



Aangetekend
De Minister van Financiën
Postbus 20201
2500 EE DEN HAAG

Datum
20 december 2017

Ons kenmerk
z2017-07835

Uw brief van
28 september 2017

Uw kenmerk

Onderwerp
Advies Implementatiebesluit herziene richtlijn betaaldiensten

Geachte,

Bij brief van 28 september 2017 hebt u de Autoriteit Persoonsgegevens (hierna: de AP) gevraagd op grond van artikel 51, tweede lid, van de Wet bescherming persoonsgegevens (hierna: de Wbp) advies uit te brengen over het ontwerp van het Implementatiebesluit herziene richtlijn betaaldiensten¹ (hierna: de ontwerp-AMvB). Tezamen met de Implementatiewet herziene richtlijn betaaldiensten² (hierna: de Implementatiewet) beoogt dit besluit te voorzien in de nationale omzetting van de richtlijn (EU) 2015/2366³ (ook bekend als de tweede Payment Services Directive; hierna: PSD2). Over de Implementatiewet heeft de AP op 22 augustus 2017 advies uitgebracht. In de kern concludeert dat advies dat in het wetsvoorstel onvoldoende rekenschap is gegeven van de verhouding met de Algemene verordening gegevensbescherming⁴ (hierna: de AVG) en de Wbp.

¹ Besluit tot wijziging van het Besluit Prudentiële regels Wft, het Besluit Markttoegang financiële ondernemingen Wft en het Besluit Gedragstoezicht financiële ondernemingen Wft ter implementatie van richtlijn 2015/2366/EU van het Europees Parlement en de Raad van 25 november 2015 betreffende betaaldiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PbEU 2015, L 337).

² Wijziging van de Wet op het financieel toezicht, de Wet bekostiging financieel toezicht, het Burgerlijk Wetboek en de Wet handhaving consumentenbescherming ter implementatie van richtlijn nr. 2015/2366/EU van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PbEU 2015, L 337).

³ Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PbEU 2015, L 337).

⁴ 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 (PbEU 2016, L 119).



Datum
20 december 2017

Ons kenmerk
z2017-07835

In dit advies komt de AP tot de slotsom dat de ontwerp-AMvB de verhouding met de AVG (en de Wbp) onjuist adresseert. Deels in navolging van het advies over de Implementatiewet zal in het onderhavige advies worden ingegaan op drie hoofdaspecten in relatie tot de ontwerp-AMvB, namelijk (1) de verhouding met de AVG, (2) het toestemmingsvereiste en (3) de allocatie van het toezicht op de bescherming van persoonsgegevens in het kader van PSD2.

Inhoud AMvB

De ontwerp-AMvB wijzigt een drietal algemene maatregelen van bestuur, te weten het Besluit prudentiële regels Wft (hierna: het Bpr), het Besluit Markttoegang financiële ondernemingen Wft en het Besluit Gedragstoezicht financiële ondernemingen Wft.

Wettelijk kader

De AP verwijst kortheidshalve naar het wettelijk kader zoals weergegeven in het advies over de Implementatiewet van 22 augustus 2017. In aanvulling hierop dient te worden vermeld dat inmiddels het wetsvoorstel Uitvoeringswet Algemene verordening gegevensbescherming (hierna: de Uitvoeringswet AVG) bij de Tweede Kamer is ingediend.⁵ Dit wetsvoorstel bevat regels waarmee in Nederland uitvoering wordt gegeven aan de AVG.

Beoordeling

1 Verhouding PSD2 en AVG

De PSD2 betreft een herziening van het bestaande juridisch kader voor betalingsdiensten⁶ binnen de Europese Economische Ruimte. Ten opzichte van de eerste richtlijn beoogt de Uniewetgever met PSD2 onder meer de bevordering van innovatieve mobiele en internetbetalingsdiensten en de regels op de markt voor betalingsdiensten in de EU te harmoniseren, alsmede versterking van consumentenrechten. Dit dient gepaard te gaan met een adequaat niveau van gegevensbescherming. De preambule bij PSD2 verwijst wat de juridische basis voor de verwerking van persoonsgegevens betreft naar het algemene Unierechtelijke kader voor gegevensbescherming,⁷ in het bijzonder naar Richtlijn 95/46/EG (hierna: de Privacyrichtlijn).⁸

⁵ Kamerstukken II 2017-2018, 34 851.

⁶ In de Nederlandse taalversie van PSD2-richtlijn worden de begrippen "betalingsdienst" en "betalingsgegevens" gebezigd. In de ontwerp-AMvB en de Wft worden de termen betaaldienst en betaalgegevens gehanteerd. Uit het oogpunt van leesbaarheid en eenduidigheid is in dit advies ervoor gekozen "betalingsdienst" en "betalingsgegevens" te bezigen.

⁷ Overweging 89 van de preambule bij PSD2, deze luidt:

"Het aanbieden van betalingsdiensten door de betalingsdienaars kan de verwerking van persoonsgegevens met zich mee brengen. Richtlijn 95/46/EG van het Europees Parlement en de Raad [...], de nationale voorschriften tot omzetting van Richtlijn 95/46/EG en Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad [...] 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 gegevensverwerkingsystemen die in het kader van deze richtlijn worden ontwikkeld en gebruikt, de beginselen gegevensbescherming by design en gegevensbescherming by default in acht worden genomen."



Datum
20 december 2017

Ons kenmerk
z2017-07835

De Privacyrichtlijn is in Nederland omgezet in de Wbp. Hierbij zij opgemerkt dat PSD2 dateert van 25 november 2015 en is bekendgemaakt op 23 december 2015. Deze richtlijn dateert dus van vóór de AVG (die is bekendgemaakt op 4 mei 2016). Ingevolge artikel 94, tweede lid, van de AVG gelden verwijzingen naar de Privacyrichtlijn als verwijzingen naar de AVG. Dit betekent dat de verwerking van persoonsgegevens in een betalingssysteem en door een betalingsdienstaanbieder moet voldoen aan de vereisten die daaraan per 25 mei 2018 op grond van de AVG worden gesteld en tot die datum aan de vereisten die daaraan op grond van de Privacyrichtlijn zijn gesteld en in Nederland zijn neergelegd in de Wbp.

De AVG bevat een - algemeen - juridisch kader voor de bescherming van persoonsgegevens en het vrije verkeer van die gegevens. Het doel van de AVG is verdergaande harmonisatie van de regels rond de bescherming van persoonsgegevens en de bevordering van het vrije verkeer van gegevens binnen de EU. De AVG zal in Nederland in de plaats treden van de Wbp. De AVG biedt een gelijk beschermingsniveau voor de verwerking van persoonsgegevens in de gehele EU. De AP en haar collega-privacytoezichthouders in de andere lidstaten houden vanaf die datum toezicht op de naleving van de AVG, waarin ook regels voor samenwerking en geschilbeslechting tussen de privacytoezichthouders zijn opgenomen. Dit laatste is in het bijzonder van belang bij grensoverschrijdende verwerkingen van persoonsgegevens. Bij de dienstverlening door betalingsdienstaanbieders zal daarvan vaak sprake zijn.

Naast de verwijzing naar het algemene Unierechtelijke kader inzake gegevensbescherming geeft PSD2 in hoofdstuk IV specifieke regels met betrekking tot de verwerking van persoonsgegevens ten behoeve van betalingsdiensten. Artikel 94, tweede lid, van PSD2 stelt een voorwaarde aan de rechtmatige verwerking van persoonsgegevens in het kader van betalingsdiensten, namelijk dat aanbieders van deze diensten alleen met de “uitdrukkelijke” toestemming van de betalingsdienstgebruiker toegang mogen krijgen tot persoonsgegevens die noodzakelijk zijn voor het aanbieden van hun betalingsdiensten, deze verwerken en bewaren. De ontwerp-AMvB beoogt te voorzien in het opnemen van deze bepaling in het nationale recht. In verband hiermee wordt in de Implementatiewet een delegatiegrondslag toegevoegd aan artikel 3.17 van de Wet op het financieel toezicht (Wft).⁹

1.1 Onderscheid (gevoelige) betaalgegevens en persoonsgegevens

In de ontwerp-AMvB wordt een onderscheid gemaakt tussen gevoelige betaalgegevens en persoonsgegevens in het voorgestelde artikel 26c van het Bpr door deze twee begrippen in een nevenschikking te plaatsen. In paragraaf 3.5 van de ontwerp-nota van toelichting (hierna: de NvT) wordt in verband met dit onderscheid gesteld:

“Elke betaaldienstverlener heeft de plicht om beveiligingsmaatregelen te nemen ter bescherming van de vertrouwelijkheid en integriteit van de persoonlijke beveiligingsgegevens van betaaldienstgebruikers. Één van die beveiligingsmaatregelen is het toepassen van authenticatieprocedures, waaronder sterke cliëntauthenticatie. De richtlijn maakt echter een duidelijk onderscheid tussen gevoelige betaalgegevens en persoonsgegevens. Vanwege dit

⁸ Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEU 2015, L 281).

⁹ Artikel I, onder R, van het wetsvoorstel Implementatiewet herziene richtlijn betaaldiensten



Datum
20 december 2017

Ons kenmerk
z2017-07835

onderscheid wordt verondersteld dat ook de bepalingen die betrekking hebben op authenticatieprocedures moeten worden opgevat als een *lex specialis* ten opzichte van de AVG. Daarom wordt DNB aangewezen om toezicht te houden op deze bepalingen.”

In deze passage wordt een onjuist onderscheid gemaakt en de daarop gebaseerde gevolgtrekking over het toezicht is evenzeer niet juist. Op de allocatie van het toezicht wordt hierna, onder 3 verder ingegaan. Voor het gemaakte onderscheid tussen betalingsgegevens en persoonsgegevens zijn noch in de preambule, noch in de tekst van PSD2 aanknopingspunten te vinden. Bovendien bevat de AVG geen bepalingen over authenticatieprocedures,¹⁰ zodat er op dit punt geen toepassingsconflict is met PSD2. Betalingsdienstverleners zijn uit hoofde van het voorgestelde artikel 26h van het Bpr in beginsel gehouden om de identiteit van hun cliënten vast te stellen aan de hand van de in dit artikel beschreven authenticatieprocedure. Op het moment dat de authenticatie plaatsvindt zijn (gevoelige) betalingsgegevens te herleiden tot een individu en betreffen deze gegevens informatie over een natuurlijke persoon. Zo bezien zijn betalingsgegevens tevens persoonsgegevens. In dit verband wijst de AP op de definitie van persoonsgegevens in artikel 4, ten eerste, van de AVG:

“alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon”.

1.2 Verwerkingen van persoonsgegevens in het kader van PSD2

Artikel 94 van PSD2 voorziet in normen die betrekking hebben op hetzelfde onderwerp als de AVG, namelijk een grondslag voor een rechtmatige verwerking van persoonsgegevens. Gelet hierop rijst de vraag welke norm voorrang heeft. De AVG bevat algemene regels over de verwerking van persoonsgegevens. De PSD2 is een sectorale richtlijn over betalingsdiensten en bevat specifieke regels voor de verwerking van persoonsgegevens door een betalingsdientaanbieder. In het Unierecht prevaleren specifieke sectorale bepalingen in beginsel boven algemene bepalingen. Artikel 94, eerste lid, van PSD2 geeft lidstaten de opdracht te voorzien in een wettelijk kader voor de verwerking van persoonsgegevens in verband met voorkoming en bestrijding van betalingsfraude. Dit is een specifieke grondslag voor gegevensverwerking in dit kader. Verder specificiert de norm van artikel 94, tweede lid van PSD2 de “algemenere” norm van toestemming voor verwerking van persoonsgegevens die is neergelegd in de AVG. Het voorgaande leidt tot de conclusie dat, gelet op het beginsel van “*lex specialis derogat legi generali*”, PSD2 op deze twee punten een *lex specialis* vormt voor de verwerking van persoonsgegevens ten behoeve van betalingsdiensten. Paragraaf 3.5 van de NvT merkt terecht op dat dit onverlet laat dat als er persoonsgegevens worden verwerkt, deze verwerking wel overeenkomstig de overige eisen van de AVG dient te geschieden.

1.3 Verwerking van persoonsgegevens voor fraudedetectie

Op grond van de Wbp mogen persoonsgegevens alleen worden verwerkt voor een bepaald doel en dient de gegevensverwerking te zijn gebaseerd op een van de in de wet vermelde gronden. Dit is onder de AVG niet

¹⁰ Volledigheidshalve zij opgemerkt dat de AVG wel algemene bepalingen over passende beveiliging kent, bijvoorbeeld artikel 5, eerste lid, aanhef en onder f, en artikel 32.



Datum
20 december 2017

Ons kenmerk
z2017-07835

anders. Artikel 94, eerste lid, van PSD2 verplicht lidstaten toe te staan dat betalingssystemen en betalingsdienstaanbieders persoonsgegevens verwerken wanneer dit noodzakelijk is voor de voorkoming van, het onderzoek naar en de opsporing van betalingsfraude. Niettegenstaande de duidelijk geformuleerde opdracht die de Uniewetgever hierin aan de nationale wetgever geeft, behoeft deze bepaling volgens de transponeringstabel bij de ontwerp-AMvB geen implementatie. De artikelsgewijze toelichting bij het voorgestelde artikel 26d (lees: 26e) van het Bpr vermeld in verband hiermee nog: “Voor aspecten van gegevensverwerking die niet specifiek in de PSD II zijn geregeld, zal de AVG onverkort toepassing vinden. Daartoe strekt ook artikel 94 (1) van de richtlijn.”

Artikel 94, eerste lid, van PSD2 komt overeen met artikel 79 van Richtlijn 2007/64/EG, de vorige richtlijn over betalingsdiensten.¹¹ Deze laatste bepaling is destijds in Nederland evenmin omgezet in nationale wetgeving. De AP wijst er in dit verband op dat na de inwerkingtreding van de implementatiewetgeving van Richtlijn 2007/64/EG diverse nieuwe technieken beschikbaar zijn gekomen waarmee grote hoeveelheden persoonsgegevens gemakkelijker kunnen worden opgeslagen en ontsloten. Deze data kunnen worden gebruikt ten behoeve van profiling (profilering).¹² Ingeval artikel 94, eerste lid, van PSD2 niet zal worden omgezet, ontbreekt een normatief kader op dit punt. Om de in die bepaling bedoelde gegevens rechtmatig te kunnen verwerken, dient de verwerking van persoonsgegevens niettemin plaats te vinden met inachtneming van de AVG, in het bijzonder met inachtneming van het bepaalde in artikel 6. In verband hiermee wijst de AP erop dat de verwerkingsgrondslag van artikel 6, eerste lid, aanhef en onder f, van de AVG altijd de daarin vermelde toetsing aan de beginselen van proportionaliteit en subsidiariteit - waarbij een afweging plaatsvindt tussen de inbreuk op de fundamentele rechten van de betrokkene versus het belang van de verwerkingsverantwoordelijke - in het concrete geval vergt. Daarbij heeft een betrokkene op grond van artikel 21, eerste lid, van de AVG het recht om bezwaar te maken tegen profiling op basis van artikel 6, eerste lid, aanhef en onder f, van de AVG. Verder is in dit verband van belang dat een betrokkene het recht heeft om niet te worden onderworpen aan op profiling gebaseerde besluitvorming (artikel 22, eerste lid, van de AVG). Dit geldt niet in de in artikel 22, tweede lid, van de AVG vermelde gevallen. Ingevolge sub b van deze bepaling is een op profiling gebaseerd besluit toegestaan als daartoe is voorzien bij een Unierechtelijke of lidstaatrechtelijke bepaling die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene. De AP adviseert aan deze punten passende aandacht te besteden.

2 De uitleg van “uitdrukkelijke toestemming” voor de verwerking van persoonsgegevens
Ter implementatie van artikel 94, tweede lid, van PSD2 is in het voorgestelde artikel 26e van het Bpr bepaald dat een betalingsdienstverlener, met uitzondering van de betalingsdienstverlener die uitsluitend

¹¹ Richtlijn 2007/64/EG van het Europees Parlement en de Raad van 13 november 2007 betreffende betalingsdiensten in de interne markt tot wijziging van de Richtlijnen 97/7/EG, 2002/65/EG, 2005/60/EG en 2006/48/EG, en tot intrekking van Richtlijn 97/5/EG (PbEU 2007, L 319).

¹² Met “big data” kunnen organisaties mensen in groepen indelen. Ook kunnen zij big data gebruiken om het gedrag van mensen te voorspellen. Zowel groepsindelingen als voorspellingen worden “profiling” (in de Nederlandse vertaling van de AVG: profilering) genoemd. Analyses van big data kunnen bijvoorbeeld worden ingezet om fraudeurs op te sporen, of om ongewenste klanten te weren, zoals bij een aanvraag voor een lening. Profiling kan zo gezien een vorm van risicomangement zijn.



Datum
20 december 2017

Ons kenmerk
z2017-07835

rekeninginformatiediensten verleent,¹³ alleen met de uitdrukkelijke toestemming van de betalingsdienstgebruiker toegang tot diens persoonsgegevens verkrijgt, om deze gegevens te verwerken en te bewaren, voor zover noodzakelijk voor het verlenen van betalingsdiensten.

Wellicht ten overvloede - maar bepaald niet onbelangrijk - merkt de AP op dat de gegeven toestemming alleen betrekking kan hebben op persoonsgegevens van degene die toestemming heeft gegeven. Betalingsgegevens die persoonsgegevens bevatten van derden (bijvoorbeeld degene aan wie een geldbedrag wordt overgemaakt) kunnen dan ook niet enkel op basis van deze toestemming worden verwerkt door betalingsdientaanbieders.

De voorwaarde van uitdrukkelijke toestemming in artikel 26e van het Bpr ziet specifiek op de verwerking van de noodzakelijke gegevens voor de betalingsdienst. Deze verwerkingsgrondslag is soortgelijk aan de verwerkingsgrondslag van artikel 6 van de AVG. Afhankelijk van de inhoud van de overeenkomst kan gesteld worden dat de verwerking van gegevens als bedoeld in het voorgestelde artikel 26e noodzakelijk is voor de uitvoering van de overeenkomst die ten grondslag ligt aan de verrichting van de betalingsdienst (vergelijk artikel 6, eerste lid, aanhef en onder b, van de AVG). Zoals in de NvT bij de ontwerp-AMvB is vermeld, beoogt PSD2 aanvullende bescherming ten opzichte van de AVG te bieden.¹⁴ Met oog daarop zal bij een concrete verwerking van persoonsgegevens ten behoeve van de verrichting van een betalingsdienst de norm waaraan moet worden getoetst steeds zijn of uitdrukkelijke toestemming voor deze verwerking is verkregen. Een andere uitleg zou afbreuk doen aan de met artikel 94, tweede lid van PSD2 beoogde privacywaarborg, die vereist dat de betalingsdienstgebruiker wordt geïnformeerd over de te verwerken persoonsgegevens en een handeling verricht die is gericht op het geven van een uitdrukkelijke verklaring van toestemming.¹⁵ Afgezien van het hiervoor besproken vereiste van uitdrukkelijke toestemming is de AVG verder onverkort van toepassing op betalingsdiensten. Dit betekent bijvoorbeeld dat betalingsdientaanbieders het verzoek om uitdrukkelijke toestemming om persoonsgegevens te mogen verwerken in begrijpelijke taal moeten presenteren aan gebruikers en dat gebruikers de toestemming vrijelijk moeten kunnen geven (artikel 7 van de AVG). Als de betalingsdientaanbieder tevens toestemming vraagt voor de verwerking van andere persoonsgegevens dan die noodzakelijk zijn voor het verlenen van de betalingsdienst, of gegevens aanvullend voor een ander doel zou willen verwerken, dan is daarop het voorgestelde artikel 26e niet van toepassing. Die toestemming en de daarop gebaseerde verwerking valt geheel onder het bereik van de AVG. De NvT maakt hier weliswaar ook melding van, maar is op dit punt niet consistent en duidelijk.

Het voorgestelde artikel 26e van het Bpr wordt opgenomen in hoofdstuk 4 van het Bpr, dat regels bevat met betrekking tot de bedrijfsvoering van vergunninghoudende financiële ondernemingen. Het toezicht op de naleving van deze bepaling zal gelet daarop plaatsvinden in het kader van de beoordeling of een

¹³ De tekst van de ontwerp-AMvB verwijst naar de betalingsdiensten, vermeld onder 8 van de bijlage bij PSD2. Dit betreft rekeninginformatiediensten. Artikel 94 maakt onderdeel uit van titel IV van PSD2. Gelet op artikel 33, tweede lid, van PSD2 - waarin de toepassing van titel IV wordt uitgesloten - is artikel 94 niet van toepassing op rekeninginformatiediensten.

¹⁴ NvT; artikelsgewijze toelichting bij artikel I, onderdeel D, ten aanzien van artikel 26d (lees: 26e).

¹⁵ De uniforme wijze waarop alle privacytoezichthouders "toestemming" en "uitdrukkelijke toestemming" op grond van de AVG binnen de EU gaan uitleggen en toepassen is zeer recent verwoord in een guideline die inmiddels is vastgesteld in het overleg van alle voorzitters van die toezichthouders (de Artikel 29-werkgroep).



Datum
20 december 2017

Ons kenmerk
z2017-07835

betalingsdienstaanbieder werkzaam mag zijn op de financiële markten, terwijl de norm van uitdrukkelijke toestemming ex artikel 94, tweede lid, van PSD2 een voorwaarde voor het verrichten van de betalingsdienst in het concrete geval betreft. De in de ontwerp-AMvB voorgestelde wettelijke positionering van het vereiste van uitdrukkelijke toestemming leidt ertoe dat dit vereiste is vormgegeven als een vergunningvoorschrift voor de betalingsdienstaanbieder. Artikel 94 is evenwel opgenomen in hoofdstuk 4, “Gegevensbescherming”, dat onderdeel is van titel IV van PSD2, die bepalingen bevat omtrent de rechten en plichten met betrekking tot het aanbieden en het gebruik van betalingsdiensten, terwijl de vereisten voor een vergunning zijn opgenomen in titel II van PSD2. Dit brengt mee dat een betalingsdienstaanbieder zich niet alleen bij de vergunningverlening, maar ook ná toetreding tot de markt aan de norm van artikel 94, tweede lid, van PSD2 dient te houden. De voorgestelde positionering van het vereiste van uitdrukkelijke toestemming in het Bpr doet zo bezien afbreuk aan de betekenis en draagwijdte van de richtlijn in kwestie en aan de daarin duidelijk en nauwkeurig gestelde waarborg met betrekking tot gegevensbescherming. Met als gevolg dat dit in strijd is met de doelstelling van PSD2 en de aard van het daarbij toegekende recht aan de betrokkenen. Derhalve leidt de voorgestelde opname van de norm van artikel 94, tweede lid, van PSD2 in hoofdstuk 4 van het Bpr tot een onjuiste implementatie van PSD2.

De conclusie van het voorgaande is dat artikel 94, tweede lid, van PSD2 geen ruimte biedt voor de in de ontwerp-AMvB voorgestelde implementatie van die bepaling. Deze implementatie van PSD2 leidt op het punt van gegevensbescherming niet tot het met de richtlijn beoogde resultaat. De AP adviseert u de implementatiewetgeving op dit punt aan te passen.

3. Allocatie van het toezicht

Zoals onder 1.2 is uiteengezet is de AVG in volle omvang van toepassing op de verwerkingen op basis van PSD2. Slechts enkele bepalingen uit PSD2 gelden als *lex specialis* ten opzichte van de AVG. Dat betekent dat alle bepalingen uit de AVG die onder meer verband houden met toezicht door een onafhankelijke toezichthouder, de samenwerking en coherentie tussen die toezichthouders binnen de EU, het recht van betrokkenen om een klacht in te dienen bij de toezichthouder en de regeling voor de afdoening bij grensoverschrijdende verwerkingen volledig van toepassing zijn.

Ingevolge artikel 51, eerste lid, van de AVG bepaalt elke lidstaat dat één of meer onafhankelijke overheidsinstanties verantwoordelijk zijn voor het toezicht op de toepassing van de AVG. De taken en bevoegdheden van de toezichthoudende autoriteit zijn uitgewerkt in de hoofdstukken VI en VII van de AVG. In artikel 6, tweede lid, van de Uitvoeringswet AVG is de AP aangewezen als enige toezichthoudende autoriteit in de zin van de AVG. De AP is ook als enige toezichthouder verantwoordelijk voor de uitvoering van de samenwerking tussen toezichthoudende autoriteiten en voor de toetsing van de conformiteit van de toetsingskaders van verschillende autoriteiten (hoofdstuk VII van de AVG). De voorzitter van de AP is ook namens de nationale toezichthoudende autoriteit lid van het Europees Comité voor gegevensbescherming (European Data Protection Board; EDPB).¹⁶ Op grond van artikel 68, derde lid, van de AVG heeft de voorzitter van één toezichthoudende autoriteit per lidstaat een zetel in dit Comité.

¹⁶ Zie in dit verband de memorie van toelichting bij de Uitvoeringswet AVG; Kamerstukken II 2017-2018, 34 851, nr. 3, p. 23.



Datum
20 december 2017

Ons kenmerk
z2017-07835

De wetgever lijkt bij de omzetting van PSD2 op twee gedachten te hinken. Enerzijds lijkt onomstreden dat de AP ten volle toezicht houdt op de verwerking van persoonsgegevens in het kader van PSD2, anderzijds wordt de omzetting van artikel 94, tweede lid, van PSD2 opgenomen in een AMvB die de Wft als delegatiegrondslag heeft. In de Wft is de AP niet vermeld als toezichthouder. Dit heeft tot gevolg dat De Nederlandsche Bank (hierna: DNB) belast is met het toezicht op de verwerking van persoonsgegevens als bedoeld in het voorgestelde artikel 26e van het Bpr. DNB is evenwel in de Uitvoeringswet AVG niet aangewezen als toezichthoudende autoriteit in de zin van de AVG en neemt derhalve in Europees verband niet deel aan het hiervoor gememoreerde afstemmings- en coherentiemechanisme.

Uit oogpunt van een consistente toepassing van de regelgeving over gegevensbescherming in het kader van betalingsdiensten en met oog op de afstemming in Europees verband moet het toezicht op een juiste naleving van de normen over gegevensbescherming in dit verband zijn belegd bij de AP. Hiertoe dient te worden voorzien in een toereikende en juiste wettelijke grondslag. Om iedere twijfel hierover weg te nemen adviseert de AP om een dergelijke grondslag op te nemen in de Uitvoeringswet AVG, die inhoudt dat de AP toezichthouder is op de verwerking van persoonsgegevens, met inbegrip van verwerkingen in het kader van PSD2.

Overigens volgt uit een inventarisatie onder de leden van de Financial Matters-subgroep, opererend onder de Artikel 29-werkgroep, dat Nederland alleen staat bij een eventuele keuze om het toezicht op de norm van artikel 94, tweede lid, van PSD2 niet bij dezelfde toezichthouder als de toezichthouder op de AVG onder te brengen.¹⁷ Mede met oog hierop is recentelijk op de plenaire vergadering van de Artikel 29-werkgroep besloten tot monitoring van de ontwikkelingen rondom de implementatie van PSD2 in de onderscheiden lidstaten.

Conclusie

Samenvattend constateert de AP dat de ontwerp-AMvB de verhouding met de AVG (en de Wbp) onjuist adresseert. De AP adviseert derhalve de ontwerp-AMvB op de aangedragen punten te herzien en de normen over bescherming van persoonsgegevens uit PSD2 te implementeren op een wijze die recht doet aan het met de richtlijn beoogde resultaat én de verhouding met de AVG, alsmede een effectief toezicht op gegevensbescherming.

Hoogachtend,
Autoriteit persoonsgegevens,

mr. A. Wolfsen
Voorzitter

¹⁷ Op de questionnaire die was uitgezet binnen de Financial Matters-subgroep (waarin medewerkers van nationale dataproctietoezichthouders zijn vertegenwoordigd) zijn reacties over de implementatiewetgeving van 11 verschillende landen binnengekomen. Uit die reacties kan worden geconcludeerd dat van deze 11 landen alleen in Nederland de wetgever voornemens is om het toezicht op de norm van artikel 94, tweede lid, van PSD2 niet bij de nationale dataproctietoezichthouder onder te brengen. Volgens de overige 10 respondenten volgt uit de (voorgenomen) nationale implementatiewetgeving dat het toezicht op die norm is belegd bij dezelfde autoriteit als die toezicht houdt op de naleving van de AVG.