmaker	Ministerie van Justitie en Veiligheid
Beleidsmaker	Ministerie van Financiën
Betaalinstellingen	Mastercard
Betaalinstellingen	Visa
Betaalinstellingen	Mollie
Brancheverenigingen	Detailhandel NL / MKB NL
Brancheverenigingen	PSD2SIG
Brancheverenigingen	BVN (Betaalvereniging Nederland)
Brancheverenigingen	VBIN
Brancheverenigingen	VGI (Verenigde Groot Incassanten)
Buitengerechtelijke geschillenbeslechter	Kifid
Consultants	Connective Payments
Consultants	Innopay
Consultants	Enigma
Consultants	Payment Advisory Group
Consumentenorganisatie	Consumentenbond
Consumentenorganisatie	Iederin
Consumentenorganisatie	Nibud
Consumentenorganisatie	Ouderenbond
Consumentenorganisatie	ANBO
Consumentenorganisatie	KBO-PCOB
Consumentenorganisatie	Privacy first
PSD2-vergunninghouder AISP	Buddy Payment B.V.
PSD2-vergunninghouder AISP	Ingenico
PSD2-vergunninghouder AISP	Invers B.V.
PSD2-vergunninghouder AISP	MoneyMonk B.V.
PSD2-vergunninghouder AISP	Plaid B.V.
PSD2-vergunninghouder AISP	Ockto
PSD2-vergunninghouder AISP & PISP	Twinfield
PSD2-vergunninghouder AISP & PISP	Buckaroo B.V.

PSD2-vergunninghouder AISP & PISP	Exact Payment Services B.V.
PSD2-vergunninghouder AISP & PISP	Flow Money Automation B.V. (Flow your money)
PSD2-vergunninghouder AISP & PISP	Online Payment Platform B.V.
PSD2-vergunninghouder AISP & PISP	Exact
Retail	Thuiswinkel.nl
Retail	NSO Sigaretten/gemakswinkels
Retail	VNO/MKB
Retail	Just Eat Takeway (thuisbezorgd)
Toezichthouder	ACM
Toezichthouder	AFM
Toezichthouder	AP
Toezichthouder	DNB
Wetenschap	Dr. I. Graef, Associate Professor of Competition Law, Tilburg University
Wetenschap	Prof. mr. E.M.L. Moerel, Professor of Global ICT Law, Tilburg University
Wetenschap	Prof. dr. W. Bolt, Professor of payment systems, VU Amsterdam

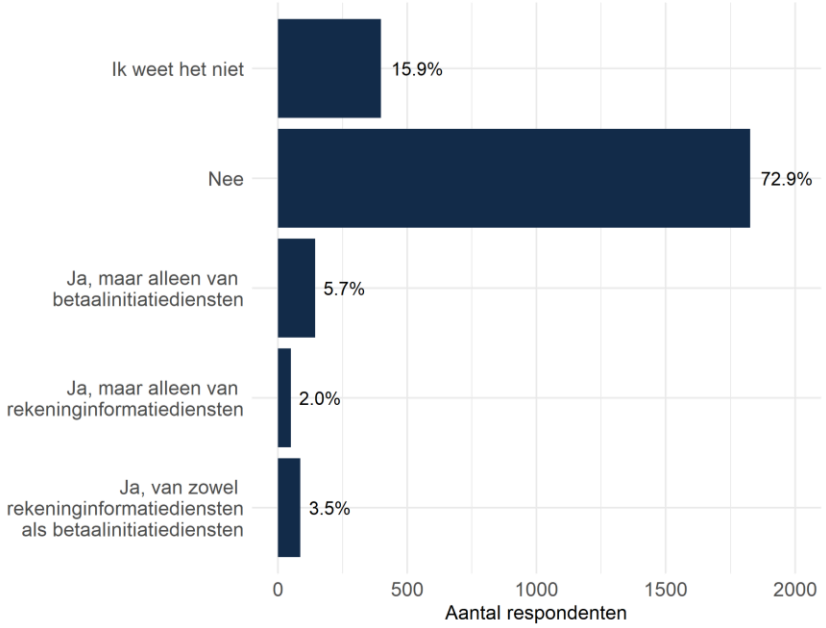
Bijlage C Consumentenenquête

Vraag 1 Wist u voor u deze vragenlijst invulde wat PSD2 was?



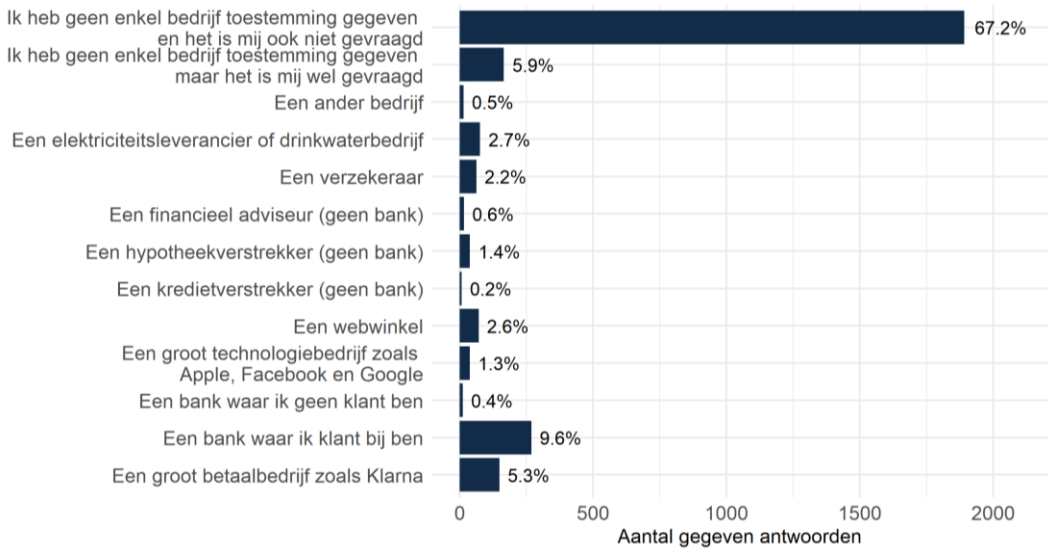
Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2508

Vraag 1ex Hebt u wel eens gebruikgemaakt van rekeninginformatiediensten of betaalinitiatiediensten?



Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2506

Vraag 2 Welke van de onderstaande bedrijven hebt u de afgelopen twee jaar toestemming gegeven om de betaalgegevens van uw betaalrekening te gebruiken voor het aanbieden van rekeninginformatiediensten?

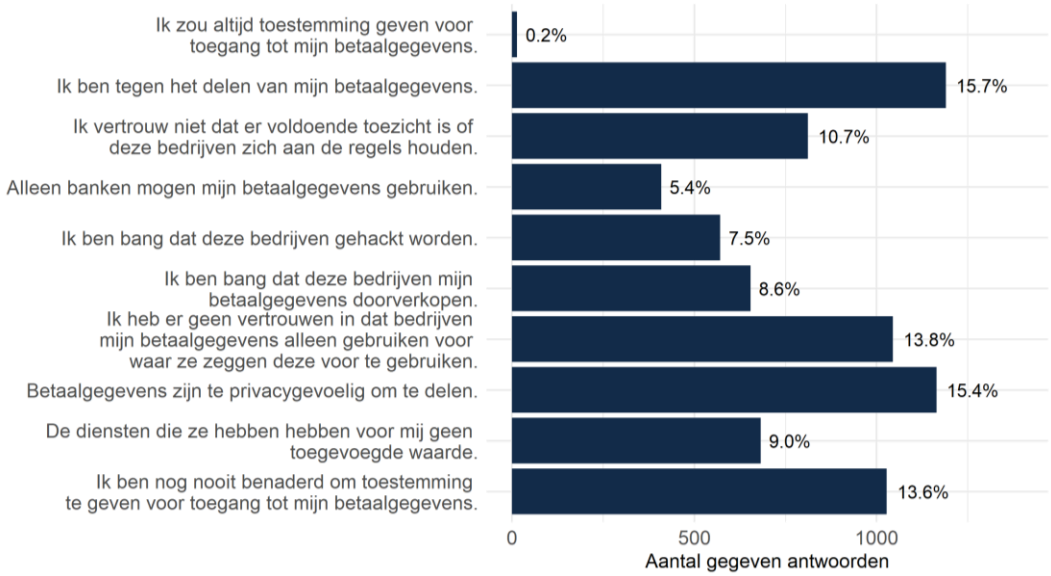


Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2505. Bij deze vraag konden respondenten meerdere antwoorden geven. Het percentage geeft daarom het aandeel antwoorden ten opzichte van het totaal aantal gegeven antwoorden (k = 2815) weer.

Vraag 3 Welke van de onderstaande bedrijven hebt u de afgelopen twee jaar toestemming gegeven voor betaalinitiatiediensten om online betalingen voor u te doen door toegang tot uw betaalrekening te geven?

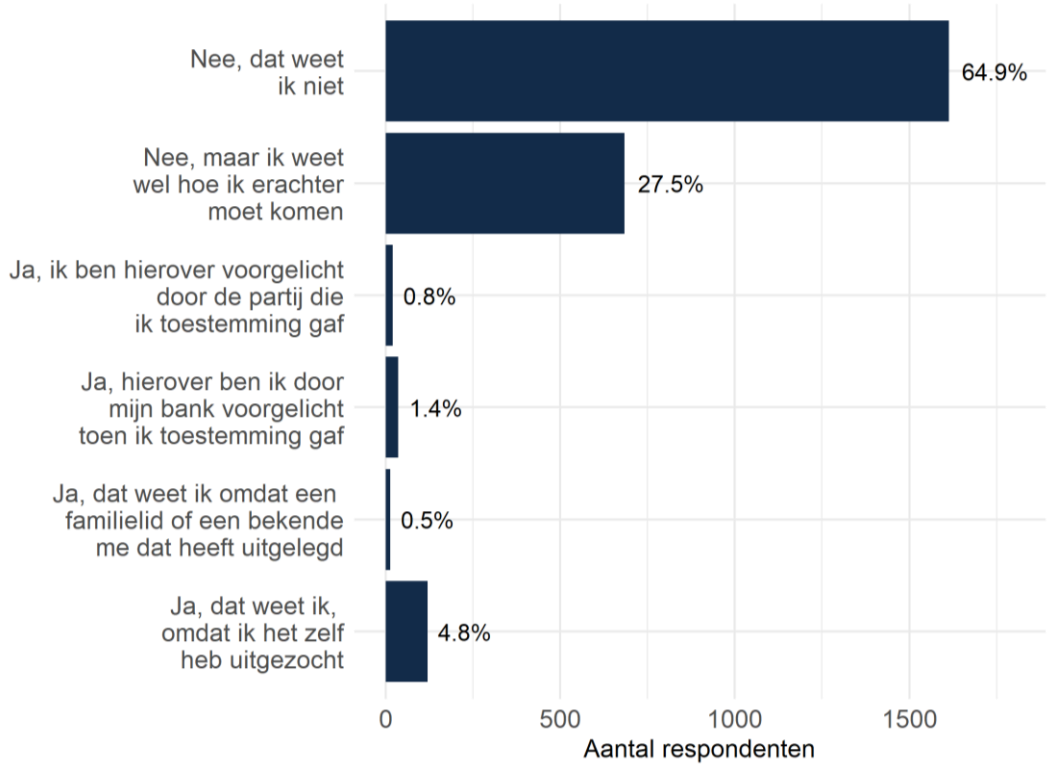
Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2498. Bij deze vraag konden respondenten meerdere antwoorden geven. Het percentage geeft daarom het aandeel antwoorden ten opzichte van het totaal aantal gegeven antwoorden (k = 2900) weer.

Vraag 5 Wat zijn voor u de belangrijkste redenen om bedrijven geen toestemming te geven voor toegang tot uw betaalgegevens voor betaalinitiatiediensten of rekeninginformatiediensten?



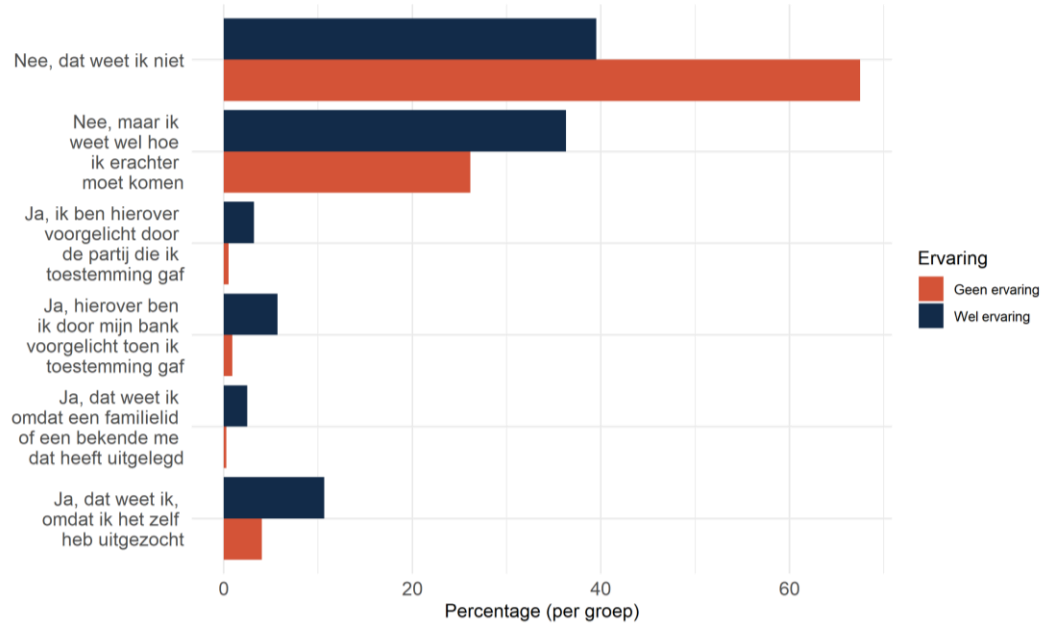
Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2486. Bij deze vraag konden respondenten meerdere antwoorden geven. Het percentage geeft daarom het aandeel antwoorden ten opzichte van het totaal aantal gegeven antwoorden (k = 7568) weer.

Vraag 6 Weet u hoe u toestemming voor toegang tot uw betaalgegevens voor rekeninginformatiediensten kunt intrekken?



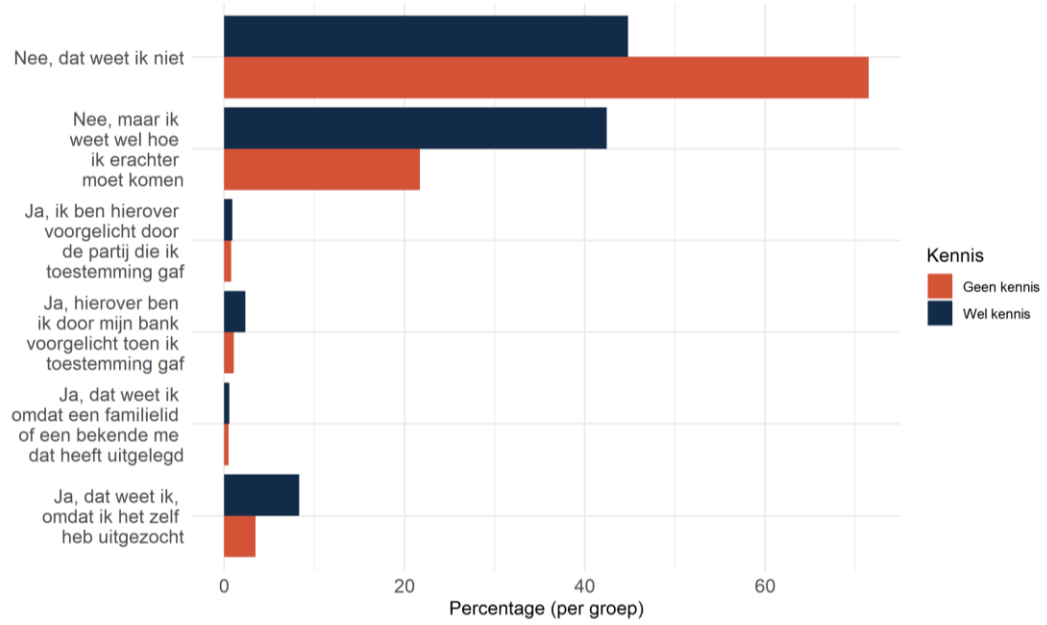
Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2486.

Vraag 6 Weet u hoe u toestemming voor toegang tot uw betaalgegevens voor rekeninginformatiediensten kunt intrekken? (uitgesplitst naar ervaring met PSD2)



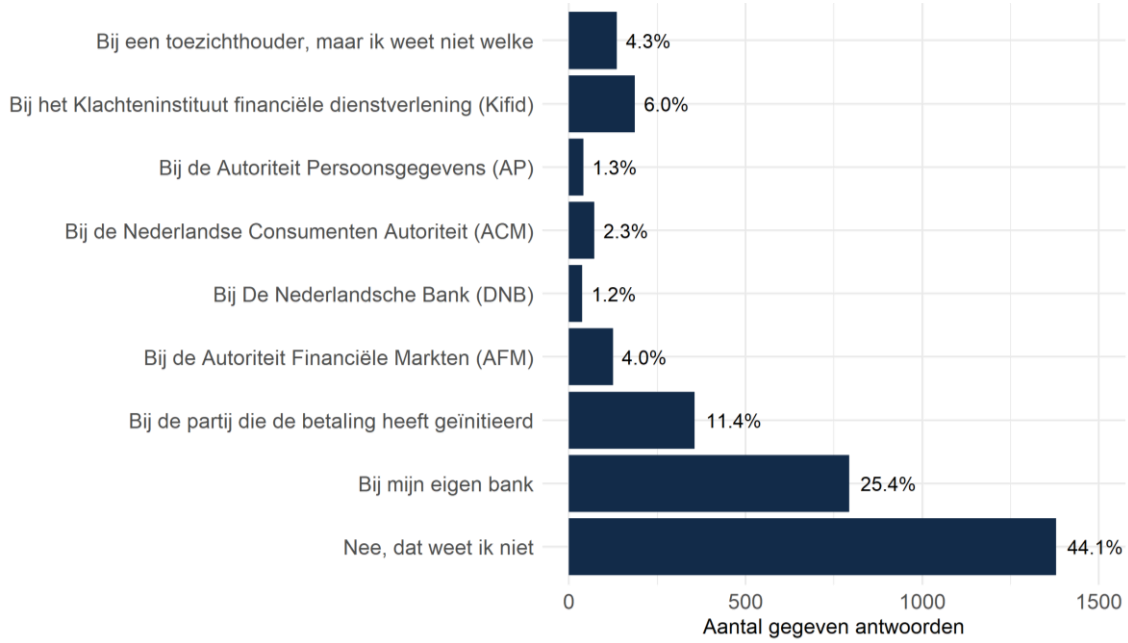
Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2486.

Vraag 6 Weet u hoe u toestemming voor toegang tot uw betaalgegevens voor rekeninginformatiediensten kunt intrekken? (uitgesplitst naar kennis over PSD2)



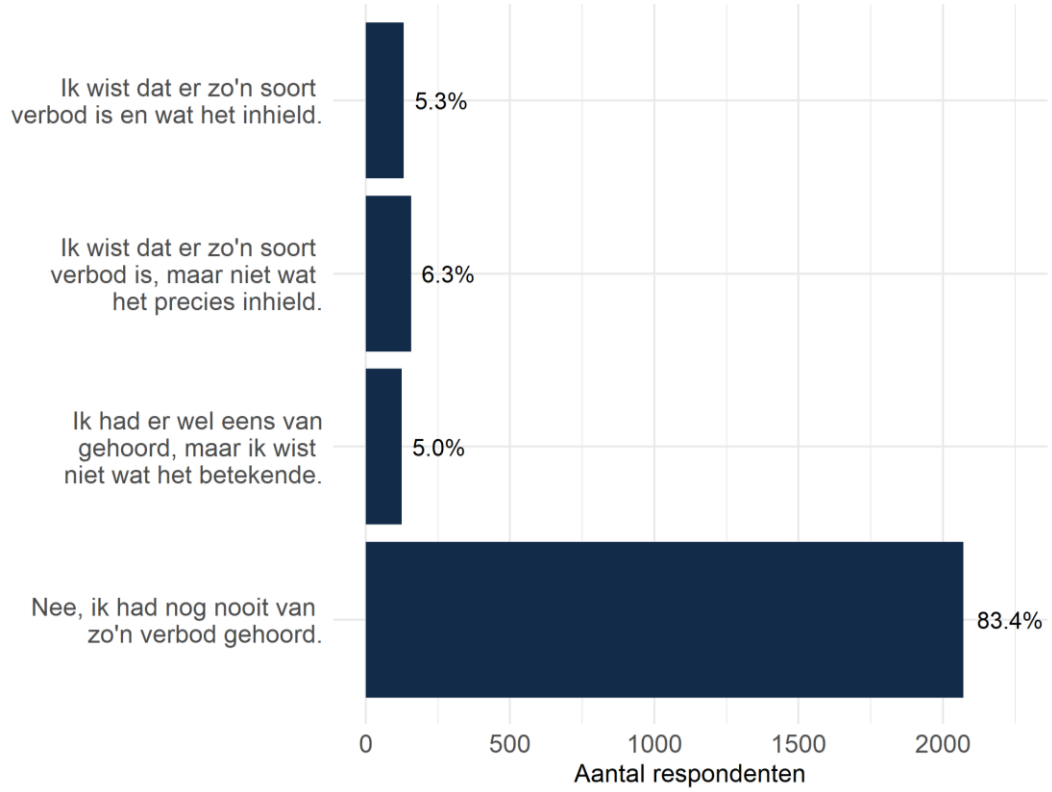
Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2486.

Vraag 7 Als een betaling door een andere partij dan uw bank is uitgevoerd en u hebt hier een klacht over, weet u dan waar u terechtkunt?



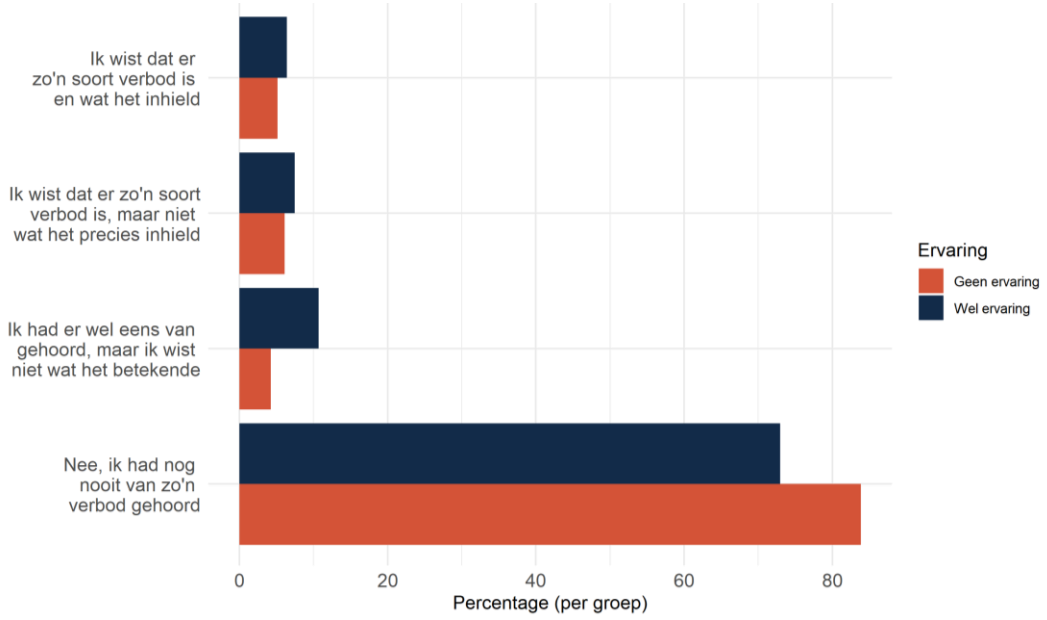
Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2485. Bij deze vraag konden respondenten meerdere antwoorden geven. Het percentage geeft daarom het aandeel antwoorden ten opzichte van het totaal aantal gegeven antwoorden (k = 3128) weer.

Vraag 8 Wist u voor u deze vragenlijst invulde dat er een verbod op surcharging bestond?



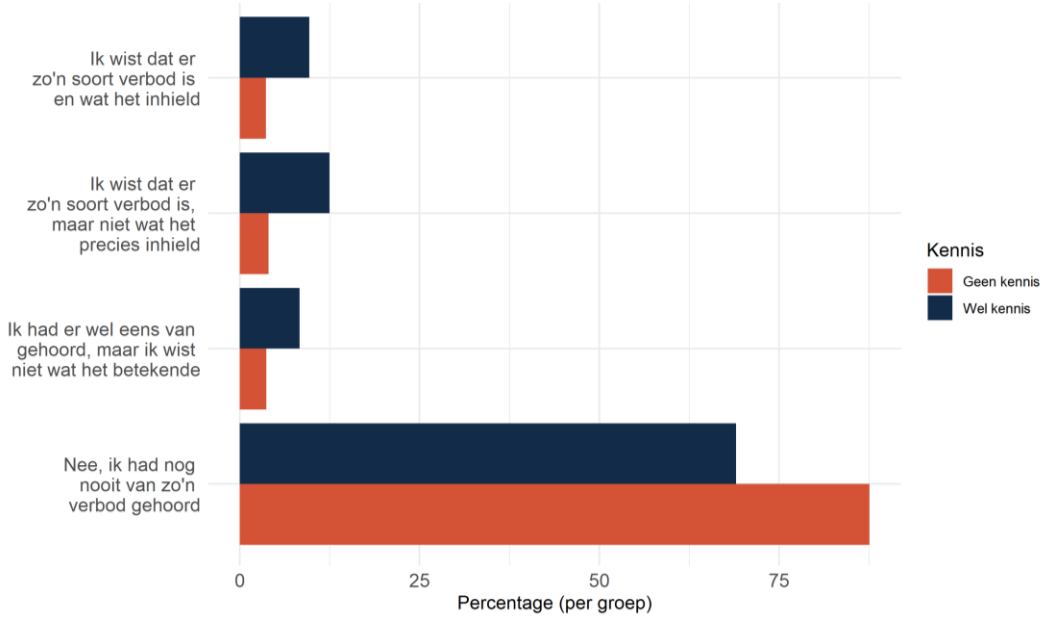
Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2484.

Vraag 8 Wist u voor u deze vragenlijst invulde dat er een verbod op surcharging bestond? (uitgesplitst naar ervaring met PSD2)



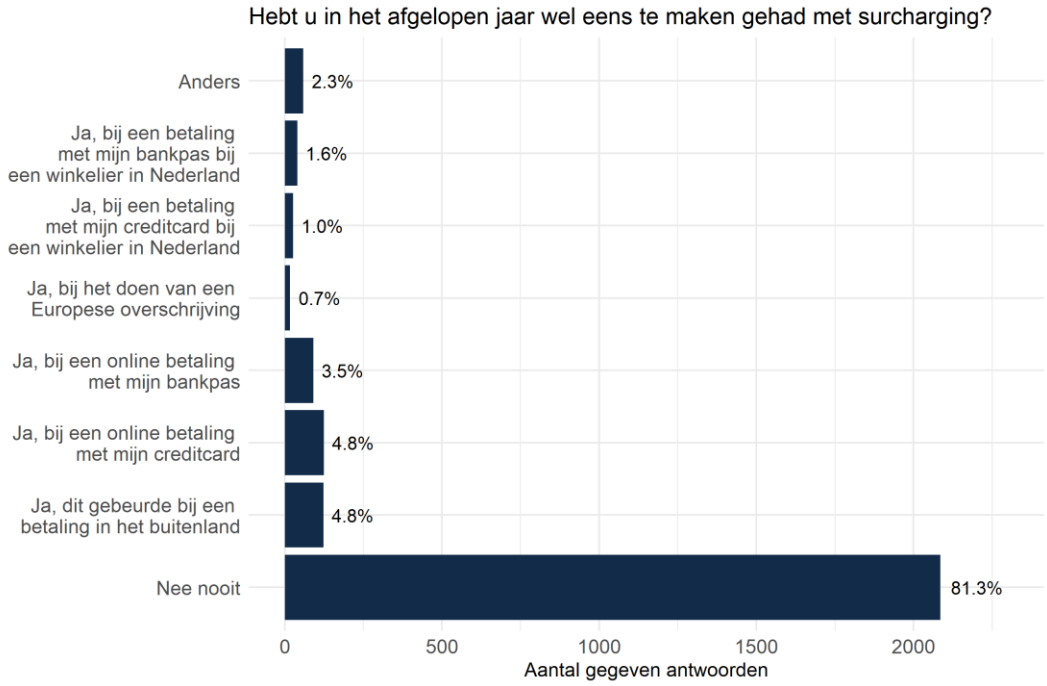
Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2484

Vraag 8 Wist u voor u deze vragenlijst invulde dat er een verbod op surcharging bestond? (uitgesplitst naar kennis over PSD2)



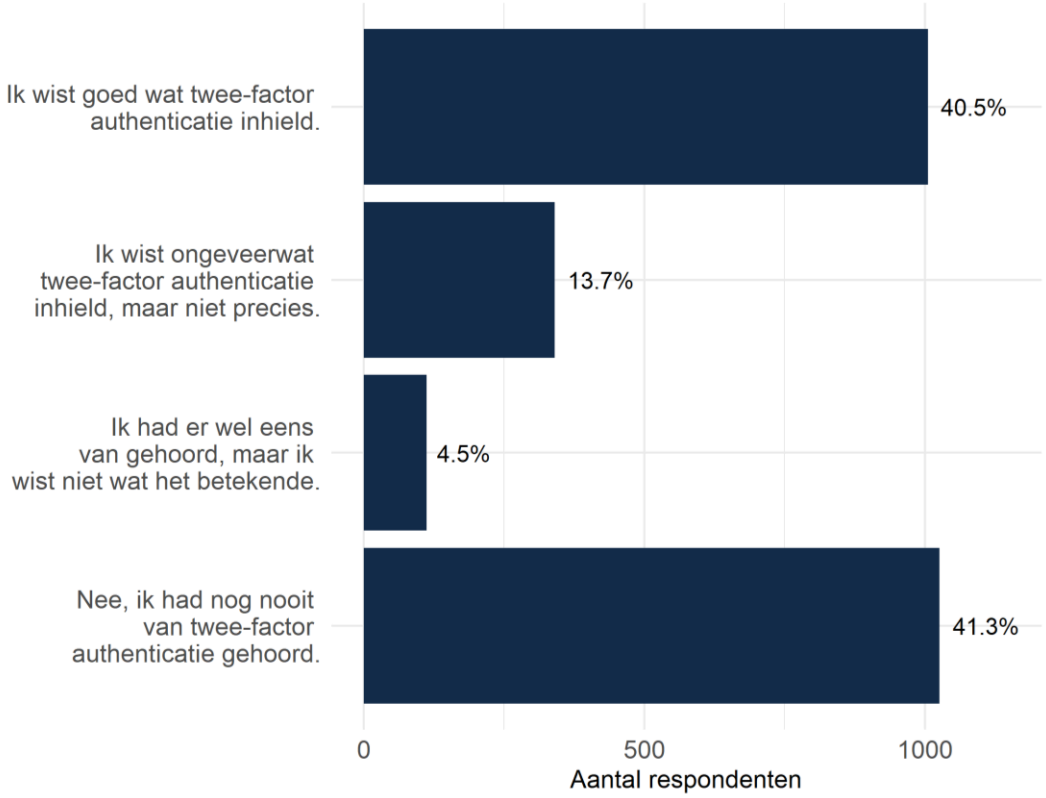
Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2484

Vraag 9 Hebt u in het afgelopen jaar wel eens te maken gehad met surcharging?



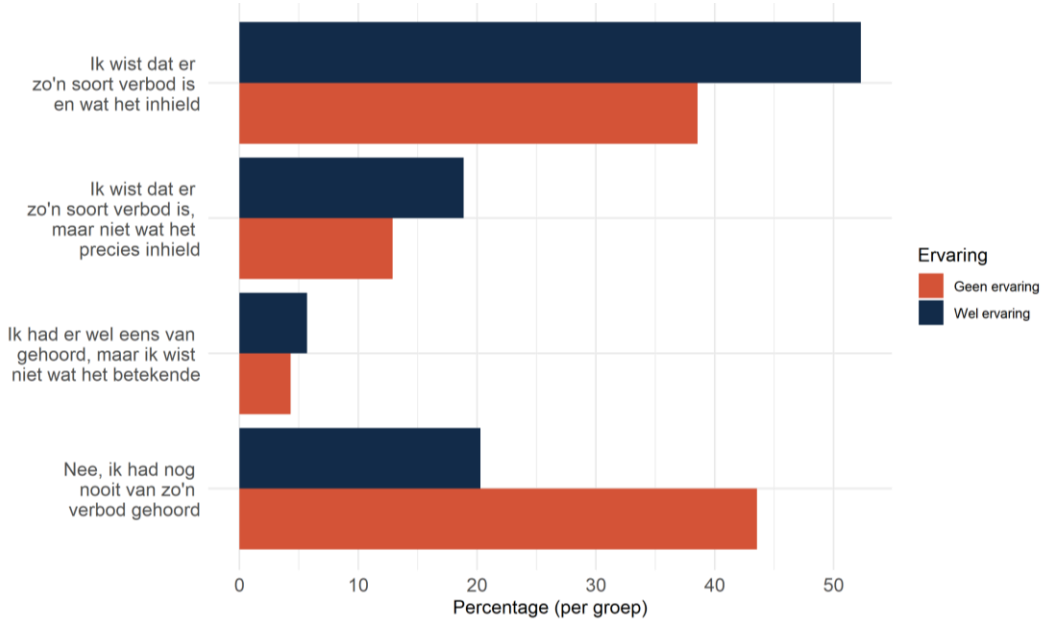
Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2484. Bij deze vraag konden respondenten meerdere antwoorden geven. Het percentage geeft daarom het aandeel antwoorden ten opzichte van het totaal aantal gegeven antwoorden (k = 2566) weer.

Vraag 10 Wist u voor u deze vragenlijst invulde wat twee-factor authenticatie inhield?



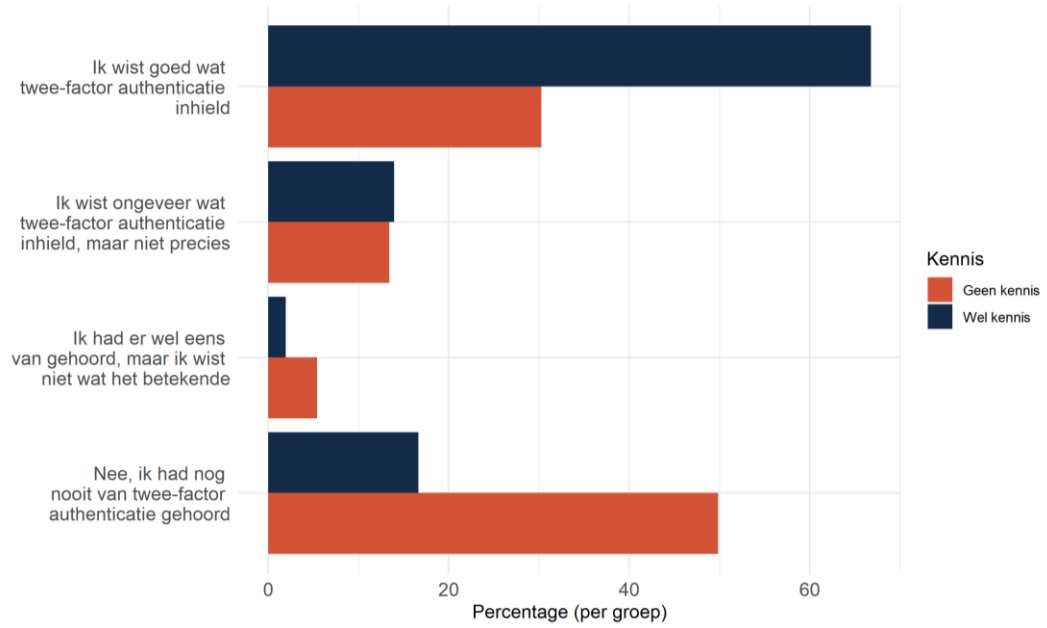
Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2483.

Vraag 10 Wist u voor u deze vragenlijst invulde wat twee-factor authenticatie inhield? (Uitgesplitst naar ervaring met PSD2)



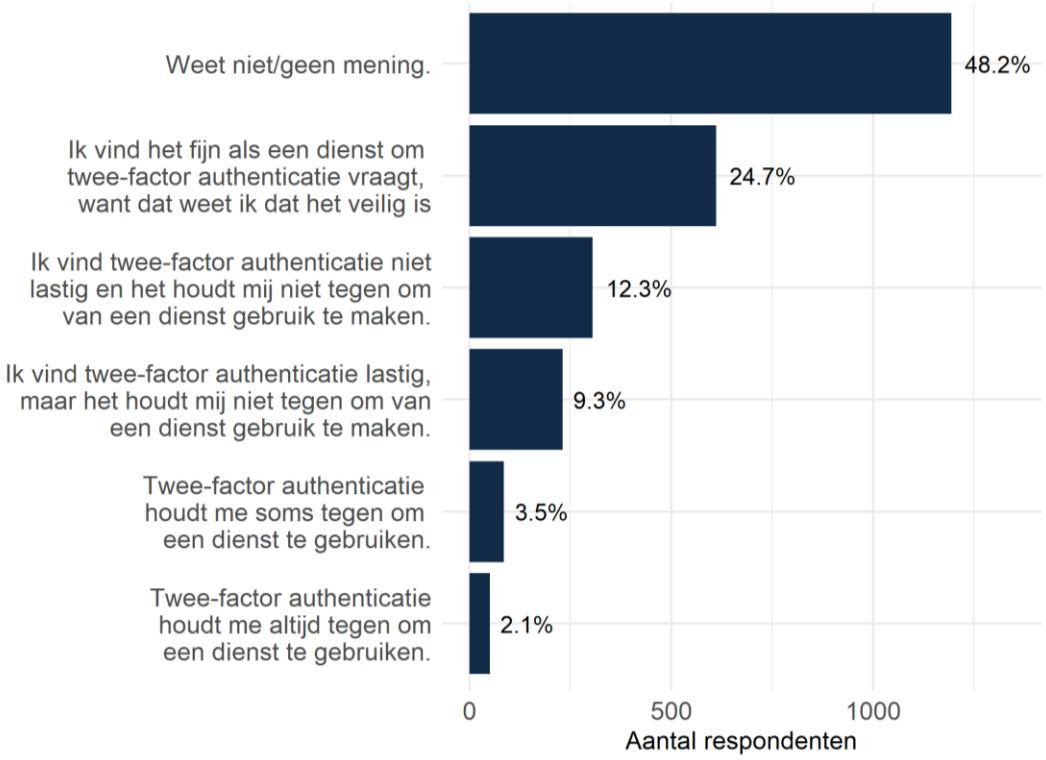
Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2483.

Vraag 10 Wist u voor u deze vragenlijst invulde wat twee-factor authenticatie inhield? (Uitgesplitst naar kennis over PSD2)



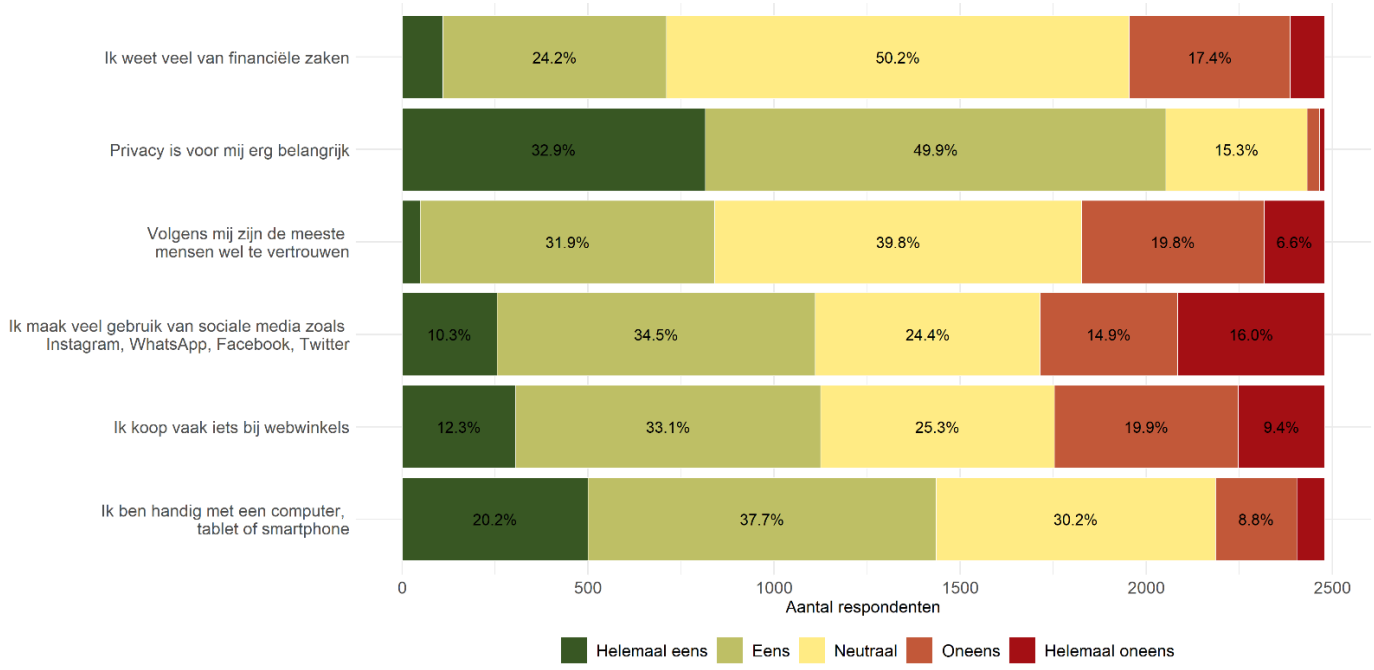
Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2483

Vraag 11 Wat is uw ervaring met twee-factor authenticatie als u wilt betalen voor een aankoop of dienst?



Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2481

Vraag 12 In welke mate zijn de volgende uitspraken op u van toepassing?



Bron: SEO Economisch Onderzoek (2021), o.b.v. consumentenenquête, n = 2480

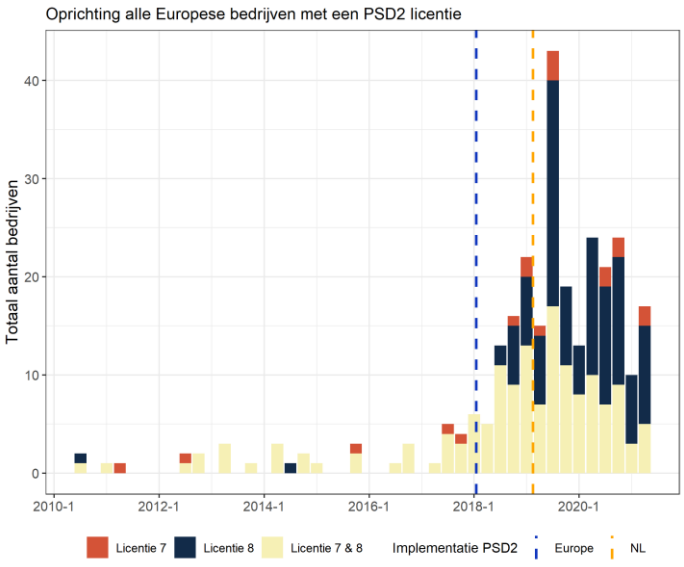
Bijlage D Overzicht partijen met 7 en 8 vergunningen

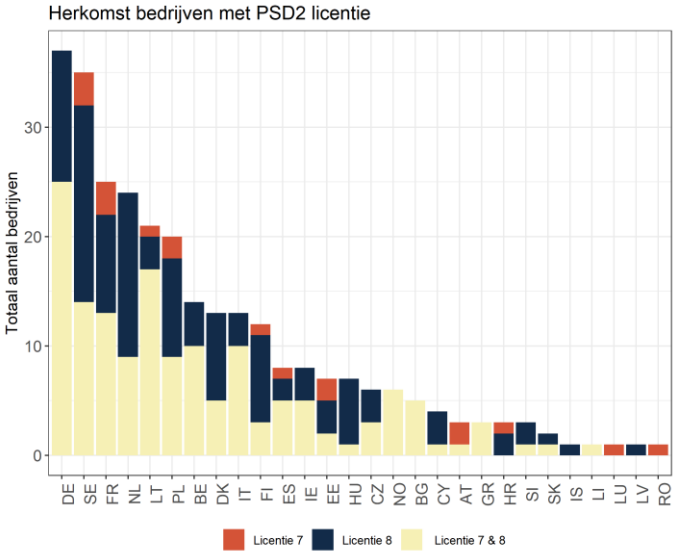
Bedrijfsnaam	Datum opgericht	Diensten	Bedrijven of Consumenten	Korte beschrijving
12Budget B.V. (Knip)	2020-06-30	8	B2C	Financieel advies
Bizcuit Payments B.V.	2019-11-16	7, 8	B2B	Zakelijke betalingsoplossingen (factuurering, betaling van facturen), geïntegreerd met de betaalrekening van de klant (vanaf LinkedIn)
Buckaroo B.V.	2019-02-19	1, 3A, 3B, 3C, 5A, 5B, 7, 8	B2B	Ruime keuze aan betaalmethoden, oplossingen voor kredietbeheer, ondersteuning van bedrijfsmodellen op basis van abonnementen, marktplaatsen voor gesplitste betalingen, slimme kassa's
Buddy Payment B.V.	2020-03-13	8	B2C	Budgetbeheer en schuldpreventie app voor particulieren
Ceron IT Solutions B.V.	2020-12-01	8		Licentie ingetrokken
Dyme B.V.	2019-10-01	8	B2C	Budget- en abonnementenbeheer
Exact Payment Services B.V.	2020-04-16	7, 8	B2B	Diverse oplossingen voor bedrijfsbeheer; HR, klantrelaties, projectbeheer, automatisering van productieprocessen, verkoop, financiën
Financial Transaction Services B.V.	2019-07-05	7, 8	B2B	FX-producten, intercompany bankieren (leningadministratie, netting), liquiditeitsvoorspelling, multibank pooling
FinMaster B.V.	2021-05-28	8	B2B	Boekhoudsoftware, facturering
Floryn B.V.	2019-12-18	8	B2B	Flexibel krediet voor bedrijven
Flow Money Automation B.V.	2020-07-14	7, 8	B2C	Geldbeheer/budgettering app
iban-XS B.V.	2021-03-17	7, 8	B2B	Enkelvoudige en meervoudige SEPA-overboekingen, uitgestelde en terugkerende SEPA-overboekingen, grensoverschrijdende overboekingen naar niet-SEPA-landen
Invers B.V.	2019-08-21	8	B2B	Bankgegevens aggregatie, financiële analyse
Jortt B.V.	2020-05-19	8	B2B	"Ondernemersgerichte boekhouding"; boekhoudsoftware, analytics
Lendex Nederland B.V.	2020-11-28	8	B2C	Consumentenkrediet met snelle evaluatie
MoneyMonk B.V.	2019-07-31	8	B2B	Ecosysteem voor boekhouding en bedrijfsbeheer voor freelancers

Ockto B.V.	2020-06-23	8	B2B, B2C	App waarmee financiële gegevens van consumenten eenvoudig kunnen worden gedeeld met banken, verhuurders, etc. Ockto biedt ook diensten voor het opvragen van gegevens op initiatief van het bedrijf, in plaats van de consument (met toestemming van de consument)
Online Payment Platform B.V.	2019-02-19	3A, 3B, 3C, 5A, 5B, 7, 8	B2B	Multi-split betalingssystemen, geschillenafhandeling, escrow-betaling, analytics
Peaks B.V.	2019-06-04	7, 8	B2C	Biedt beleggingsdiensten aan, vergelijkbaar met Etoro, Trading 212, enz. De investering is meer gestructureerd dan bij de handelsplatformen: Peaks biedt een keuze uit vier portefeuilles met verschillende risico-rendementsprofielen
Plaid, B.V.	2021-03-17	8	B2B	API-leverancier voor banken
SkillSource B.V.	2020-07-14	8	B2B	Software voor automatisering van bedrijfsprocessen (zowel online als offline)
Tellow B.V.	2020-05-07	8	B2B	Boekhoud- en bedrijfsbeheerecosysteem voor freelancers
Tintel B.V.	2019-02-19	3A, 3B, 3C, 5A, 5B, 7, 8	B2B	Betalingsprocesdiensten; hun aanbod omvat dynamische betaallinks, responsieve betalingsmenu's, tweedekans e-mails, en toelating voor meerdere valuta's (EUR, USD, GBP, JPY)
Twinfield International N.V.	2019-10-18	8	B2B	Bedrijfsadministratie en boekhouding

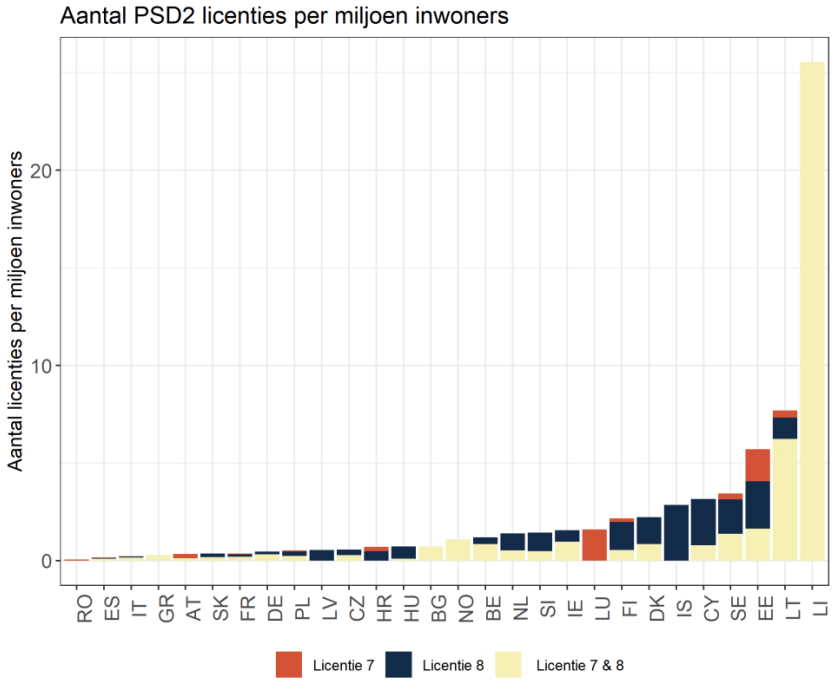
Bijlage E Overzicht data EBA-register

Bijlage E.1 Overzicht alle landen



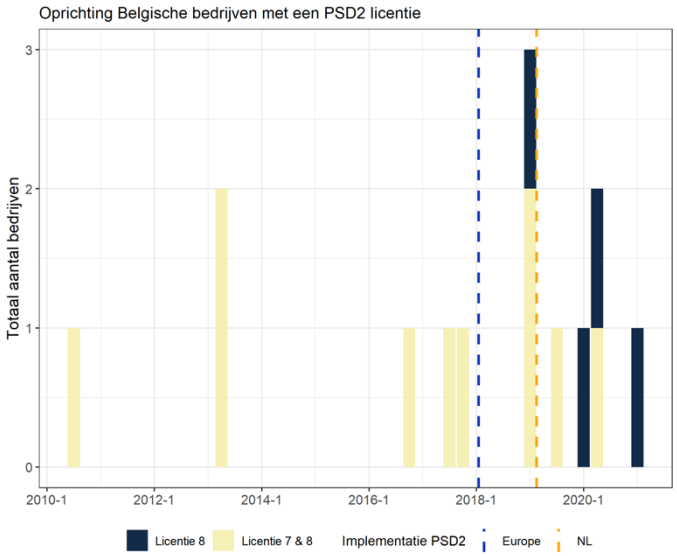


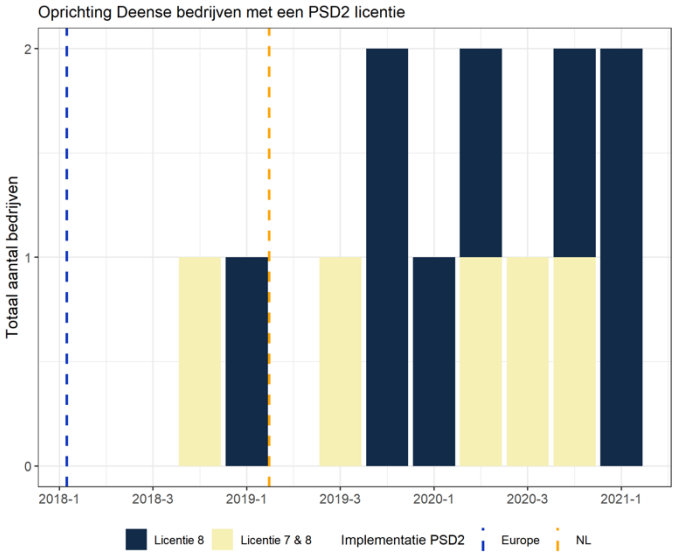
Bron: EBA (2021), o.b.v. analyse EBA register



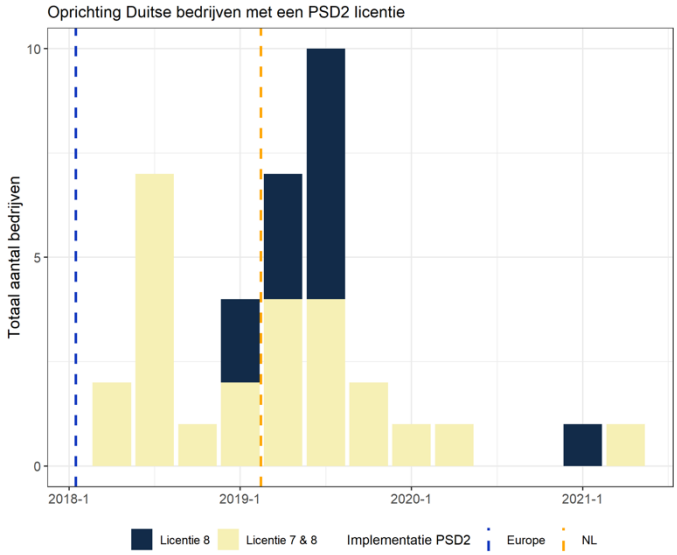
Bron: EBA (2021), o.b.v. analyse EBA register e

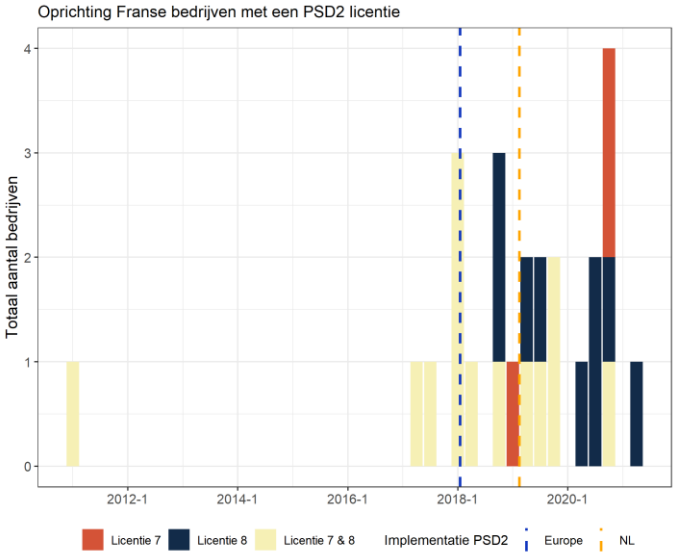
Bijlage E.2 Overzicht oprichting partijen actief in eigen markt



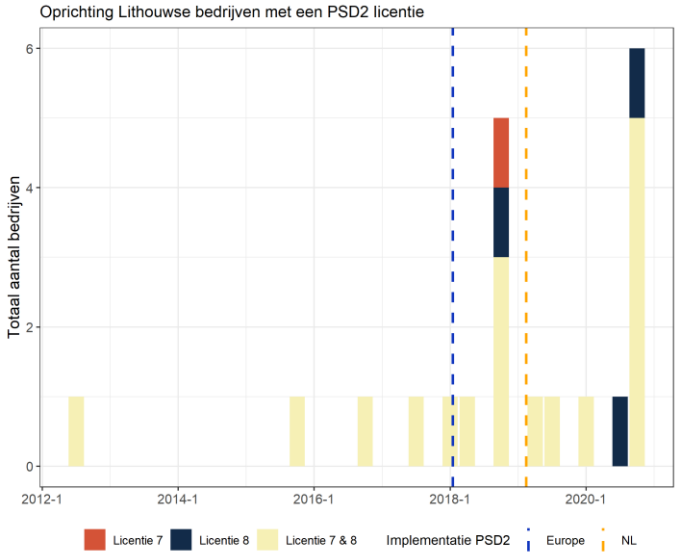


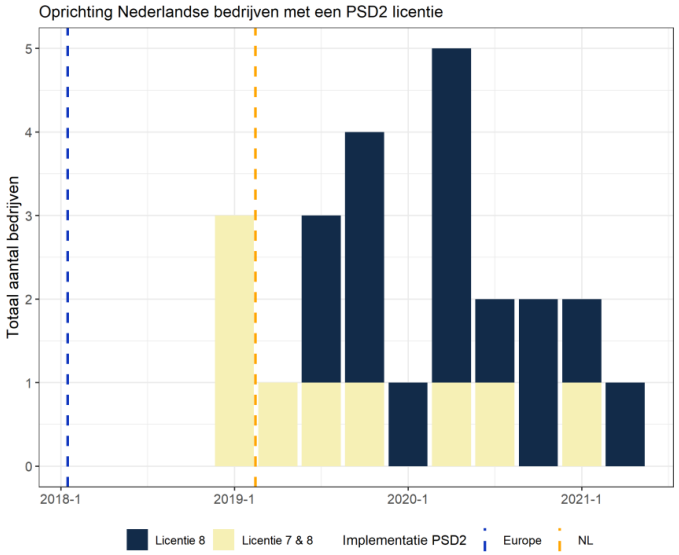
Bron: EBA (2021), o.b.v. analyse EBA register



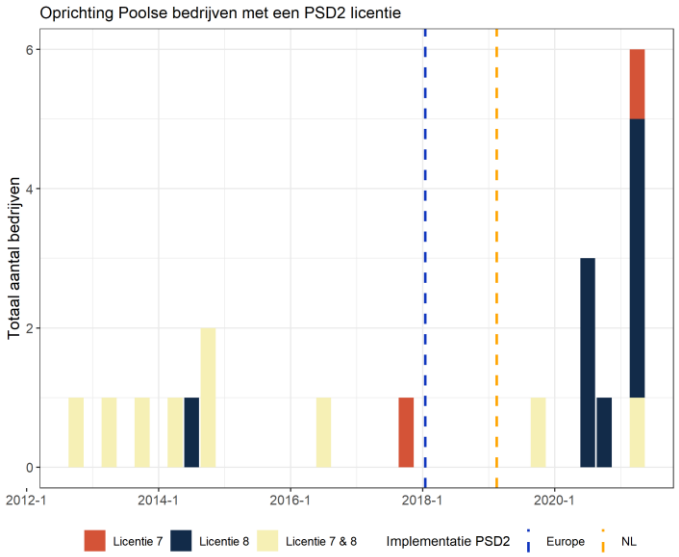


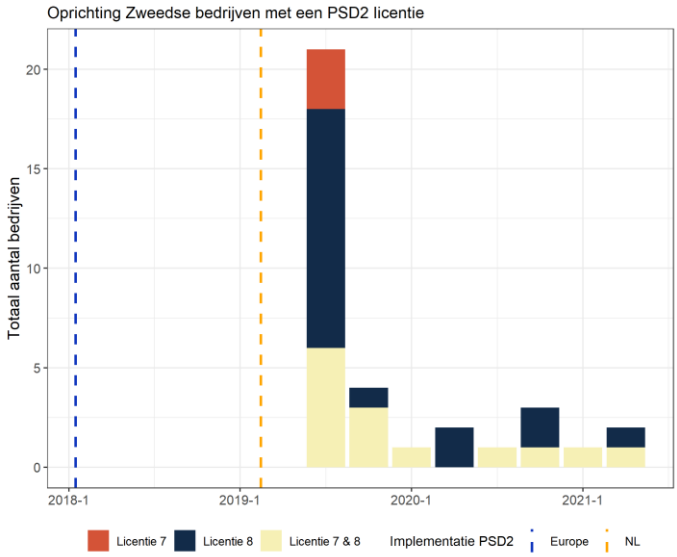
Bron: EBA (2021), o.b.v. analyse EBA-register





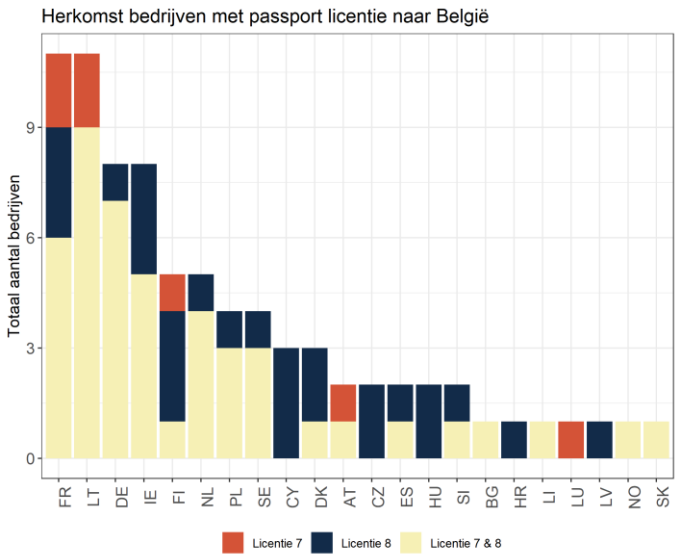
Bron: EBA (2021), o.b.v. analyse EBA-register

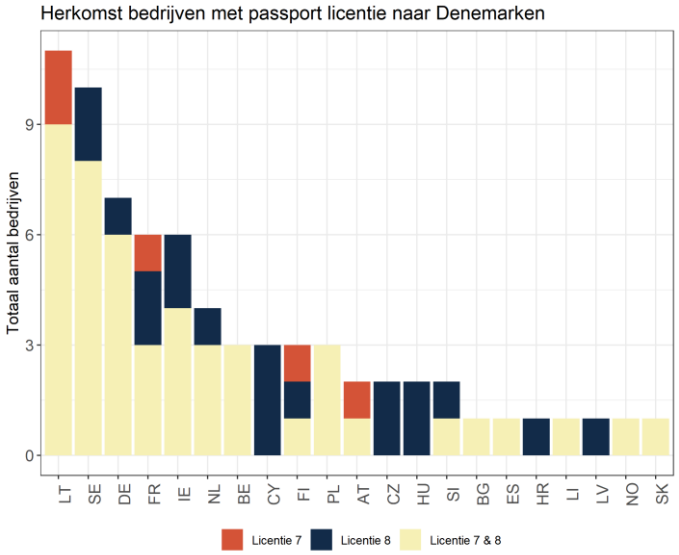




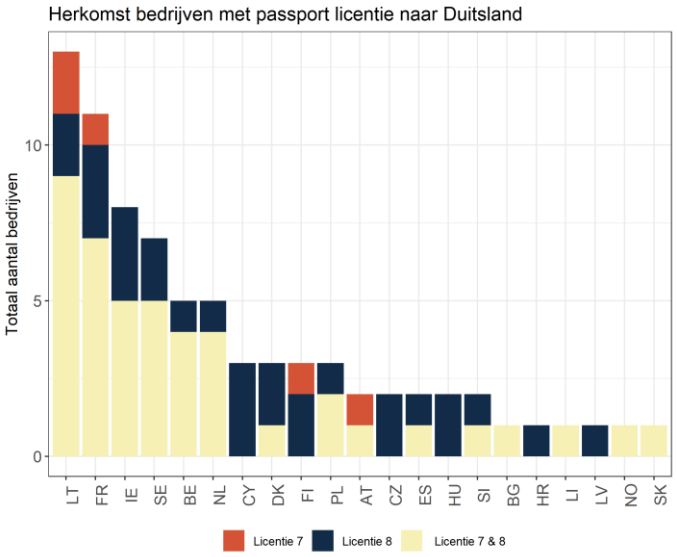
Bron: EBA (2021), o.b.v. analyse EBA-register

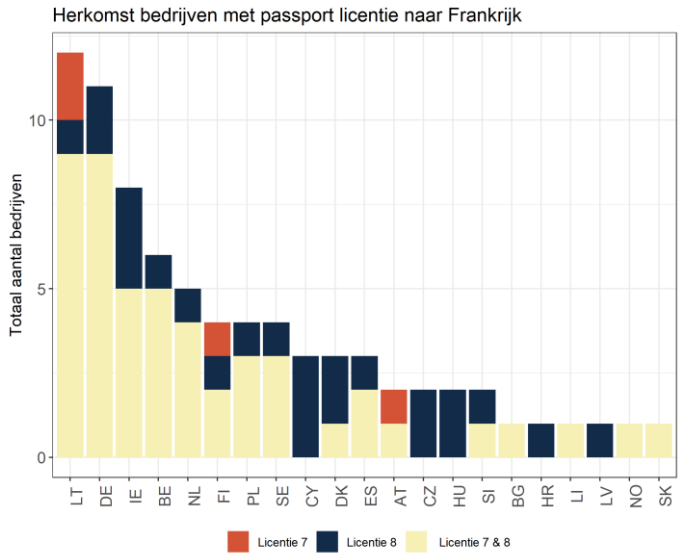
Bijlage E.3 Herkomst bedrijven met passport licentie



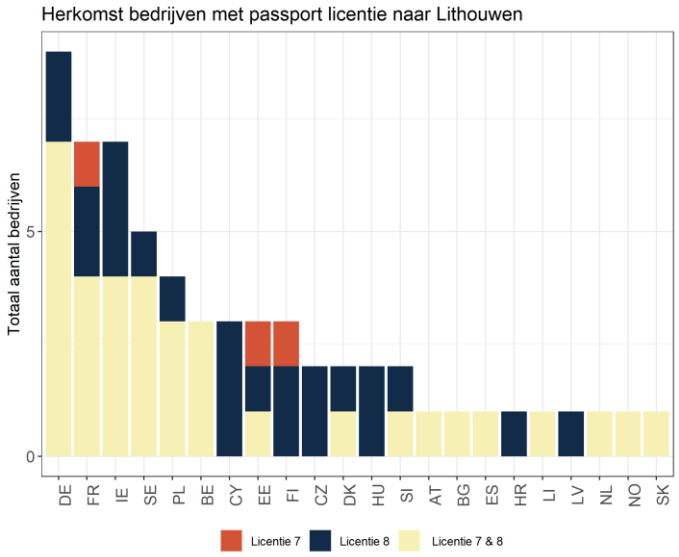


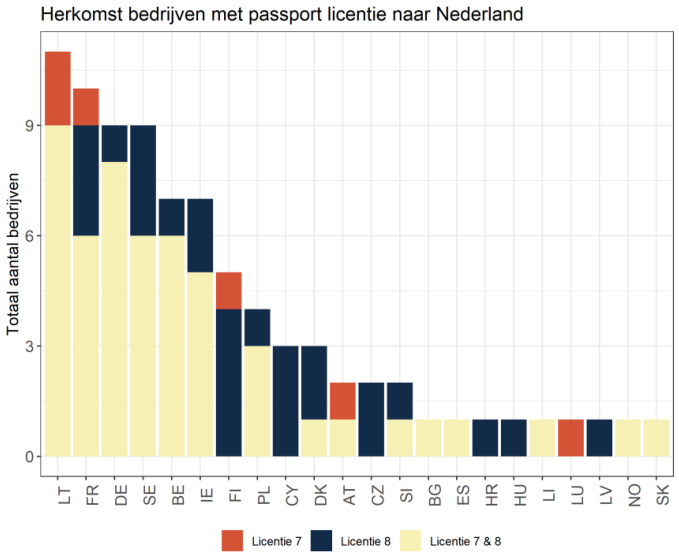
Bron: EBA (2021), o.b.v. analyse EBA-register



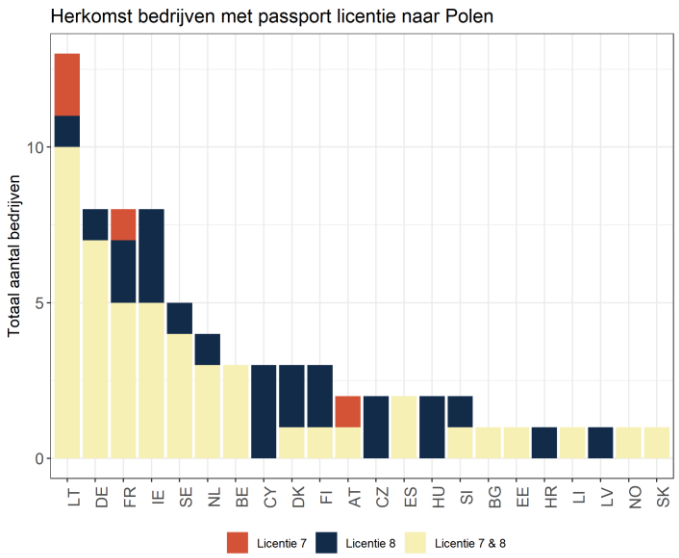


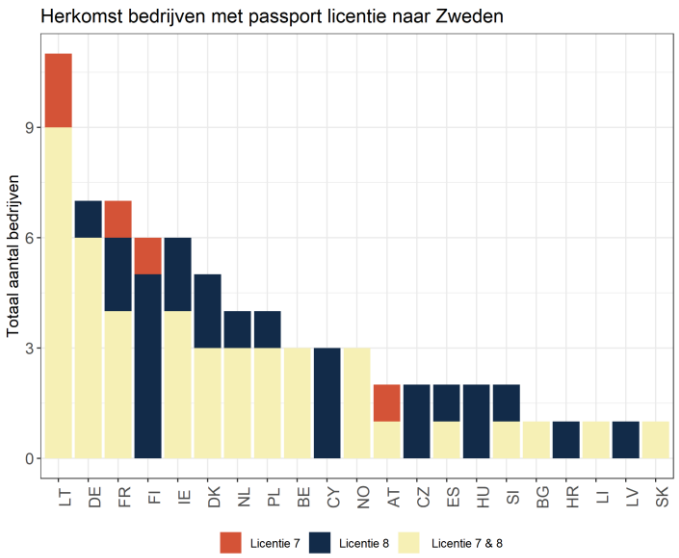
Bron: EBA (2021), o.b.v. analyse EBA-register





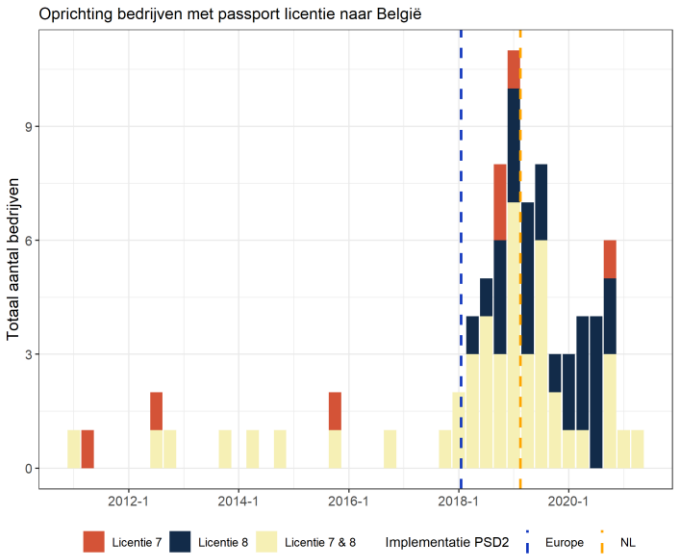
Bron: EBA (2021), o.b.v. analyse EBA-register

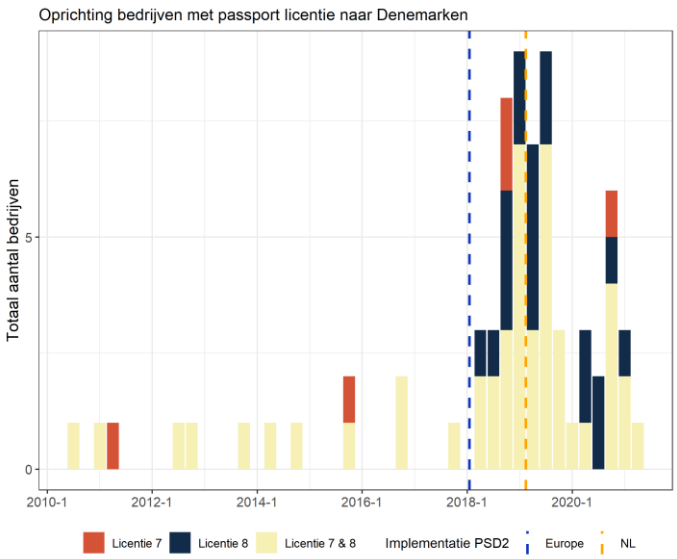




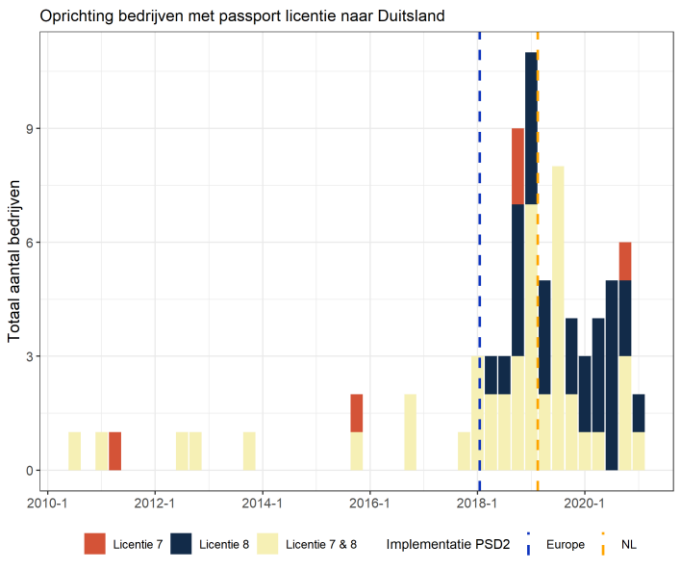
Bron: EBA (2021), o.b.v. analyse EBA-register

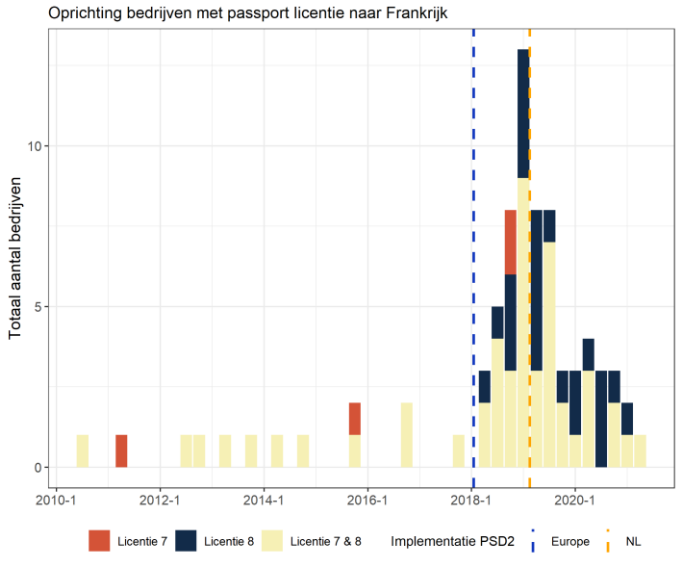
Bijlage E.4 Oprichting bedrijven met passport licentie



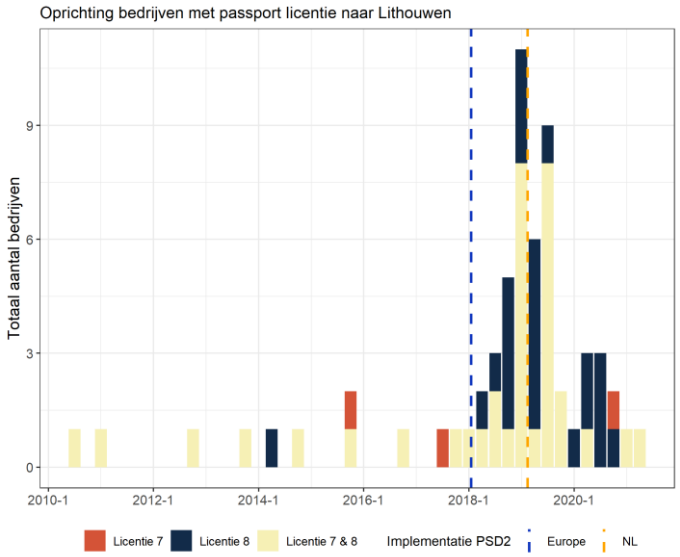


Bron: EBA (2021), o.b.v. analyse EBA-register

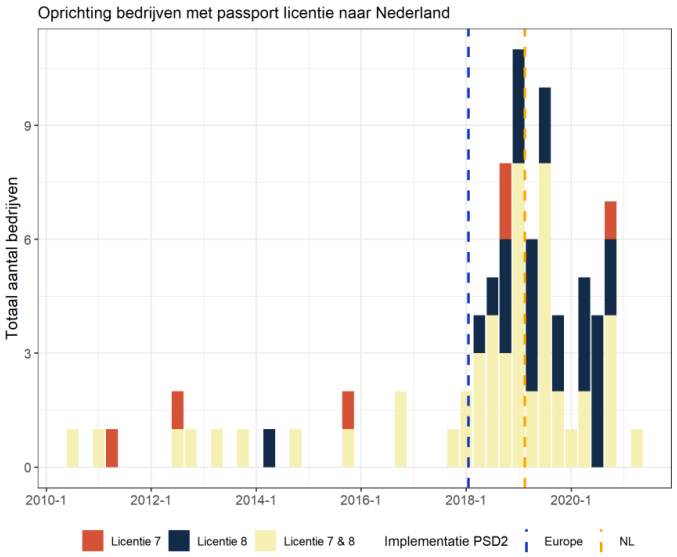




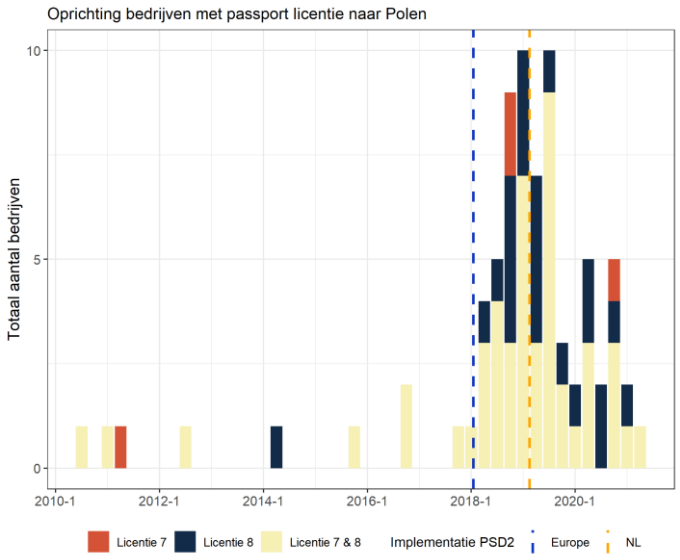
Bron: EBA (2021), o.b.v. analyse EBA-register

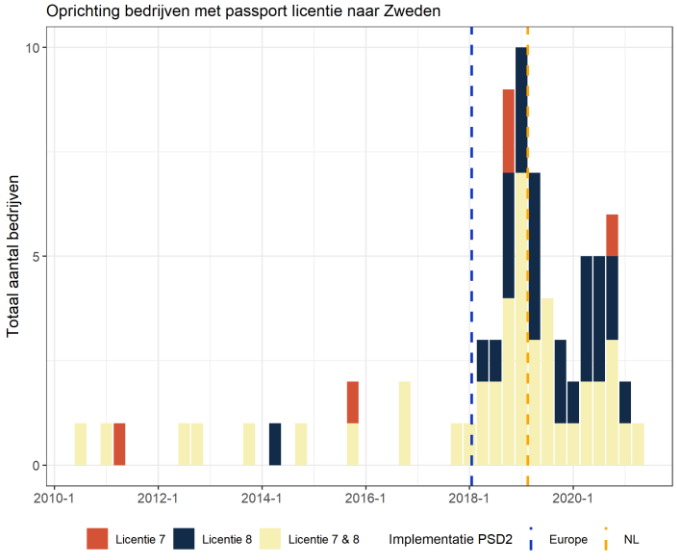


**



Bron: EBA (2021), o.b.v. analyse EBA-register





Bron: EBA (2021), o.b.v. analyse EBA-register

Bijlage F Tijdlijn

Datum	Gebeurtenis
24-07-2013	De Europese Commissie komt met het voorstel om PSD1 te vervangen voor PSD2.
08-10-2015	Het Europese Parlement neemt het voorstel om PSD1 te vervangen voor PSD2 aan van de Europese Commissie.
17-11-2015	De Europese Raad neemt het voorstel om PSD1 te vervangen voor PSD2 aan van de Europese Commissie.
08-12-2015	De EBA publiceert een discussie paper over SCA en de consultatie op de RTS conceptversie. Hierin nodigt zij uit om feedback te geven. Daarnaast legt ze de eerste ideeën en interpretaties van het EBA-mandaat uit.
11-12-2015	De EBA publiceert een consultatie paper over het ontwerp van de RTS betreffende het kader voor samenwerking en informatie-uitwisseling tussen bevoegde autoriteiten voor paspoortkennisgevingen, in het kader van PSD2.
23-12-2015	De richtlijn PSD2 werd gepubliceerd in het officiële tijdschrift van de EU.
12-01-2016	De richtlijn PSD2 is opgesteld. EU-lidstaten akkoord gingen om PSD2 om te schrijven naar nationale wetgeving voor 13 januari 2018. Uiteindelijk trad in Nederland de PSD2 pas op 13 februari 2019 in werking (dit komt verderop ook ter sprake. NB: op voorhand was hierover geen afspraak met de Europese Commissie).
12-08-2016	De EBA publiceert een consultatie paper over het ontwerp van de RTS waarin de vereisten van SCA en CSC onder PSD2 worden gespecifieerd.
12-10-2016	Einde van consultatie op de ontwerpversie RTS (SCA en CSC). De EBA ontving in totaal 224 reacties.
17-11-2016	Internetconsultatie in Nederland gaat van start. Het wetsvoorstel implementatiewet PSD2 en de daarbij behorende memorie van toelichting is gedurende vier weken ter consultatie aangeboden.
15-12-2016	Internetconsultatie in Nederland loopt af. Er zijn 16 reacties ontvangen die verschillende suggesties bevatten. Een aantal zijn in het wetsvoorstel en de toelichting overgenomen. Zo is er een verduidelijking opgenomen omtrent de uitzondering voor handelsagenten.
23-02-2017	De definitieve versie van het ontwerp over de RTS over SCA en CSC is uitgebracht.
13-06-2017	De Berlin Group stelt een raamwerk voor Europese API-specificaties op (NextGenPSD2-specificaties). Het is niet een volledig geharmoniseerde standaard omdat deelnemers eigen keuzes kunnen maken bij de implementatie.
29-06-2017	De EBA reageert op het advies van de Europese Commissie inzake het gedeeltelijk bevestigen en aanpassen van de definitieve conceptversie van de RTS over SCA en CSC.
24-07-2017	De EBA publiceert een consultatie paper over RTS waarin technische voorschriften voor de ontwikkeling, de werking en het onderhoud van het elektronische centrale registeren en de toegang tot de daarin opgenomen informatie staan beschreven. Daarnaast betreft het details en een structuur over de informatie die de bevoegde autoriteiten opnemen in hun openbare registers en doorgeven aan de EBA.
22-08-2017	De AP stuurt een advies voor een wetsvoorstel omtrent privacy toezicht bij PSD2.
01-09-2017	Holland FinTech, AFM, ACM en DNB organiseerde het evenement 'FinTech meets the regulator' in Amsterdam. Dit evenement gaf aan Nederlandse toezichthouders en

	bedrijven actief in de financiële technologie een mogelijkheid om problemen omtrent de PSD2-regulatie te discussiëren.
15-09-2017	De Ministerraad in Nederland gaat akkoord met de implementatiewet PSD2.
03-10-2017	Er is een adviesaanvraag aanhangig bij Raad van State over de implementatiewet PSD2.
04-10-2017	De Raad van State brengt een advies uit omtrent de Implementatiewet PSD2.
23-10-2017	De implementatiewet PSD2 is ingediend bij de Tweede Kamer. Hierna volgt een kamerbrief. Het wetsvoorstel regelt de invoering van PSD2 in Nederlandse wetgeving.
01-12-2017	De vaste commissie voor Financiën brengt een verslag uit over haar bevindingen omtrent de implementatiewet herziene betaalrichtlijnen. Ze menen dat het wetsvoorstel kan bijdragen aan de betrouwbaarheid en veiligheid van financiële transacties. Echter hebben wij nog wel enkele vragen of opmerkingen.
13-12-2017	De EBA publiceert een definitief rapport met het voorstel over RTS waarin technische voorschriften voor de ontwikkeling, de werking en het onderhoud van het elektronische centrale registeren en de toegang tot de daarin opgenomen informatie staan beschreven. Daarnaast betreft het details en een structuur over de informatie die de bevoegde autoriteiten opnemen in hun openbare registers en doorgeven aan de EBA.
20-12-2017	AP stuurt een advies voor een wetsvoorstel omtrent privacy toezicht op PSD2. In de kern concludeert het advies dat in het wetsvoorstel onvoldoende rekenschap is gegeven van de verhouding met de Algemene Verordening Gegevensbescherming (AVG) en de Wet bescherming persoonsgegevens (Wbp). De brief is gericht aan het Ministerie van Financiën.
13-01-2018	Lidstaten kregen tot 13 januari 2018 de tijd om PSD2 in nationaal recht om te zetten. Ook moest de SCA worden ingebouwd. In Nederland is vertraging ontstaan bij de implementatie van de PSD2 in nationale wetgeving.
13-03-2018	De RTS werd als gedelegeerde verordening gepubliceerd in het officiële 'Journal of the European Union'.
Mei-2018	DNB start namens het MOB de PSD2-publiekscampagne onder de slogan 'U beslist'.
13-06-2018	EBA publiceert de 'Opinion on the implementation of the RTS on SCA and CSC'.
22-06-2018	EBA voegt PSD2 toe aan haar online interactieve 'Single Rulebook' en Q&A tool.
19-06-2018	Nota van wijziging implementatiewet PSD2. Voorstel: toezicht op Art 94(2) toe te delen aan de AP.
20-06-2018	Nota n.a.v. verslag implementatiewet in Nederland.
06-07-2018	Implementatiewet aangemeld voor plenaire behandeling Tweede Kamer Nederland.
11-09-2018	Wetsvoorstel aangenomen door Tweede Kamer Nederland.
18-10-2018	De AP heeft met Q&A's voor betaaldienstverleners verduidelijkt waar de 'uitdrukkelijke toestemming' van consumenten aan moet voldoen.
29-10-2018	Voorlopig verslag implementatiewet in Nederland.
13-11-2018	Memorie van antwoord implementatiewet in Nederland.
27-11-2018	(Eindeverslag), aangemeld voor (plenaire) behandeling Nederland.
04-12-2018	De Eerste Kamer Nederland heeft het wetsvoorstel implementatiewet PSD2 als hamerstuk afgedaan. De PvdA, GroenLinks, DENK, 50PLUS, D66, VVD, SGP, CDA, ChristenUnie en FvD waren voor. De PVV, PvdD en SP waren tegen. PVV en PvdD is daarbij aantekening verleend (deze partijen waren tegen, maar waren op het moment van de stemming niet aanwezig).

27-12-2018	Bekendmaking van wetwijzing van de Wet op het financieel toezicht, de Wet bekostiging financieel toezicht, het Burgerlijk Wetboek en de Wet handhaving consumentenbescherming ter implementatie van PSD2.
14-02-2019	ACM publiceert een stuk over de invoering van PSD2. Hier geven ze kort de belangrijkste wijzigingen van PSD2.
18-02-2019	Besluit tot vaststelling van het tijdstip van inwerkingtreding van de Implementatiewet herziene richtlijn betaaldiensten en het Implementatiebesluit herziene richtlijn betaaldiensten.
19-02-2019	PSD2 is in Nederland in werking gestreden. De Nederlandse regels van PSD2 zijn te vinden in de wet, een algemene maatregel van bestuur en in de vrijstellingsregeling.
19-02-2019	ACM publiceert een stuk over wat ACM doet omtrent PSD2. Daarnaast geven ze informatie wat andere toezichthouders doen.
21-02-2019	DNB en de AP sluiten een convenant dat ziet op de samenwerking en informatie-uitwisseling tussen beide toezichthouders toezicht te houden op de PSD2.
11-03-2019	DNB start namens het MOB een voorlichtende publiekscampagne over de PSD2: "PSD2 Bankieren, Nieuwe mogelijkheden, U beslist". De campagne had tot doel mensen bewust te maken van de komst van PSD2 en daarbij de mogelijkheid dat rekeninghouders gevraagd kunnen worden of zij toegang tot hun betaalrekening willen geven.
22-09-2019	Privacy First zet een PSD2-me-niet-register op. Deze krijgt later een gevolg in een PSD2-me-niet filter. Doel hiervan is consumenten de mogelijkheid te bieden bijzondere (persoonsgevoelige) gegevens te filteren om te voorkomen dat deze gedeeld worden met derde partijen.
01-09-2021	AP stuurt een brief naar de NVB over richtlijnen voor de verdere verwerking van transactiegegevens voor direct marketingdoeleinden.
14-09-2019	RTS treedt in werking. In de voorafgaande transitieperiode tussen 13-03-2018 en 14-09-2019 konden betalingsdienstverleners al hun diensten aan te bieden onder PSD2, maar waren nog niet verplicht om de bijbehorende veiligheidsmaatregelen in te voeren.
Mei-2020	Het MOB stemt in met 'good practices' opgesteld rond transparantie over rekeninginformatiediensten. Deze hadden het doel dat consumenten en ondernemers het verzoek voor toegang op een eenduidige manier kunnen beoordelen.
16-09-2020	De consultatieperiode van de EDPB over de verhouding tussen de PSD2-richtlijn en de AVG loopt af. Deze openbare consultatie begon 22 juli 2020.
15-12-2020	EDPB verduidelijkt in haar richtsnoeren de wisselwerking tussen PSD2 en de AVG op het gebied van persoonsgegevens.
01-01-2021	Laatste implementatie fase PSD2. Partijen moeten per deze datum volledig voldoen aan de RTS. EBA had een datum vastgesteld voor de dubbele beveiliging voor online kaartbetalingen. Halverwege 2019 heeft de EBA marktpartijen 14 maanden (tot 2021) aanpassingstijd toegezegd.
Begin 2021	Afronding van het migratieproject omtrent de dubbele beveiliging (SCA) van de Betaalvereniging. De Betaalvereniging had samen met relevante marktpartijen dit project opgestart om de invoering van de dubbele beveiliging bij online creditcards zo rimpelloos mogelijk te laten verlopen.
19-07-2021	PSD2-me-niet filter (verpakt in een API) is gepubliceerd. Hiermee hebben consumenten de mogelijkheid om betalingen te filteren.

“De wetenschap dat het goed is.”

SEO Economisch Onderzoek doet onafhankelijk toegepast onderzoek in opdracht van overheid en bedrijfsleven. Ons onderzoek helpt onze opdrachtgevers bij het nemen van beslissingen. SEO Economisch Onderzoek is gelieerd aan de Universiteit van Amsterdam. Dat geeft ons zicht op de nieuwste wetenschappelijke methoden. We hebben geen winstoogmerk en investeren continu in het intellectueel kapitaal van de medewerkers via promotietrajecten, het uitbrengen van wetenschappelijke publicaties, kennisnetwerken en congresbezoek.

SEO-rapport ?
ISBN ?

Informatie & Disclaimer
SEO Economisch Onderzoek heeft op de verkregen informatie en data geen onderzoek uitgevoerd dat het karakter draagt van een accountantscontrole of due diligence. SEO is niet verantwoordelijk voor fouten of omissies in de verkregen informatie en data.

seo • economisch onderzoek

Roetersstraat 29
1018 WB, Amsterdam

+31 20 525 1630
secretariaat@seo.nl
www.seo.nl