Rondetafelgesprek PSD2 - position paper

Aan:	Vaste commissie voor Financiën, Tweede Kamer
Van:	Erik van der Zee, PwC (erik.van.der.zee@pwc.com)
Datum:	15 november 2017

PwC adviseert binnen de financiële sector over digitale transformatie, operationele effectiviteit en het voldoen aan wet- en regelgeving. Erik van der Zee is partner bij PwC Nederland. Hij adviseert partijen in de financiële sector op PSD2 en is betrokken bij het vanuit San Francisco geleide onderzoeksproject 'DeNovo', een digitaal FinTech-platform van PwC. Dit position paper is opgesteld in voorbereiding op het rondetafelgesprek over de betaaldiensten PSD2.

PSD2 is van groot belang voor het Nederlandse betalingsverkeer in het algemeen en de financiële sector in het bijzonder. De richtlijn bereidt ons voor op een wereld van "open banking". Door het openstellen van toegang tot consumentengegevens en bancaire infrastructuur, verlaagt PSD2 de toetredingsdrempel voor derde partijen, zoals financieel-technologische bedrijven (FinTech). PSD2 maakt de weg vrij voor nieuwe businessmodellen.

Nederland wordt wereldwijd gezien als toonaangevend op het gebied van betalingsverkeer. De Nederlandse infrastructuur staat bekend als betrouwbaar en efficiënt. Veel betalingen verlopen digitaal. Ook is Nederland vooroplopend ten aanzien van internet- en smartphonegebruik. Daarmee kan PSD2 worden aangegrepen om ruimte te maken voor nieuwe bancaire diensten die van toegevoegde waarde kunnen zijn voor gebruikers en vervolgens ingezet kunnen worden als exportproduct.

De voorbereiding van de implementatie van de richtlijn laat te wensen over. Daardoor zijn nog weinig Europese banken klaar voor PSD2. Dit blijkt uit recent onderzoek van PwC onder 39 grote banken uit 18 Europese landen. Hoewel in Nederland aan de minimumvereisten lijkt te worden voldaan en vrijwel alle banken actief zijn met PSD2, buigt in Europa 38% van de banken zich nog over de precieze impact. Nog slechts 9% is begonnen met de implementatie.

Dat is reden tot zorg. De Nederlandse economie is in grote mate afhankelijk van het vlekkeloos verlopen van de afhandeling en toegankelijkheid van het betalingsverkeer. Ook voor kleinere bedragen geldt dat problemen bij de afhandeling ontwrichtend kunnen werken. In dit position paper wordt achtereenvolgens ingegaan op de gevolgen van PSD2 voor 1) de consument, 2) aanbieders van financiële diensten en 3) toezichthouders.

PricewaterhouseCoopers B.V., Thomas R. Malthusstraat 5, 1066 JR Amsterdam, Postbus 90351, 1006 BJ Amsterdam
T: 088 792 00 20, F: 088 792 96 40, www.pwc.nl

1. Consumenten zijn nog onvoldoende bekend met de implicaties van PSD2

Betaalgegevens behoren tot de meest persoonlijke informatie van mensen. Ze bevatten gegevens over de precieze activiteiten die iemand op enig moment en locatie onderneemt. Dat is waardevolle informatie voor consumenten zelf (waar geef ik mijn geld aan uit en – bijvoorbeeld – hoe kan ik betalingsachterstanden voorkomen?) en voor aanbieders (hoe kan de dienstverlening aan klanten worden verbeterd?). Tegelijkertijd is het voor consumenten vaak onduidelijk wat er met hun gegevens gebeurt, en wat in de praktijk de begrenzing is van de toestemming die zij geven aan hun bank.

Dat kan problematisch zijn, omdat het belang van de consument niet altijd samenvalt met het belang van de aanbieder. Immers, het zogenoemde toestemmingsvereiste is contextafhankelijk. In hoeverre moet worden toegestaan dat betaalinformatie wordt gedeeld omwille van gebruiksgemak of een lagere prijs? Begrijpen alle consumenten het, en zijn ze voldoende kritisch? Het is voor een individuele consument niet eenvoudig een inschatting te maken van de mogelijke gevolgen van het afstaan met slechts een “vinkje” van persoonlijke gegevens in ruil voor veelal ongedefinieerde toekomstige diensten. Daarom moet op de bescherming van informatie van consumenten goed worden toegezien.

2. Bestaande en nieuwe aanbieders hebben baat bij duidelijkere regels

Uit het eerder genoemde PwC-onderzoek blijkt dat banken verwachten dat de impact van PSD2 het grootst zal zijn voor technologie, APIs (application programming interfaces) en autorisatie en authenticatie. Wij hebben de indruk dat het maken van betrouwbare APIs (gebaseerd op gemeenschappelijke afspraken tussen financiële instellingen over standaarden en protocollen) een haalbare kaart is, mits de standaarden waarop banken en derde partijen de PSD2-richtlijn moeten uitvoeren helder en eenvoudig zijn. Vooralsnog ontbreekt die gemeenschappelijke API-standaard.

Verder verwachten wij dat banken zullen innoveren binnen hun eigen businessmodellen. Hierbij kunnen zij gebruikmaken van bestaande en veilige infrastructuren, bekende klantenbestanden en hun ervaring als financieel dienstverleners. Opvallend is dat 50% van de ondervraagde banken aangeven een “Bank-as-a-platform”- aggregator te willen worden, wat betekent dat zij derde partijen willen toelaten om hun eigen producten en diensten te integreren met het aanbod van de bank. Veel FinTech-spelers werken dan ook in partnerships met bestaande banken of worden daarin zelfs opgenomen.

Middels concurrentie en samenwerking zal de huidige exclusiviteit op het betalingsverkeer van banken door PSD2 worden verkleind, zoals ook de expliciete bedoeling is van de richtlijn. Daarbij is wel onze verwachting dat FinTechs zich in eerste instantie zullen richten op de meest lucratieve schakels in de waardeketen, zoals aankoopbetalingen, financieringen en financiële planning. Banken mogen om een gelijk speelveld vragen, zowel wat betreft veiligheidstechnologie als een eerlijke verdeling van investeringen en baten. Nu is de zorg dat tech-partijen meedoen, zonder dat ze bank zijn.

Hierdoor ontstaan voorts zorgen over het risicomanagement van de gehele betaal- of informatieketen. Wie is verantwoordelijk en aansprakelijk indien problemen ontstaan? Denk hierbij aan datalekken of overtredingen van de GDPR[1]. Het is erg belangrijk om op die momenten de echte veroorzaker aan te pakken. De PSD2-richtlijn gaat ook op dit punt nog onvoldoende in.

[1] EU General Data Protection Regulation

3. Toezichthouders moeten digitaler worden

Ten aanzien van PSD2 wordt van toezichthouders verwacht dat zij hun krachten bundelen op de volgende terreinen:

- Beschermen van privacy en goed definiëren en interpreteren van toestemming door consumenten;
- Bewaken van autorisatie en authenticatie in zorgvuldige balans met gebruikersgemak;
- Komen tot goede API- en *screen scraping*-standaarden[2];
- Waarborgen van de betrouwbaarheid van het Nederlandse betalingsverkeer.

Zoals hiervoor beschreven, begrijpen niet alle consumenten wat hun toestemming precies inhoudt en wat hiervan de mogelijke consequenties zijn. Consumenten moeten tegen zichzelf worden beschermd. Daarom is ten eerste streng toezicht op toestemmingsvereisten, en de reikwijdte hiervan, noodzakelijk, opdat problemen worden voorkomen.

Ten tweede is PSD2 een zeer dynamische omgeving, en moeten toezichthouders zich verdiepen in nieuwe vormen van autorisatie en authenticatie. Binnen PSD2 zijn – voor bedragen boven de dertig euro – autorisatie en authenticatie bepaald op *Multi-factor Authentication* (MFA), met als veelvoorkomende variant *Two-factor Authentication* (2FA). Voorkomen moet worden dat dit voor gebruikers te bewerkelijk wordt, bijvoorbeeld indien altijd een *device* vereist is. Het verdient aanbeveling gebruik te maken van gegevens die relatief moeilijk te vervalsen zijn, zoals biomedische kenmerken (vingerafdruk of spraakherkenning). *Identitiy Access Management* (IAM) wordt hierdoor van steeds groter belang. Niet alleen om klanten te herkennen en binnen te laten, maar ook om fraudeurs en andere kwaadwillenden buiten te houden.

Daarnaast schrijft PSD2 voor op welke wijze de voornoemde APIs kunnen worden beveiligd. Uit het PwC-onderzoek blijkt dat veel partijen de voorschriften nog niet hebben doorgevoerd maar hierover wel in gesprek zijn met mogelijke partners. Als dit ertoe leidt dat alle banken hun eigen API definiëren, zal het moeilijker worden voor transactie- of informatiedienstverleners om hierop aan te sluiten. Evenzeer dient screen scraping veilig en betrouwbaar te zijn. Hier ligt een derde belangrijke toezichtstaak.

Ten slotte heeft de toezichthouder een belangrijke rol bij het bewaken van een gelijk speelveld. Daarvoor moet een verschuiving plaatsvinden van toezicht op entiteiten naar toezicht op activiteiten. Wanneer bijvoorbeeld een “tech giant” een eigen betalingssysteem creëert, zou dat dan niet aan dezelfde regels moeten voldoen als wanneer een bank dat doet?

Gezien deze ontwikkelingen geldt de behoefte aan digitale vaardigheden niet alleen voor banken, maar net zo goed voor toezichthouders zelf. Zij moeten aan de slag als “SupTech”: supervisors die FinTech en RegTech toepassen. SupTech kan helpen om niet alleen terugkijkend te sanctioneren maar ook

[2] Screen scraping is een techniek waarmee derde betaaldienstverleners toegang kunnen krijgen tot de bankrekening van de klant met de inloggegevens van de klant.

vooruitkijkend risico's te beheersen. Kortom, toezicht moet meegroeien met de digitalisering van onze samenleving.

Aanbevelingen

Duidelijk is dat PSD2 een noodzakelijke volgende stap is in het regelgevende kader waarbinnen bancaire diensten zich verder kunnen ontwikkelen. De vernieuwing is al volop aan de gang, maar moet wel worden beheerst. Toezichthouders zullen hierin een actievere rol moeten vervullen.

PwC doet de volgende aanbevelingen:

- Bepaal per casus wat de precieze impact is van de toestemming door de consument en wat hiervan de gevolgen zijn voor de privacy. Hoe wordt de overdracht van gegevens beschermd, hoe worden deze gebruikt en hoe wordt de consument hierover geïnformeerd?

- Dwing veilige en gebruiksvriendelijke authenticatie af. Maak daarbij gebruik van de smartphones die consumenten reeds bezitten (waarmee authenticatie eenvoudig wordt mogelijk gemaakt, ook wel "bring your own identity" genoemd);

- Zorg voor duidelijke, gemeenschappelijke standaarden, voor API en screen scraping, zodat onnodige complexiteit wordt voorkomen en de implementatie kan worden versneld;

- Zorg voor duidelijkheid over de verantwoordelijkheid voor en afhandeling van incidenten;

Tot slot: eventuele extra maatregelen vanuit Nederland, moeten ook in Europese context worden bezien. Aanbieders en consumenten kunnen arbitrage plegen tussen nationale stelsels, waardoor te lage eisen kunnen leiden tot ongewenste toetreders en te hoge eisen de Nederlandse concurrentiekracht kunnen beperken ten opzichte van andere landen.

Bijlage:

- Waiting until the Eleventh Hour – European banks' reaction to PSD2 (PwC, oktober 2017)