Richtsnoeren 06/2020 inzake de wisselwerking tussen de tweede richtlijn betalingsdiensten en de AVG

Versie 2.0

Vastgesteld op 15 december 2020

Versiegeschiedenis

Versie 2.0	15.12.2020	Vaststelling van de richtsnoeren na openbare raadpleging
Versie 1.0	17.07.2020	Vaststelling van de richtsnoeren voor openbare raadpleging

Inhoudsopgave

Het Europees Comité voor gegevensbescherming

Gezien artikel 70, lid 1, punt e), van 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 (hierna "AVG" genoemd),

Gezien de EER-overeenkomst en in het bijzonder bijlage XI en protocol 37 van die overeenkomst, als gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018[1],

Gezien de artikelen 12 en 22 van zijn reglement van orde,

Overwegende hetgeen volgt:

(1) De algemene verordening gegevensbescherming biedt een samenhangend geheel van regels voor de verwerking van persoonsgegevens in de gehele EU.

(2) De tweede richtlijn betalingsdiensten (Richtlijn 2015/2366/EU van het Europees Parlement en de Raad van 23 december 2015, hierna "PSD2" genoemd) strekt tot intrekking van Richtlijn 2007/64/EG en bevat nieuwe voorschriften om consumenten, handelaren en ondernemingen in de betalingsketen rechtszekerheid te bieden en het rechtskader voor de markt voor betalingsdiensten te moderniseren[2]. De lidstaten hadden tot 13 januari 2018 de tijd om de RBD2 in intern recht om te zetten.

(3) Een belangrijk kenmerk van de RBD2 is de invoering van een rechtskader voor nieuwe betalingsinitiatiediensten en rekeninginformatiediensten. De RBD2 stelt deze nieuwe betalingsdienstaanbieders in staat om toegang te krijgen tot betaalrekeningen van betrokkenen voor het aanbieden van voornoemde diensten.

(4) Met betrekking tot gegevensbescherming is in artikel 94, lid 1, RBD2 bepaald dat de verwerking van persoonsgegevens, met inbegrip van de verstrekking van informatie over de verwerking, voor de doeleinden van de RBD2 geschiedt overeenkomstig de AVG[3] en Verordening (EU) nr. 2018/1725.

(5) In overweging 89 RBD2 staat dat wanneer er voor de toepassing van de RBD2 persoonsgegevens worden verwerkt, het precieze doel wordt aangegeven, de desbetreffende rechtsgrondslag wordt vermeld, de relevante beveiligingsvoorschriften van de AVG worden nageleefd en de beginselen noodzaak, evenredigheid, doelbegrenzing en een niet-buitensporige bewaarperiode in acht worden genomen. Ook moeten in alle gegevensverwerkingssystemen die in het kader van de RBD2 worden ontwikkeld en gebruikt, de beginselen gegevensbescherming by design (gegevensbescherming door ontwerp) en gegevensbescherming by default (gegevensbescherming door standaardinstellingen) in acht worden genomen[4].

(6) In overweging 93 van de RBD2 staat dat de betalingsinitiatiedienstaanbieders en de rekeninginformatiedienstaanbieders enerzijds en de rekeninghoudende betalingsdienstaanbieders anderzijds de noodzakelijke gegevensbeschermings- en beveiligingsvoorschriften in acht dienen te

[1] Verwijzingen naar "lidstaten" in dit document moeten worden gelezen als verwijzingen naar "lidstaten van de EER".
[2] Overweging 6 RBD2.
[3] Aangezien de RBD2 ouder is dan de AVG, wordt nog verwezen naar Richtlijn 95/46. Artikel 94 AVG bepaalt dat verwijzingen naar de ingetrokken richtlijn 95/46 als verwijzingen naar de AVG gelden.
[4] Overweging 89, RBD2.

nemen die zijn vastgesteld door of waarnaar wordt verwezen in deze richtlijn of die zijn opgenomen in de technische reguleringsnormen.

HEEFT DE VOLGENDE RICHTSNOEREN VASTGESTELD

1. INLEIDING

1. Bij de tweede richtlijn betalingsdiensten (RBD2) zijn een aantal nieuwigheden op het gebied van betalingsdiensten ingevoerd. Hoewel deze richtlijn nieuwe kansen creëert voor consumenten en de transparantie op dit gebied verbetert, doet de toepassing van de RBD2 enige vragen en bezorgdheid rijzen over het feit dat de betrokkenen volledige zeggenschap over hun persoonsgegevens moeten behouden. De algemene verordening gegevensbescherming (AVG) is van toepassing op de verwerking van persoonsgegevens, met inbegrip van verwerkingsactiviteiten in het kader van betalingsdiensten zoals gedefinieerd in de RBD2[5]. Verwerkingsverantwoordelijken die actief zijn op het gebied dat onder de RBD2 valt, moeten er dus altijd voor zorgen dat zij voldoen aan de vereisten van de AVG, met inbegrip van de beginselen van gegevensbescherming zoals beschreven in artikel 5 AVG, en aan de relevante bepalingen van de e-privacyrichtlijn[6]. Hoewel de RBD2[7] en de technische reguleringsnormen voor sterke cliëntauthenticatie en gemeenschappelijke en veilige open communicatiestandaarden (hierna: "technische reguleringsnormen"[8]) een aantal bepalingen ten aanzien van gegevensbescherming en beveiliging bevatten, is er twijfel gerezen over de uitlegging van die bepalingen en over de wisselwerking tussen het algemene kader voor gegevensbescherming en de RBD2.

2. Op 5 juli 2018 heeft het EDPB een brief opgesteld over de RBD2, waarin het nadere toelichting heeft gegeven over vragen met betrekking tot de bescherming van persoonsgegevens in het kader van de RBD2, in het bijzonder met betrekking tot de verwerking van persoonsgegevens van niet-overeenkomstsluitende partijen (zogeheten "silent party data" of derdengegevens) door rekeninginformatiedienstaanbieders en betalingsinitiatiedienstaanbieders, de procedures voor het verlenen en intrekken van toestemming, de technische reguleringsnormen en de samenwerking tussen rekeninghoudende betalingsdienstaanbieders op het gebied van beveiligingsmaatregelen. Bij de voorbereidende werkzaamheden voor deze richtsnoeren is input verzameld bij belanghebbenden, zowel schriftelijk als tijdens een evenement voor belanghebbenden, teneinde de meest prangende uitdagingen vast te stellen.

3. Deze richtsnoeren moeten een verdere leidraad verschaffen inzake gegevensbeschermingsaspecten in de context van de RBD2, in het bijzonder inzake het verband tussen de desbetreffende bepalingen van de AVG en de RBD2. De nadruk ligt in deze richtsnoeren

[5] Artikel 1, lid 1, AVG.
[6] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie); PB L 201 van 31.7.2002, blz. 0037.
[7] Artikel 94 BRD enz.
[8] Gedelegeerde Verordening (EU) 2018/389 van de Commissie van 27 november 2017 tot aanvulling van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad wat betreft technische reguleringsnormen voor sterke cliëntauthenticatie en gemeenschappelijke en veilige open communicatiestandaarden (Voor de EER relevante tekst); C/2017/7782; PB L 69 van 13.3.2018, blz. 23. beschikbaar op https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32018R0389&from=NL

vooral op de verwerking van persoonsgegevens door rekeninginformatiedienstaanbieders en betalingsinitiatiedienstaanbieders. In dit document wordt daarom ingegaan op de voorwaarden voor het verlenen van toegang tot rekeninginformatie door rekeninghoudende betalingsdienstaanbieders en voor de verwerking van persoonsgegevens door betalingsinitiatiedienstaanbieders en rekeninginformatiedienstaanbieders, met inbegrip van de vereisten en waarborgen ten aanzien van de verwerking van persoonsgegevens door betalingsinitiatiedienstaanbieders en rekeninginformatiedienstaanbieders voor andere doeleinden dan de doeleinden waarvoor de gegevens oorspronkelijk werden verzameld, in het bijzonder wanneer zij werden verzameld bij het aanbieden van rekeninginformatiediensten[9]. In dit document komen ook verschillende begrippen met betrekking tot uitdrukkelijke toestemming in het kader van de RBD2 en de AVG aan bod, alsook de verwerking van derdengegevens, de verwerking van bijzondere categorieën van persoonsgegevens door betalingsinitiatiedienstaanbieders en rekeninginformatiedienstaanbieders en de toepassing van de belangrijkste beginselen voor gegevensbescherming van de AVG, waaronder gegevensminimalisatie, transparantie, verantwoordingsplicht en beveiligingsmaatregelen. De RBD2 behelst functie-overschrijdende verantwoordelijkheden op het gebied van onder meer consumentenbescherming en mededingingsrecht. Overwegingen ten aanzien van deze rechtsgebieden vallen niet onder deze richtsnoeren.

4. Om de lezing van de richtsnoeren te verbeteren, wordt hieronder een overzicht gegeven van de belangrijkste definities die in dit document zijn gebruikt.

1.1 Definities

“Rekeninginformatiedienstaanbieder”: de aanbieder van een onlinedienst voor het verstrekken van geconsolideerde informatie over een of meer betaalrekeningen die de betalingsdienstgebruiker bij een andere betalingsdienstaanbieder of bij meer dan één betalingsdienstaanbieder aanhoudt;

“rekeninghoudende betalingsdienstaanbieder”: een betalingsdienstaanbieder die ten behoeve van een betaler een betaalrekening aanbiedt en beheert;

“minimale gegevensverwerking”: een beginsel van gegevensverwerking dat inhoudt dat persoonsgegevens toereikend en ter zake dienend moeten zijn en beperkt moeten blijven tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt;

“betaler”: een natuurlijke persoon of rechtspersoon die houder is van een betaalrekening en een betalingstransactie vanaf die betaalrekening toestaat, hetzij, bij ontbreken van een betaalrekening, een natuurlijke persoon of rechtspersoon die een betalingsopdracht geeft;

“begunstigde”: natuurlijke persoon of rechtspersoon die de beoogde uiteindelijke ontvanger is van de geldmiddelen waarop een betalingstransactie betrekking heeft;

“betaalrekening”: een op naam van één of meer betalingsdienstgebruikers aangehouden rekening die voor de uitvoering van betalingstransacties wordt gebruikt;

[9] Een rekeninginformatiedienst is een onlinedienst voor het verstrekken van geconsolideerde informatie over één of meer betaalrekeningen die de betalingsdienstgebruiker bij een andere betalingsdienstaanbieder of bij meer dan één betalingsdienstaanbieder aanhoudt.

“betalingsinitiatiedienstaanbieder”: de aanbieder van een dienst voor het initiëren van een betalingsopdracht, op verzoek van de betalingsdienstgebruiker, met betrekking tot een betaalrekening die bij een andere betalingsdienstaanbieder wordt aangehouden;

“betalingsdienstaanbieder”: een orgaan bedoeld in artikel 1, lid 1, RBD2[10] of een natuurlijke persoon of rechtspersoon aan wie een vrijstelling op grond van artikel 32 of 33 van de RBD2 is verleend;

“betalingsdienstgebruiker”: een natuurlijke persoon of rechtspersoon die in de hoedanigheid van betaler, begunstigde of beide van een betalingsdienst gebruikmaakt;

“persoonsgegevens”: iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (“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;

“gegevensbescherming door ontwerp”: in een product of dienst geïntegreerde technische en organisatorische maatregelen die zijn ontworpen om de beginselen van gegevensbescherming op doeltreffende wijze uit te voeren en om de nodige waarborgen in de verwerking in te bouwen om tegemoet te komen aan de vereisten van de AVG en de rechten van betrokkenen te beschermen;

“gegevensbescherming door standaardinstellingen”: in een product of dienst geïntegreerde passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking;

“technische reguleringsnorm”: Gedelegeerde Verordening (EU) 2018/389 van de Commissie van 27 november 2017 tot aanvulling van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad wat betreft technische reguleringsnormen voor sterke cliëntauthenticatie en gemeenschappelijke en veilige open communicatiestandaarden;

“derde-aanbieder”: zowel betalingsinitiatiedienstaanbieders als rekeninginformatiedienstaanbieders.

[10] In artikel 1, lid 1, RBD2 is bepaald dat bij de RBD2 de voorschriften worden vastgesteld op grond waarvan de lidstaten een onderscheid maken tussen de volgende categorieën van betalingsdienstaanbieders:
a) kredietinstellingen als gedefinieerd in punt 1 van artikel 4, lid 1, van Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad, met inbegrip van bijkantoren ervan zoals gedefinieerd in punt 17 daarvan, indien die bijkantoren zich in de Unie bevinden, ongeacht of de hoofdkantoren van die bijkantoren zich in de Unie of, in overeenstemming met artikel 47 van Richtlijn 2013/36/EU en met het nationale recht, buiten de Unie bevinden;
b) instellingen voor elektronisch geld als gedefinieerd in artikel 2, punt 1, van Richtlijn 2009/110/EG, met inbegrip van, overeenkomstig artikel 8 van die richtlijn en het nationale recht, bijkantoren ervan, ingeval die bijkantoren zich binnen de Unie bevinden en de hoofdkantoren van die bijkantoren buiten de Unie, voor zover de door die bijkantoren aangeboden betalingsdiensten verband houden met de uitgifte van elektronisch geld;
c) postcheque- en girodiensten die krachtens nationale wetgeving gemachtigd zijn om betalingsdiensten aan te bieden;
d) betalingsinstellingen;
e) de ECB en nationale centrale banken wanneer zij niet handelen in hun hoedanigheid van monetaire autoriteit of andere publieke autoriteit;
f) de lidstaten en hun regionale en lokale overheden wanneer zij niet handelen in hun hoedanigheid van overheidsinstantie.

1.2 Diensten in het kader van de RBD2

5. Met de RBD2 zijn twee nieuwe soorten (aanbieders van) betalingsdiensten ingevoerd: betalingsinitiatiedienstaanbieders en rekeninginformatiedienstaanbieders. Bijlage 1 van de RBD2 bevat de acht betalingsdiensten die onder de RBD2 vallen.

6. Betalingsinitiatiedienstaanbieders bieden diensten aan voor het initiëren van een betalingsopdracht, op verzoek van de betalingsdienstgebruiker, met betrekking tot een betaalrekening van de gebruiker die bij een andere betalingsdienstaanbieder wordt aangehouden[11]. Een betalingsinitiatiedienstaanbieder kan een rekeninghoudende betalingsdienstaanbieder (gewoonlijk een bank) verzoeken om een transactie te initiëren namens de betalingsdienstgebruiker. De (betalingsdienst)gebruiker kan een natuurlijke persoon (betrokkene) of een rechtspersoon zijn.

7. Rekeninginformatiedienstaanbieders bieden onlinediensten aan voor het verstrekken van geconsolideerde informatie over een of meer betaalrekeningen die de betalingsdienstgebruiker bij een andere betalingsdienstaanbieder of bij meer dan één betalingsdienstaanbieder aanhoudt[12]. Volgens overweging 28 RBD2 kan de betalingsdienstgebruiker onmiddellijk een overzicht van zijn financiële situatie krijgen.

8. In het kader van rekeninginformatiediensten kunnen er verschillende soorten diensten worden aangeboden, waarbij de nadruk ligt op de verschillende kenmerken en doeleinden. Zo kunnen sommige aanbieders gebruikers diensten aanbieden zoals budgetplanning of uitgavencontrole. De verwerking van persoonsgegevens in het kader van die diensten valt onder de RBD2. Diensten waarbij kredietwaardigheidsbeoordelingen van de betalingsdienstgebruiker komen kijken of controlediensten worden verricht op basis van de verzameling van informatie via een rekeninginformatiedienst, vallen buiten het toepassingsgebied van de RBD2 en vallen daardoor onder de AVG. Andere rekeningen dan betaalrekeningen (bv. spaar- of beleggingsrekeningen) vallen evenmin onder de RBD2. Hoe dan ook geldt de AVG als rechtskader voor de verwerking van persoonsgegevens.

Voorbeeld 1:

HappyPayments is een onderneming die een onlinedienst aanbiedt waarbij informatie over een of meer betaalrekeningen wordt verstrekt via een mobiele app, om zo een financieel overzicht te verschaffen (een rekeninginformatiedienst). Met deze dienst kan de betalingsdienstgebruiker in één oogopslag zijn saldi en recente verrichtingen op twee of meer betaalrekeningen bij verschillende banken bekijken. Wanneer de betalingsdienstgebruiker hiervoor kiest, kan hij uitgaven en inkomsten ook indelen in verschillende categorieën (loon, vrije tijd, energie, hypotheek enz.), wat de betalingsdienstgebruiker helpt bij de financiële planning. Binnen deze app biedt HappyPayments ook een dienst aan om betalingen te initiëren rechtstreeks vanaf de door de gebruiker aangewezen betaalrekening(en) (een betalingsinitiatiedienst).

9. Voor het aanbieden van die diensten zijn in de RBD2 de wettelijke voorwaarden vastgesteld waaronder betalingsinitiatiedienstaanbieders en rekeninginformatiedienstaanbieders toegang kunnen krijgen tot betaalrekeningen om een dienst aan te bieden aan de betalingsdienstgebruiker.

10. In artikel 66, lid 1, en artikel 67, lid 1, RBD2 is bepaald dat de toegang en het gebruik van betalings- en rekeninginformatiediensten het recht zijn van de betalingsdienstgebruiker. Dat betekent dat de

[11] Artikel 4, punt 15, RBD2.
[12] Artikel 4, punt 16, RBD2.

betalingsdienstgebruiker volledig vrij moet zijn om dat recht uit te oefenen en niet kan worden gedwongen er gebruik van te maken.

11. De toegang tot betaalrekeningen en het gebruik van betaalrekeninginformatie zijn gedeeltelijk geregeld in de artikelen 66 en 67 RBD2, die waarborgen bevatten ten aanzien van de bescherming van (persoons)gegevens. In artikel 66, lid 3, punt f), RBD2 is bepaald dat de betalingsinitiatiedienstaanbieder geen gegevens van de betalingsdienstgebruiker vraagt die niet nodig zijn voor het verstrekken van de betalingsinitiatiedienst, en artikel 66, lid 3, punt g), RBD2 luidt dat betalingsinitiatiedienstaanbieders niet overgaan tot het gebruiken, zich toegang verschaffen tot of opslaan van gegevens voor andere doelstellingen dan het verstrekken van de door de betalingsdienstgebruiker uitdrukkelijk gevraagde betalingsinitiatiedienst. Bovendien is de toegang van rekeninginformatiedienstaanbieders volgens artikel 67, lid 2, punt d), RBD2 beperkt tot de informatie van de aangewezen betaalrekeningen en de betrokken betalingstransacties, terwijl in artikel 67, lid 2, punt f), RBD2 is bepaald dat rekeninginformatiedienstaanbieders niet overgaan 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. In dat laatste punt wordt benadrukt dat persoonsgegevens in de context van rekeninginformatiediensten uitsluitend mogen worden verzameld voor specifieke, uitdrukkelijke en rechtmatige doeleinden. Rekeninginformatiedienstaanbieders moeten derhalve uitdrukkelijk in de overeenkomst vermelden voor welk specifiek doel persoonlijke rekeninginformatiegegevens zullen worden verwerkt in het kader van de rekeninginformatiedienst die zij aanbieden. De overeenkomst moet rechtmatig, behoorlijk en transparant zijn overeenkomstig artikel 5 AVG en moet tevens voldoen aan andere wetten inzake consumentenbescherming.

12. Naargelang van de specifieke omstandigheden kunnen betalingsdienstaanbieders verwerkingsverantwoordelijken of verwerkers zijn volgens de AVG. In deze richtsnoeren zijn “verwerkingsverantwoordelijken” betalingsdienstaanbieders die, alleen of samen met anderen, de doeleinden en middelen voor de verwerking van persoonsgegevens bepalen. Nadere informatie hieromtrent is te vinden in EDPB-richtsnoeren 07/2020 inzake de begrippen verwerkingsverantwoordelijke en verwerker in de AVG.

2 RECHTMATIGE GRONDEN EN VERDERE VERWERKING UIT HOOFDE VAN DE RBD2

2.1 Rechtmatige gronden voor verwerking

13. Volgens de AVG moeten de verwerkingsverantwoordelijken een rechtsgrond hebben om persoonsgegevens te verwerken. Artikel 6, lid 1, AVG bevat een volledige, restrictieve lijst van zes rechtsgronden voor de verwerking van persoonsgegevens op grond van de AVG[13]. Het is aan de verwerkingsverantwoordelijke om de passende rechtsgrond te bepalen en te waarborgen dat aan alle voorwaarden voor die rechtsgrond is voldaan. Om te bepalen welke rechtsgrond geldig is en het meest geschikt is in een specifieke situatie, moet worden gekeken naar de omstandigheden waarin de verwerking plaatsvindt, met inbegrip van de verwerkingsdoeleinden en de relatie tussen de verwerkingsverantwoordelijke en de betrokkene.

2.2 Artikel 6, lid 1, punt b), AVG (verwerking is noodzakelijk voor de uitvoering van een overeenkomst)

14. Betalingsdiensten worden verricht op basis van een overeenkomst tussen de betalingsdienstgebruiker en de betalingsdienstaanbieder. Zoals in overweging 87 RBD2 is vermeld, "[dient] deze richtlijn [...] alleen betrekking te hebben op contractuele verplichtingen en aansprakelijkheden tussen de betalingsdienstgebruiker en de betalingsdienstaanbieder". In termen van de AVG is de belangrijkste rechtsgrondslag voor de verwerking van persoonsgegevens voor het aanbieden van betalingsdiensten artikel 6, lid 1, punt b), AVG, wat betekent dat de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.

15. De betalingsdiensten die onder de RBD2 vallen, zijn gedefinieerd in bijlage 1 bij de RBD2. Het aanbieden van die diensten zoals gedefinieerd in de RBD2 is een vereiste voor het vaststellen van een overeenkomst uit hoofde waarvan de partijen toegang krijgen tot betaalrekeninggegevens van

[13] Volgens artikel 6 is de verwerking alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:

(a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;

(b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;

(c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;

(d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;

(e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;

(f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

de betalingsdienstgebruiker. Deze betalingsdienstaanbieders moeten ook vergunninghoudende marktdeelnemers zijn. Wat betalingsinitiatiediensten en rekeninginformatiediensten in het kader van de RBD2 betreft, kunnen overeenkomsten ook bepalingen bevatten waarmee voorwaarden worden opgelegd met betrekking tot aanvullende diensten die niet in de RBD2 zijn geregeld. In EDPB-richtsnoeren 2/2019 betreffende de verwerking van persoonsgegevens op grond van artikel 6, lid 1, onder b), van de AVG in het kader van de verlening van onlinediensten aan betrokkenen is duidelijk gesteld dat verwerkingsverantwoordelijken moeten beoordelen welke verwerking van persoonsgegevens objectief noodzakelijk is om de overeenkomst uit te voeren. In deze richtsnoeren wordt erop gewezen dat de rechtvaardiging van de noodzaak afhankelijk is van de aard van de dienst, de wederzijdse perspectieven en verwachtingen van de partijen bij de overeenkomst, de rationale van de overeenkomst en de essentiële elementen van de overeenkomst.

16. In EDPB-richtsnoeren 2/2019 is ook duidelijk vermeld dat in het licht van artikel 7, lid 4, AVG een onderscheid wordt gemaakt tussen verwerkingsactiviteiten die noodzakelijk zijn voor de uitvoering van een overeenkomst en bepalingen die bepaalde verwerkingsactiviteiten die feitelijk niet noodzakelijk zijn voor de uitvoering van de overeenkomst, als voorwaarde stellen voor de dienst. "Noodzakelijk voor de uitvoering" vereist duidelijk meer dan een contractuele voorwaarde[14]. De verwerkingsverantwoordelijke moet kunnen aantonen hoe het belangrijkste onderwerp van de specifieke overeenkomst met de betrokkene feitelijk niet kan worden uitgevoerd als de specifieke verwerking van de betreffende persoonsgegevens niet plaatsvindt. Slechts de verwijzing of vermelding van gegevensverwerking in een overeenkomst is niet voldoende om de betreffende verwerking te laten vallen binnen de reikwijdte van artikel 6, lid 1, punt b), AVG.

17. In artikel 5, lid 1, punt b), AVG is het beginsel van doelbinding vastgelegd, dat inhoudt dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en niet verder mogen worden verwerkt op een met die doeleinden onverenigbare wijze. Bij de beoordeling of artikel 6, lid 1, punt b), een geschikte rechtsgrondslag is voor verwerking in het kader van een online(betalings)dienst, moet worden gekeken naar het specifieke doel, het doeleinde of de doelstelling van de dienst[15]. De doeleinden van de verwerking moeten duidelijk worden gespecificeerd en meegedeeld aan de betrokkene, in overeenstemming met de verplichtingen van de verwerkingsverantwoordelijke op het gebied van doelbinding en transparantie. Voor de beoordeling van wat "noodzakelijk" is, moet een gecombineerde, op feiten gebaseerde beoordeling van de verwerking "voor het beoogde doeleinde, en of deze minder indringend is in vergelijking met andere opties voor het bereiken van hetzelfde doel" worden uitgevoerd. Artikel 6, lid 1, punt b), is niet van toepassing op verwerking die nuttig is, maar niet objectief gezien noodzakelijk voor de uitvoering van een contractuele dienst of voor het op verzoek van de betrokkene nemen van maatregelen vóór de sluiting van de overeenkomst, zelfs als dit noodzakelijk is voor de andere zakelijke doeleinden van de verwerkingsverantwoordelijke[16].

18. Uit EDPB-richtsnoeren 2/2019 blijkt duidelijk dat een overeenkomst de categorieën van persoonsgegevens of de soorten verwerkingsactiviteiten die de verwerkingsverantwoordelijke moet uitvoeren voor de uitvoering van de overeenkomst in de zin van artikel 6, lid 1, punt b), niet kunstmatig kan uitbreiden[17]. In deze richtsnoeren wordt ook ingegaan op gevallen waarin situaties

[14] Richtsnoeren 2/2019 betreffende de verwerking van persoonsgegevens op grond van artikel 6, lid 1, onder b), van de AVG in het kader van de verlening van onlinediensten aan betrokkenen, EDPB, blz. 8.
[15] Idem.
[16] Idem, bladzijde 9.
[17] Idem, bladzijde 11.

ontstaan waarbij betrokkenen moeten instemmen met de gehele bundel, terwijl ze mogelijk slechts geïnteresseerd zijn in een van de diensten. Dat kan gebeuren wanneer een verwerkingsverantwoordelijke verschillende afzonderlijke diensten of elementen van een dienst met verschillende wezenlijke doelstellingen, functies of rationales wil bundelen in één overeenkomst. Wanneer de overeenkomst bestaat uit verschillende afzonderlijke diensten of elementen van een dienst die feitelijk redelijkerwijs ook onafhankelijk van elkaar kunnen worden uitgevoerd, moet de toepasselijkheid van artikel 6, lid 1, punt b), worden beoordeeld in het kader van elk van deze diensten afzonderlijk, waarbij wordt gekeken naar wat objectief gezien noodzakelijk is voor de uitvoering van elk van de afzonderlijke diensten waarom de betrokkene actief heeft verzocht of waarvoor hij zich actief heeft aangemeld[18].

19. In overeenstemming met bovengenoemde richtsnoeren moeten de verwerkingsverantwoordelijken beoordelen wat objectief noodzakelijk is om de overeenkomst uit te voeren. Wanneer verwerkingsverantwoordelijken niet kunnen aantonen dat de verwerking van de persoonsgegevens objectief noodzakelijk is voor de verlening van elk van deze diensten afzonderlijk, is artikel 6, lid 1, punt b), AVG geen geldige rechtsgrond voor verwerking. In die gevallen moet de verwerkingsverantwoordelijke een andere rechtsgrond voor verwerking overwegen.

2.3 Fraudepreventie

20. In artikel 94, lid 1, RBD2 is bepaald dat de lidstaten toestaan dat betalingssystemen en betalingsdienstaanbieders persoonsgegevens verwerken wanneer zulks noodzakelijk is voor de voorkoming van, het onderzoek naar en de opsporing van betalingsfraude. De verwerking van persoonsgegevens die strikt noodzakelijk is voor fraudepreventie is ook een gerechtvaardigd belang van de verwerkingsverantwoordelijke in kwestie, voor zover die belangen niet ondergeschikt zijn aan de belangen of fundamentele rechten en vrijheden van de betrokkene[19]. Verwerkingsactiviteiten met het oog op fraudepreventie moeten gebaseerd zijn op een zorgvuldige beoordeling per geval door de verwerkingsverantwoordelijke, in overeenstemming met het verantwoordingsbeginsel. Daarnaast kunnen verwerkingsverantwoordelijken, om fraude te voorkomen, ook worden onderworpen aan specifieke wettelijke verplichtingen die de verwerking van persoonsgegevens noodzakelijk maken.

2.4 Verdere verwerking (AISP en PISP)

21. In artikel 6, lid 4, AVG zijn de voorwaarden bepaald voor de verwerking van persoonsgegevens voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld. Dergelijke verdere verwerking mag meer specifiek plaatsvinden wanneer zij berust op een Unierechtelijke bepaling of een lidstaatrechtelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van de in artikel 23, lid 1, bedoelde doelstellingen, wanneer de betrokkene zijn toestemming heeft gegeven of wanneer de verwerking voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld niet onverenigbaar met de oorspronkelijke doeleinden is.

22. Er moet terdege rekening worden gehouden met artikel 66, lid 3, punt g), en artikel 67, lid 2, punt f), RBD2. Zoals hierboven vermeld, is in artikel 66, lid 3, punt f), RBD2 bepaald dat de betalingsinitiatiedienstaanbieder niet overgaat 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. In artikel 67, lid 2, punt f), RBD2 is bepaald dat de

[18] Idem, bladzijde 13.
[19] Overweging 47 AVG.

rekeninginformatiedienstaanbieder 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.

23. Bijgevolg worden de mogelijkheden voor verwerking voor andere doeleinden bij artikel 66, lid 3, punt g), en artikel 67, lid 2, punt f), RBD2 aanzienlijk beperkt, wat betekent dat verwerking voor een ander doel niet is toegestaan tenzij de betrokkene toestemming heeft gegeven overeenkomstig artikel 6, lid 1, punt a), AVG of de verwerking is vastgelegd in het Unierecht of het recht van de lidstaat waaraan de verwerkingsverantwoordelijke is onderworpen, overeenkomstig artikel 6, lid 4, AVG. Wanneer de verwerking voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld niet berust op de toestemming van de betrokkene of een Unierechtelijke of lidstaatrechtelijke bepaling, blijkt uit de in artikel 66, lid 3, punt g), en artikel 67, lid 2, punt f), RBD2 vastgelegde beperkingen duidelijk dat andere doelen niet verenigbaar zijn met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld. De verenigbaarheidstoets van artikel 6, punt 4, AVG kan geen aanleiding geven tot een rechtsgrond voor verwerking.

24. Artikel 6, lid 4, AVG biedt de mogelijkheid tot verdere verwerking op grond van het Unierecht of het recht van de lidstaat. Zo zijn alle betalingsinitiatiedienstaanbieders en rekeninginformatiedienstaanbieders meldingsplichtige entiteiten in de zin van artikel 3, lid 2, punt a), van Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering. Die meldingsplichtige entiteiten zijn derhalve verplicht cliëntenonderzoeksmaatregelen toe te passen zoals bepaald in de richtlijn. De persoonsgegevens die in verband met een RBD2-dienst worden verwerkt, worden derhalve verder verwerkt op basis van ten minste één wettelijke verplichting die op de dienstaanbieder rust[20].

25. Zoals vermeld in punt 20 is in artikel 6, lid 4, AVG bepaald dat de verwerking voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld, kan berusten op de toestemming van de betrokkene, indien aan alle voorwaarden voor toestemming uit hoofde van de AVG is voldaan. Zoals hierboven uiteengezet, moet de verwerkingsverantwoordelijke aantonen dat het mogelijk is toestemming te weigeren of in te trekken zonder nadelige gevolgen (overweging 42 AVG).

2.5 Rechtmatige grond voor het verlenen van toegang tot de rekening (rekeninghoudende betalingsdienstaanbieders)

26. Zoals vermeld in punt 10 kunnen betalingsdienstgebruikers hun recht uitoefenen om gebruik te maken van betalingsinitiatie- en rekeninginformatiediensten. De bij artikel 66, lid 1, en artikel 67, lid 1, RBD2 aan de lidstaten opgelegde verplichtingen moeten in het interne recht worden omgezet om te waarborgen dat het recht van de betalingsdienstgebruiker om van de bovengenoemde betalingsdiensten te profiteren, daadwerkelijk wordt toegepast. De daadwerkelijke toepassing van dat recht zou niet mogelijk zijn zonder het bestaan van een overeenkomstige verplichting voor de rekeninghoudende betalingsdienstaanbieders, gewoonlijk een bank, om de betalingsdienstaanbieder toegang te bieden tot de rekening, op voorwaarde dat de betalingsdienstaanbieder aan alle vereisten heeft voldaan om toegang te krijgen tot de rekening van de betalingsdienstgebruiker. Voorts is in artikel 66, lid 5, en artikel 67, lid 4, RBD2 duidelijk bepaald dat het aanbieden van betalingsinitiatiediensten en van rekeninginformatiediensten niet mag afhangen van het bestaan van een contractuele relatie tussen de

[20] Er zij op gewezen dat een grondig onderzoek van de vraag of de antiwitwasrichtlijn voldoet aan de norm van artikel 6, lid 4, AVG buiten het toepassingsgebied van dit document valt.

betalingsinitiatiedienstaanbieders/rekeninginformatiedienstaanbieders en de rekeninghoudende betalingsdienstaanbieders.

27. De verwerking van persoonsgegevens door de rekeninghoudende betalingsdienstaanbieders, waarbij toegang wordt verleend tot de door de betalingsinitiatiedienstaanbieder en rekeninginformatiedienstaanbieder gevraagde persoonsgegevens opdat zij hun betalingsdiensten aan de betalingsdienstgebruiker kunnen verlenen, berust op een wettelijke verplichting. Om de doelstellingen van de RBD2 te verwezenlijken, moeten rekeninghoudende betalingsdienstaanbieders de persoonsgegevens voor de diensten van de betalingsinitiatiedienstaanbieders en rekeninginformatiedienstaanbieders verstrekken, als noodzakelijke voorwaarde opdat de betalingsinitiatiedienstaanbieders en rekeninginformatiedienstaanbieders hun diensten kunnen verlenen en zo de in artikel 66, lid 1, en artikel 67, lid 1, RBD2 vastgelegde rechten kunnen waarborgen. De toepasselijke rechtsgrond is in dit geval dus artikel 6, lid 1, punt c), AVG.

28. Aangezien in de AVG is bepaald dat verwerking op basis van een wettelijke verplichting duidelijk moet zijn vastgelegd bij het Unierecht of het lidstatelijk recht (zie artikel 6, lid 3, AVG), moet de verplichting voor de rekeninghoudende betalingsdienstaanbieders om toegang te verlenen voortvloeien uit de nationale wetgeving tot omzetting van de RBD2.

3 UITDRUKKELIJKE TOESTEMMING

3.1 Toestemming op grond van de AVG

29. Volgens de AVG is toestemming een van de zes rechtsgronden voor de rechtmatigheid van de verwerking van persoonsgegevens. In artikel 4, punt 11, AVG is toestemming gedefinieerd als "elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt". Deze vier voorwaarden — vrij, specifiek, geïnformeerd en ondubbelzinnig — zijn van essentieel belang voor de geldigheid van de toestemming. Volgens EDPB-richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679 kan toestemming alleen een passende rechtsgrond zijn als een betrokkene controle kan uitoefenen en echt een keuze heeft met betrekking tot het accepteren of afwijzen van de aangeboden voorwaarden of het afwijzen ervan zonder nadeel. Wanneer de verwerkingsverantwoordelijke om toestemming verzoekt, heeft hij de plicht om na te gaan of aan alle vereisten voor het verkrijgen van geldige toestemming is voldaan. Indien de toestemming geheel overeenkomstig de AVG wordt verkregen, is toestemming een instrument dat de betrokkenen controle geeft over het al dan niet verwerken van hun persoonsgegevens. Indien dit niet het geval is, is deze controle van de betrokkene slechts schijn, en geen geldige grond voor verwerking, waardoor de verwerkingsactiviteiten onrechtmatig worden[21].

30. De AVG bevat ook verdere waarborgen in artikel 7, waarin is bepaald dat de verwerkingsverantwoordelijke moet kunnen aantonen dat er ten tijde van de verwerking geldige toestemming was gegeven. Het verzoek om toestemming moet ook in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal zodanig gepresenteerd zijn dat een duidelijk onderscheid kan worden gemaakt met de andere aangelegenheden. De betrokkene moet voorts in kennis worden gesteld van zijn recht zijn toestemming te allen tijde even eenvoudig in te trekken als zij werd gegeven.

31. Volgens artikel 9 AVG is toestemming een van de uitzonderingen op het algemene verbod op de verwerking van bijzondere categorieën van persoonsgegevens. In dergelijke gevallen moet de toestemming van de betrokkene echter "uitdrukkelijk" zijn[22].

32. Volgens de EDPB-richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679 verwijst de term "uitdrukkelijk" naar de manier waarop toestemming door de betrokkene tot uitdrukking wordt gebracht. Het betekent dat de betrokkene een uitdrukkelijke verklaring van toestemming voor specifieke verwerkingsdoeleinden moet geven. Een voor de hand liggende manier om ervoor te zorgen dat toestemming uitdrukkelijk is, is het uitdrukkelijk bevestigen van toestemming in een schriftelijke verklaring. In voorkomende gevallen zou de verwerkingsverantwoordelijke ervoor kunnen zorgen dat de schriftelijke verklaring door de betrokkene wordt ondertekend, om elke mogelijke twijfel en mogelijk gebrek aan bewijs in de toekomst te voorkomen.

33. Uit potentieel dubbelzinnige verklaringen of handelingen kan in geen geval toestemming worden afgeleid. Een verwerkingsverantwoordelijke moet zich er ook van bewust zijn dat toestemming

[21] Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679, EDPB, punt 3.
[22] Zie ook Advies 15/2011 over de definitie van "toestemming" (WP 187), blz. 6-8, en/of Advies 06/2014 over het begrip "gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke" in artikel 7 van Richtlijn 95/46/EG (WP 217), blz. 9, 10, 13 en 14.

niet kan worden verkregen door middel van dezelfde handeling als die voor het instemmen met een overeenkomst of het aanvaarden van algemene voorwaarden van een dienst.

3.2 Toestemming onder de PSD2

34. Het EDPB merkt op dat het rechtskader inzake uitdrukkelijke toestemming complex is, aangezien zowel de RBD2 als de AVG het begrip "uitdrukkelijke toestemming" bevatten. Dat leidt tot de vraag of "uitdrukkelijke toestemming" zoals vermeld in artikel 94, lid 2, RBD2 op dezelfde manier moet worden uitgelegd als uitdrukkelijke toestemming op grond van de AVG.

3.2.1 Uitdrukkelijke toestemming op grond van artikel 94, lid 2, RBD2

35. De RBD2 bevat een aantal specifieke regels voor de verwerking van persoonsgegevens, met name in artikel 94, lid 1, RBD2, waarin is bepaald dat de verwerking van persoonsgegevens voor de bij de RBD2 beoogde doeleinden moeten stroken met het gegevensbeschermingsrecht van de EU. Voorts is in artikel 94, lid 2, RBD2 bepaald dat betalingsdienstaanbieders alleen met de uitdrukkelijke toestemming van de betalingsdienstgebruiker toegang mogen krijgen tot persoonsgegevens die noodzakelijk zijn voor het aanbieden van hun betalingsdiensten, en deze mogen verwerken en bewaren. Volgens artikel 33, lid 2, RBD2 geldt dit vereiste van uitdrukkelijke toestemming van de betalingsdienstgebruiker niet voor rekeninginformatiedienstaanbieders. In artikel 67, lid 2, punt a), RBD2 is evenwel nog steeds voorzien in uitdrukkelijke toestemming voor rekeninginformatiedienstaanbieders voor het verrichten van de dienst.

36. Zoals hierboven vermeld is de lijst van rechtmatige gronden voor verwerking op grond van de AVG uitputtend. Zoals vermeld in punt 14 is de rechtsgrond voor de verwerking van persoonsgegevens voor de verlening van betalingsdiensten in principe artikel 6, lid 1, punt b), AVG, wat betekent dat de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen. Daaruit volgt dat artikel 94, lid 2, RBD2 niet mag worden beschouwd als een aanvullende rechtsgrond voor de verwerking van persoonsgegevens. Het EDPB is van mening dat dit lid, gelet op het voorgaande, moet worden gelezen in samenhang met het toepasselijke rechtskader inzake gegevensbescherming en wel op zodanige wijze dat het nuttig effect ervan behouden blijft. Uitdrukkelijke toestemming op grond van artikel 94, lid 2, RBD2 moet derhalve worden beschouwd als een aanvullende eis van contractuele aard[23] in verband met de toegang tot en daaropvolgende verwerking en opslag van persoonsgegevens voor het verlenen van betalingsdiensten en is derhalve niet hetzelfde als (uitdrukkelijke) toestemming in het kader van de AVG.

37. De "uitdrukkelijke toestemming" waarvan sprake in artikel 94, lid 2, RBD2 is een contractuele toestemming. Dat houdt in dat artikel 94, lid 2, RBD2 aldus moet worden uitgelegd dat betrokkenen bij het aangaan van een overeenkomst met een betalingsdienstaanbieder op grond van de RBD2 volledig in kennis moeten worden gesteld van de specifieke categorieën persoonsgegevens die zullen worden verwerkt. Bovendien moeten zij in kennis worden gesteld van het specifieke doeleinde (de betalingsdienst) waarvoor hun persoonsgegevens zullen worden verwerkt en moeten zij uitdrukkelijk akkoord gaan met deze bedingen. Dergelijke bepalingen moeten duidelijk te onderscheiden zijn van de andere aangelegenheden die in de overeenkomst aan bod komen en moeten uitdrukkelijk worden aanvaard door de betrokkene.

[23] Brief van het EDPB over de PSD2-richtlijn van 5 juli 2018, blz. 4.

38. Centraal in het begrip “uitdrukkelijke toestemming” op grond van artikel 94, lid 2, RBD2 staat het verkrijgen van toegang tot persoonsgegevens om die gegevens vervolgens te verwerken en op te slaan met het oog op het aanbieden van betalingsdiensten. Dat houdt in dat de betalingsdienstaanbieder[24] de persoonsgegevens nog niet verwerkt, maar toegang moet hebben tot persoonsgegevens die zijn verwerkt onder de verantwoordelijkheid van een andere verwerkingsverantwoordelijke. Indien een betalingsdienstgebruiker een overeenkomst aangaat met bijvoorbeeld een betalingsinitiatiedienstaanbieder, moet die aanbieder toegang krijgen tot persoonsgegevens van de betalingsdienstgebruiker die worden verwerkt onder de verantwoordelijkheid van de rekeninghoudende betalingsdienstaanbieder. Het voorwerp van de uitdrukkelijke toestemming op grond van artikel 94, lid 2, RBD2 is de toelating om toegang te krijgen tot die persoonsgegevens, teneinde die persoonsgegevens te kunnen verwerken en opslaan die nodig zijn om de betalingsdienst te verlenen. Indien de betrokkene uitdrukkelijke toestemming geeft, is de rekeninghoudende betalingsdienstaanbieder verplicht om toegang te verschaffen tot de vermelde persoonsgegevens.

39. Hoewel de toestemming uit artikel 94, lid 2, RBD2 geen rechtsgrond is voor de verwerking van persoonsgegevens, houdt deze toestemming specifiek verband met persoonsgegevens en gegevensbescherming en waarborgt zij de transparantie en een zekere mate van controle voor de betalingsdienstgebruiker[25]. Hoewel de materiële voorwaarden voor toestemming op grond van artikel 94, lid 2, RBD2 niet worden gespecificeerd in de RBD2, moet zij, zoals hierboven vermeld, worden gezien in samenhang met het toepasselijke rechtskader inzake gegevensbescherming en op zodanige wijze dat het nuttige effect ervan behouden blijft.

40. Met betrekking tot de door verwerkingsverantwoordelijken te verschaffen informatie en het vereiste van transparantie, is in de Richtsnoeren inzake transparantie van de Groep artikel 29 gespecificeerd dat “een van de kernelementen van het transparantiebeginsel zoals bedoeld in deze bepalingen is dat betrokkenen van tevoren de reikwijdte en de gevolgen van de verwerking moeten kunnen bepalen en later niet verrast worden door andere manieren waarop hun persoonsgegevens zijn gebruikt”[26].

41. Bovendien moeten persoonsgegevens overeenkomstig het beginsel van doelbinding worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (artikel 5, lid 1, punt b), AVG). Wanneer persoonsgegevens voor meer dan één doeleinde worden verzameld, “moeten verwerkingsverantwoordelijken vermijden slechts één breed doel te identificeren om verschillende verdere verwerkingsactiviteiten te rechtvaardigen die in feite slechts losjes verband houden met het eigenlijke oorspronkelijke doel”[27]. Het EDP heeft, laatstelijk in het kader van overeenkomsten voor onlinediensten, gewezen op het risico van het opnemen van algemene verwerkingsbepalingen in overeenkomsten en heeft verklaard dat het doel van de verzameling duidelijk en specifiek moet worden vermeld: deze vermelding moet gedetailleerd genoeg zijn om te kunnen vaststellen welke soorten verwerking wel en niet vallen onder de opgegeven

[24] Dit geldt voor de diensten 1 tot en met 7 van bijlage 1 bij de RBD2.
[25] Artikel 94, lid 2, RBD2 valt onder hoofdstuk 4, “Gegevensbescherming”.
[26] Groep artikel 29, Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679, punt 10 (goedgekeurd op 11 april 2018) - bekrachtigd door het EDPB.
[27] Advies 03/2013 inzake doelbinding (WP203) van de Groep artikel 29, blz. 16.

doelstelling en om de beoordeling van de naleving van de wetgeving en de toegepaste beschermingsmaatregelen op het gebied van gegevensbescherming mogelijk te maken[28].

42. Wanneer beschouwd in de context van het aanvullende vereiste van uitdrukkelijke toestemming op grond van artikel 94, lid 2, RBD2, betekent dit dat verwerkingsverantwoordelijken betrokkenen specifieke en uitdrukkelijke informatie moeten verschaffen over de specifieke door de verwerkingsverantwoordelijke vastgestelde doeleinden waarvoor hun persoonsgegevens worden geraadpleegd, verwerkt en bewaard. Overeenkomstig artikel 94, lid 2, RBD2 moeten de betrokkenen deze specifieke doeleinden uitdrukkelijk aanvaarden.

43. Zoals hierboven in punt 10 is uiteengezet, wijst het EDPB er bovendien op dat de betalingsdienstgebruiker moet kunnen kiezen of hij al dan niet van de dienst gebruik wil maken en daartoe niet kan worden gedwongen. De toestemming op grond van artikel 94, lid 2, RBD2 moet dan ook een vrijelijk verleende toestemming zijn.

3.3 Conclusie

44. Uitdrukkelijke toestemming op grond van de RBD2 verschilt van de (uitdrukkelijke) toestemming op grond van de AVG. Uitdrukkelijke toestemming op grond van artikel 94, lid 2, RBD2 is een aanvullend vereiste van contractuele aard. Wanneer een betalingsdienstaanbieder voor het verlenen van een betalingsdienst toegang moet krijgen tot persoonsgegevens, is uitdrukkelijke toestemming van de betalingsdienstgebruiker overeenkomstig artikel 94, lid 2, RBD2 vereist.

[28] Richtsnoeren 2/2019 betreffende de verwerking van persoonsgegevens op grond van artikel 6, lid 1, onder b), van de AVG in het kader van de verlening van onlinediensten aan betrokkenen, punt 16, (versie ter openbare raadpleging) en Advies 03/2013 inzake doelbinding (WP203) van de Groep artikel 29, blz. 15-16.

4 VERWERKING VAN DERDENGEGEVENS

4.1 Derdengegevens

45. Een kwestie met betrekking tot gegevensbescherming die zorgvuldig moet worden bekeken, is de verwerking van zogeheten “derdengegevens”. In de context van dit document zijn derdengegevens persoonsgegevens met betrekking tot een betrokkene die niet de gebruiker is van een specifieke betalingsdienstaanbieder, maar wiens persoonsgegevens door die specifieke betalingsdienstaanbieder worden verwerkt voor de uitvoering van een overeenkomst tussen de aanbieder en de betalingsdienstgebruiker. Dat is bijvoorbeeld het geval wanneer een betalingsdienstgebruiker, betrokkene A, gebruikmaakt van de diensten van een rekeninginformatiedienstaanbieder en betrokkene B een reeks betalingstransacties naar de betaalrekening van betrokkene A heeft verricht. In dat geval wordt betrokkene B beschouwd als de “derde” en worden de persoonsgegevens (zoals het rekeningnummer van betrokkene B en het geldbedrag dat bij deze transacties betrokken was) met betrekking tot betrokkene B beschouwd als derdengegevens.

4.2 Het gerechtvaardigde belang van de verwerkingsverantwoordelijke

46. In artikel 5, lid 1, punt b), AVG is voorgeschreven dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verzameld en vervolgens niet verder op een met die doeleinden onverenigbare wijze mogen worden verwerkt. Daarnaast schrijft de AVG voor dat elke verwerking zowel noodzakelijk als evenredig moet zijn en in overeenstemming moet zijn met de beginselen inzake gegevensbescherming, zoals de beginselen inzake doelbinding en gegevensminimalisatie.

47. De AVG kan de verwerking van derdengegevens toelaten wanneer de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde (artikel 6, lid 1, punt f), AVG). Dergelijke verwerking kan echter alleen plaatsvinden wanneer “de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen niet zwaarder wegen” dan het gerechtvaardigde belang van de verwerkingsverantwoordelijke.

48. Een rechtmatige basis voor de verwerking van derdengegevens door betalingsinitiatiedienstaanbieders en rekeninginformatiedienstaanbieders — in de context van de verlening van betalingsdiensten in het kader van de RBD2 — zou dus het gerechtvaardigde belang van een verwerkingsverantwoordelijke of een derde om de overeenkomst met de betalingsdienstgebruiker uit te voeren kunnen zijn. De noodzaak om persoonsgegevens van de derde te verwerken is beperkt en wordt bepaald door de redelijke verwachtingen van die betrokkenen. In het kader van het aanbieden van betalingsdiensten die onder de RBD2 vallen, moeten er doeltreffende en passende maatregelen worden vastgesteld om te waarborgen dat de belangen of fundamentele rechten en vrijheden van de derden niet moeten wijken voor andere belangen en om ervoor te zorgen dat de redelijke verwachtingen van die betrokkenen ten aanzien van de verwerking van hun persoonsgegevens worden geëerbiedigd. In dat verband moet de verwerkingsverantwoordelijke (de rekeninginformatiedienstaanbieder of betalingsinitiatiedienstaanbieder) de nodige waarborgen voor de verwerking vaststellen om de rechten van de betrokkenen te beschermen. Dat omvat technische maatregelen om ervoor te zorgen dat derdengegevens niet worden verwerkt voor andere doeleinden dan die waarvoor de persoonsgegevens aanvankelijk werden verzameld door de betalingsinitiatiedienstaanbieders en de rekeninginformatiedienstaanbieders. Indien mogelijk moeten ook versleutelings- of andere

technieken worden toegepast om een passend niveau van beveiliging en minimale gegevensverwerking te bereiken.

4.3 Verdere verwerking van persoonsgegevens van de derde

49. Zoals vermeld in punt 29 kunnen persoonsgegevens in verband met een door de RBD2 geregelde betalingsdienst verder worden verwerkt op basis van wettelijke verplichtingen van de dienstverlener. Die wettelijke verplichtingen kunnen betrekking hebben op persoonsgegevens van de derde.

50. Wat de verdere verwerking van derdengegevens op basis van het gerechtvaardigde belang betreft, is het EDPB van mening dat deze gegevens niet mogen worden gebruikt voor andere doeleinden dan die waarvoor de persoonsgegevens zijn verzameld, tenzij op basis van het EU-recht of het lidstatelijk recht. Het is juridisch niet haalbaar om toestemming te krijgen van de derde omdat om deze toestemming te verkrijgen, persoonsgegevens van de derde zouden moeten worden verzameld of verwerkt, waarvoor geen rechtsgrond te vinden is in artikel 6 AVG. De verenigbaarheidstoets van artikel 6, lid 4, AVG kan evenmin een grond vormen voor de verwerking voor andere doeleinden (zoals direct-marketingactiviteiten). De rechten en vrijheden van deze derde betrokkenen worden niet geëerbiedigd indien de nieuwe verwerkingsverantwoordelijke de persoonsgegevens voor andere doeleinden gebruikt, gezien de context waarin de persoonsgegevens zijn verzameld, in het bijzonder het feit dat er geen relatie bestaat met de betrokkenen die derde partij zijn[29]; het ontbreken van enig verband tussen enig ander doeleinde en het doeleinde waarvoor de persoonsgegevens aanvankelijk zijn verzameld (het feit dat betalingsdienstaanbieders de derdengegevens slechts nodig hebben om een overeenkomst met de andere overeenkomstsluitende partij uit te voeren); de aard van de betrokken persoonsgegevens[30], de omstandigheid dat betrokkenen redelijkerwijs geen verdere verwerking kunnen verwachten of zelfs maar op de hoogte kunnen zijn van welke verwerkingsverantwoordelijke hun persoonsgegevens zou kunnen verwerken en gezien de in artikel 66, lid 3, punt g), en artikel 67, lid 2, punt f), RBD2 beschreven wettelijke beperkingen voor de verwerking.

[29] In overweging 87 RBD2 staat dat de RBD2 alleen betrekking heeft op “contractuele verplichtingen en aansprakelijkheden tussen de betalingsdienstgebruiker en de betalingsdienstaanbieder”. Derdengegevens vallen derhalve niet onder de RBD2.

[30] Aangezien de verwerking volgens de richtsnoeren voor gegevensbeschermingseffectbeoordelingen kan worden geacht het potentiële risico voor de rechten en vrijheden van personen te verhogen is bijzondere zorg vereist bij de verwerking van financiële persoonsgegevens.

5 DE VERWERKING VAN BIJZONDERE CATEGORIEËN VAN PERSOONSGEGEVENS IN HET KADER VAN DE RBD2

5.1 Bijzondere categorieën van persoonsgegevens

51. Artikel 9, lid 1, AVG verbiedt de verwerking van "persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele geaardheid".

52. Het moet worden benadrukt dat elektronische betalingen in sommige lidstaten al alomtegenwoordig zijn en dat veel mensen deze wijze van betalen bij hun dagelijkse transacties reeds verkiezen boven contant geld. Tegelijkertijd kunnen financiële transacties gevoelige informatie over een individuele betrokkene onthullen, waaronder informatie die verband houdt met bijzondere categorieën van persoonsgegevens. Naargelang van de details van de transactie, kunnen bijvoorbeeld politieke opvattingen of godsdienstige overtuigingen worden onthuld door schenkingen aan politieke partijen of organisaties, kerken of parochies. Het lidmaatschap van een vakbond kan blijken uit het feit dat een jaarlijkse lidmaatschapsbijdrage van iemands bankrekening wordt afgeboekt. Persoonsgegevens met betrekking tot de gezondheid kunnen worden verzameld door de facturen voor medische behandelingen die een betrokkene aan een arts heeft betaald (bijvoorbeeld aan een psychiater), te analyseren. Tot slot kan informatie over bepaalde aankopen informatie over het seksleven of de seksuele geaardheid van een persoon blootgeven. Zoals uit deze voorbeelden blijkt, kan zelfs één enkele transactie bijzondere categorieën van persoonsgegevens bevatten. Bovendien kunnen rekeninginformatiediensten gebruikmaken van profilering zoals gedefinieerd in artikel 4, punt 4, AVG. Zoals eerder vermeld in de Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679 van de Groep artikel 29, zoals bekrachtigd door het EDPB, "[kunnen] via profilering [...] gegevens van bijzondere categorieën worden gecreëerd op basis van gegevens die zelf niet tot bijzondere categorieën van gegevens behoren, maar wel hiertoe gaan behoren wanneer ze met andere gegevens worden gecombineerd"[31]. Dat betekent dat de combinatie van financiële transacties verschillende soorten gedragspatronen kan onthullen, die bijzondere categorieën van persoonsgegevens kunnen bevatten. De kans is dan ook groot dat een dienstverlener die informatie over financiële transacties van betrokkenen verwerkt ook bijzondere categorieën van persoonsgegevens verwerkt.

53. Met betrekking tot de term "gevoelige betalingsgegevens" merkt het EDPB het volgende op. De definitie van gevoelige betalingsgegevens in de RBD2 verschilt aanzienlijk van de manier waarop de term "gevoelige persoonsgegevens" gewoonlijk wordt gebruikt in het kader van de AVG en de gegevensbescherming(swetgeving). Terwijl "gevoelige betalingsgegevens" in de RBD2 worden gedefinieerd als "gegevens waarmee fraude kan worden gepleegd, waaronder persoonlijke beveiligingsgegevens", wordt in de AVG de nadruk gelegd op de noodzaak van specifieke bescherming voor bijzondere categorieën van persoonsgegevens die volgens artikel 9 AVG door hun aard bijzonder gevoelig zijn wat betreft de grondrechten en fundamentele vrijheden, zoals

[31] Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679 van de Groep gegevensbescherming artikel 29, WP251rev.01, blz. 17.

bijzondere categorieën van persoonsgegevens[32]. In dat verband wordt aanbevolen om ten minste het soort persoonsgegevens in kaart te brengen en nauwkeurig in te delen. Naar alle waarschijnlijkheid zal overeenkomstig artikel 35 AVG een gegevensbeschermingseffectbeoordeling vereist zijn, die zal helpen bij het in kaart brengen van het soort persoonsgegevens. Nadere richtsnoeren inzake gegevensbeschermingseffectbeoordeling zijn te vinden in de Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking „waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679 van Groep artikel 29, zoals bekrachtigd door het EDPB.

5.2 Mogelijke uitzonderingsgronden

54. Het verbod van artikel 9 AVG is niet absoluut. Aangezien de uitzonderingsgronden van de punten b) tot en met f) en h) tot en met j) van artikel 9, lid 2, AVG kennelijk niet van toepassing zijn op de verwerking van persoonsgegevens in het kader van de RBD2, zouden in het bijzonder de volgende twee afwijkingen in artikel 9, lid 2, AVG kunnen worden overwogen:

a) Het verbod geldt niet als de betrokkene uitdrukkelijke toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden (artikel 9, lid 2, AVG).

b) Het verbod geldt niet indien de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene (artikel 9, lid 2, punt g), AVG).

55. Er zij op gewezen dat de lijst van uitzonderingsgronden in artikel 9, lid 2, AVG uitputtend is. De mogelijkheid dat bijzondere categorieën van persoonsgegevens onder de persoonsgegevens vallen die worden verwerkt voor het aanbieden van een van de onder de RBD2 vallende diensten, moet door de dienstverlener worden erkend. Aangezien het verbod van artikel 9, lid 1, AVG van toepassing is op deze dienstverleners, moeten zij verzekeren dat een van de uitzonderingen van artikel 9, lid 2, AVG op hen van toepassing is. Er zij op gewezen dat wanneer de dienstverlener niet kan aantonen dat aan een van de afwijkingen is voldaan, het verbod van artikel 9, lid 1, van toepassing is.

5.3 Zwaarwegend algemeen belang

56. Betalingsdiensten mogen bijzondere categorieën van persoonsgegevens verwerken om redenen van zwaarwegend algemeen belang, maar alleen als aan alle voorwaarden van artikel 9, lid 2, punt g), AVG is voldaan. Dat betekent dat de verwerking van de bijzondere categorieën van persoonsgegevens moet worden geregeld in een specifieke afwijking van artikel 9, lid 1, AVG in het Unierecht of het lidstatelijk recht. Die bepaling moet betrekking hebben op de evenredigheid met het nagestreefde doel van de verwerking en moet passende en specifieke maatregelen omvatten om de grondrechten en de fundamentele belangen van de betrokkene te beschermen. De Unierechtelijke of lidstaatrechtelijke bepaling moet bovendien de wezenlijke inhoud van het

[32] In overweging 10 AVG worden bijzondere categorieën van persoonsgegevens bijvoorbeeld aangeduid als "gevoelige gegevens".

recht op bescherming van persoonsgegevens eerbiedigen. Tot slot moet ook worden aangetoond dat de verwerking van de bijzondere categorieën van gegevens noodzakelijk is om redenen van zwaarwegend algemeen belang, waaronder redenen van systemisch belang. Alleen wanneer volledig aan al deze voorwaarden is voldaan, kan deze afwijking van toepassing worden verklaard op aangewezen soorten betalingsdiensten.

5.4 Uitdrukkelijke toestemming

57. In gevallen waarin de afwijking van artikel 9, lid 2, punt g), AVG niet van toepassing is, lijkt het verkrijgen van uitdrukkelijke toestemming overeenkomstig de voorwaarden voor geldige toestemming van de AVG de enige mogelijke rechtmatige uitzonderingsgrond voor derde-aanbieders om bijzondere categorieën van persoonsgegevens te verwerken. In de EDPB-richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679[33] is het volgende vermeld: "Artikel 9, lid 2, erkent "noodzakelijk voor de uitvoering van een overeenkomst" niet als een uitzondering op het algemene verbod op verwerking van bijzondere categorieën gegevens. Daarom moeten verwerkingsverantwoordelijken en lidstaten die met deze situatie te maken krijgen, nagaan of een van de specifieke uitzonderingen in artikel 9, lid 2, onder b) tot en met j), van toepassing is. Wanneer dienstverleners zich beroepen op artikel 9, lid 2, punt a), AVG, moeten zij ervoor zorgen dat hun uitdrukkelijke toestemming is verleend voordat zij met de verwerking beginnen." Uitdrukkelijke toestemming zoals beschreven in artikel 9, lid 2, punt a), AVG moet aan alle vereisten van de AVG voldoen.

5.5 Geen passende uitzonderingsgrond

58. Wanneer de dienstverlener niet kan aantonen dat aan een van de afwijkingen is voldaan, is het verbod van artikel 9, lid 1, van toepassing, zoals hierboven vermeld. In dit geval kunnen er technische maatregelen worden getroffen om de verwerking van bijzondere categorieën van persoonsgegevens te voorkomen, bijvoorbeeld door de verwerking van bepaalde gegevenspunten te voorkomen. In dat verband kunnen betalingsdienstaanbieders de technische mogelijkheden onderzoeken om bijzondere categorieën van persoonsgegevens uit te sluiten en specifieke toegang toe te staan die de verwerking door derde-aanbieders van bijzondere categorieën van persoonsgegevens met betrekking tot derden zou voorkomen.

[33] Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679, EDPB, punt 99.

6 MINIMALE GEGEVENSVERWERKING, BEVEILIGING, TRANSPARANTIE, VERANTWOORDINGSPLICHT EN PROFILERING

6.1 Minimale gegevensverwerking en gegevensbescherming door ontwerp en door standaardinstellingen

59. Het beginsel van minimale gegevensverwerking is vastgelegd in artikel 5, lid 1, punt c), AVG: "Persoonsgegevens moeten [...] toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt". Volgens het beginsel van minimale gegevensverwerking mogen verwerkingsverantwoordelijken in wezen niet meer persoonsgegevens verwerken dan nodig om de specifieke doeleinden in kwestie te verwezenlijken. Zoals opgemerkt in hoofdstuk 2 worden de hoeveelheid en de aard van de persoonsgegevens die nodig zijn om de betalingsdienst te verlenen bepaald door te verwijzen naar de belangrijkste en wederzijds begrepen doelstelling van de overeenkomst[34]. Minimale gegevensverwerking geldt voor elke verwerking (bv. elke verzameling van of raadpleging en opvraging van persoonsgegevens). In EDPB-richtsnoeren 4/2019 inzake artikel 25 — Gegevensbescherming door ontwerp en door standaardinstellingen, staat te lezen dat "verwerkers en technologieaanbieders ook worden erkend als belangrijke spelers om gegevensbescherming door ontwerp en door standaardinstellingen mogelijk te maken en dat zij zich ook bewust moeten zijn van het feit dat verwerkingsverantwoordelijken verplicht zijn om persoonsgegevens uitsluitend te verwerken met behulp van systemen en technologieën die over ingebouwde gegevensbescherming beschikken"[35].

60. Artikel 25 AVG bevat de verplichtingen om gegevensbescherming door ontwerp en door standaardinstellingen toe te passen. Die verplichtingen zijn van bijzonder belang voor het beginsel van minimale gegevensverwerking. In dit artikel is bepaald dat verwerkingsverantwoordelijke, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen treft, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van de AVG en ter bescherming van de rechten van de betrokkenen. De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om ervoor te zorgen dat er in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Die verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen en de toegankelijkheid daarvan. Deze maatregelen kunnen versleuteling, pseudonimisering en andere technische maatregelen omvatten.

61. Wanneer de verplichting van artikel 25 van de AVG wordt toegepast, moet rekening worden gehouden met de stand van de techniek, met de uitvoeringskosten en met de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen die aan de verwerking zijn verbonden. Nadere toelichtingen ten aanzien van deze verplichting zijn te vinden in de bovengenoemde EDPB-richtsnoeren 4/2019 inzake artikel 25 — Gegevensbescherming door ontwerp en door standaardinstellingen.

[34] Richtsnoeren 2/2019 betreffende de verwerking van persoonsgegevens op grond van artikel 6, lid 1, onder b), van de AVG in het kader van de verlening van onlinediensten aan betrokkenen, EDPB, punt 32.
[35] Richtsnoeren 4/2019 inzake artikel 25 — Gegevensbescherming door ontwerp en door standaardinstellingen, blz. 29.

6.2 Maatregelen voor minimale gegevensverwerking

62. Derde-aanbieders die betaalrekeninggegevens raadplegen om de gevraagde diensten aan te bieden, moeten ook rekening houden met het beginsel van gegevensminimalisatie en mogen alleen persoonsgegevens verzamelen die noodzakelijk zijn om de specifieke door de betalingsdienstgebruiker gevraagde diensten te verlenen. De toegang tot de persoonsgegevens moet in beginsel worden beperkt tot wat noodzakelijk is voor het aanbieden van betalingsdiensten. Zoals aangegeven in hoofdstuk 2, schrijft de RBD2 voor dat rekeninghoudende betalingsdienstaanbieders informatie over betalingsdienstgebruikers op verzoek van de betalingsdienstgebruiker delen wanneer de betalingsdienstgebruiker een betalingsinitiatiedienst of een rekeninginformatiedienst wil gebruiken.

63. Wanneer niet alle betaalrekeninggegevens noodzakelijk zijn voor de uitvoering van de overeenkomst, moet de rekeninginformatiedienstaanbieder een selectie van de relevante gegevenscategorieën maken voordat de gegevens worden verzameld. Voorbeelden van gegevenscategorieën die mogelijk niet noodzakelijk zijn, zijn de identiteit van de derde en de kenmerken van de transactie. Tenzij dit op grond van het lidstatelijk of het EU-recht vereist is, is het mogelijk ook niet noodzakelijk om het IBAN-nummer van de bankrekening van de derde te tonen.

64. In dat verband kan worden overwogen om een technische maatregel toe te passen die derde-aanbieders in staat stelt of helpt om hun verplichting na te komen om alleen de persoonsgegevens te raadplegen en op te vragen die nodig zijn voor de verlening van hun diensten, als onderdeel van de uitvoering van een passend gegevensbeschermingsbeleid in overeenstemming met artikel 24, lid 2, AVG. In dat verband beveelt het EDPB het gebruik aan van digitale hulpmiddelen om rekeninginformatiedienstaanbieders te ondersteunen bij hun verplichting om alleen persoonsgegevens te verzamelen die noodzakelijk zijn voor de doeleinden waarvoor zij worden verwerkt. Wanneer bijvoorbeeld een dienstverlener de kenmerken van de transactie (in het veld “Beschrijving” van de transactiegegevens) niet nodig heeft om zijn dienst te verlenen, zou een digitale selectietool als middel kunnen dienen waarmee derde-aanbieders dit veld kunnen uitsluiten van de algemene verwerkingsactiviteiten van de derde-aanbieder.

Voorbeeld 2:

HappyPayments, onze rekeninginformatiedienstverlener uit voorbeeld 1, wil ervoor zorgen dat hij alleen de persoonlijke betaalrekeninggegevens verwerkt waarin zijn gebruikers geïnteresseerd zijn. Voor het verlenen van de dienst is het niet nodig te trachten toegang te krijgen tot meer betaalrekeninggegevens. Hij biedt de gebruikers daarom de mogelijkheid om de specifieke soorten informatie te kiezen waarin zij geïnteresseerd zijn.

Gebruiker A wil een overzicht van zijn uitgaven van de afgelopen twee maanden. Hij vraagt daarom voor zijn twee bankrekeningen, bij twee verschillende rekeninghoudende betalingsdienstaanbieders, de informatie op over alle transacties van de laatste twee maanden, het bedrag van de transacties, de datum van uitvoering en de naam van de begunstigde, en vinkt de overeenkomstige vakjes aan in de gebruikersinterface van HappyPayments.

HappyPayments begint vervolgens bij de respectieve rekeninghoudende betalingsdienstaanbieders alleen die informatie op te vragen die overeenstemt met de velden die door Gebruiker A zijn ingesteld, en alleen voor de afgelopen twee maanden. Informatie zoals de “mededeling” van de overschrijving of zelfs het IBAN-nummer worden niet opgevraagd, aangezien Gebruiker A niet om deze informatie heeft gevraagd.

Om HappyPayments in staat te stellen zijn verplichtingen inzake gegevensminimalisatie na te komen, bieden de rekeninghoudende betalingsdienstaanbieders HappyPayments de mogelijkheid om specifieke velden voor een bepaalde periode op te vragen.

65. Er zij in dit verband tevens op gewezen dat rekeninghoudende betalingsdienstaanbieders volgens de RBD2 alleen toegang mogen verlenen tot betaalrekeninginformatie. De RBD2 bevat geen rechtsgrond om toegang te verlenen tot persoonsgegevens in andere rekeningen, zoals spaarrekeningen, hypotheken of beleggingsrekeningen. Volgens de RBD2 moeten er dan ook technische maatregelen worden getroffen om te verzekeren dat de toegang wordt beperkt tot de noodzakelijke betaalrekeninginformatie.

66. De dienstverlener moet niet alleen zo weinig mogelijk gegevens verzamelen, hij moet ook beperkte bewaringstermijnen hanteren. Persoonsgegevens mogen door de dienstverlener niet langer worden bewaard dan noodzakelijk is voor de door de betalingsdienstgebruiker gevraagde doeleinden.

67. Indien de overeenkomst tussen de betrokkene en de rekeninginformatiedienstaanbieder vereist dat persoonsgegevens worden doorgegeven aan derden, mogen alleen die persoonsgegevens die noodzakelijk zijn voor de uitvoering van de overeenkomst worden doorgegeven. Betrokkenen moeten ook specifiek in kennis worden gesteld van de doorgifte en van de persoonsgegevens die aan deze derde zullen worden doorgegeven.

6.3 Beveiliging

68. Het EDPB heeft reeds benadrukt dat de schending van financiële persoonsgegevens “duidelijk gevolgen heeft voor het dagelijkse leven van de betrokkene” en haalt de risico’s van betalingsfraude als voorbeeld aan[36].

69. Wanneer een datalek betrekking heeft op financiële gegevens, kan de betrokkene aan aanzienlijke risico’s worden blootgesteld. Afhankelijk van de gelekte informatie kunnen betrokkenen worden blootgesteld aan het risico aan het risico van identiteitsdiefstal, diefstal van de tegoeden op hun rekeningen en andere activa. Bovendien bestaat de mogelijkheid dat de blootstelling van transactiegegevens verband houdt met aanzienlijke privacyrisico’s, aangezien transactiegegevens verwijzingen kunnen bevatten naar alle aspecten van het privéleven van een betrokkene. Tegelijkertijd zijn financiële gegevens duidelijk waardevol voor criminelen en dus een aantrekkelijk doelwit.

70. Als verwerkingsverantwoordelijken zijn betalingsdienstaanbieders verplicht om passende maatregelen te nemen om de persoonsgegevens van betrokkenen te beschermen (artikel 24, lid 1, AVG). Hoe hoger de risico’s waarmee de door de verwerkingsverantwoordelijke uitgevoerde verwerkingsactiviteit gepaard gaat, hoe hoger de beveiligingsnormen die moeten worden toegepast. Aangezien aan de verwerking van financiële gegevens verscheidene ernstige risico’s verbonden zijn, moeten de beveiligingsmaatregelen dienovereenkomstig hoog zijn.

71. Dienstverleners moeten aan hoge normen worden onderworpen, waaronder sterke mechanismen voor cliëntauthenticatie en hoge beveiligingsnormen voor de technische uitrusting[37]. Andere

[36] Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679 van Groep artikel 29, WP248 rev.01 — bekrachtigd door het EDPB.
[37] Zie de technische reguleringsnorm.

procedures, zoals het screenen van verwerkers op beveiligingsnormen en het uitvoeren van procedures tegen ongeoorloofde toegang, zijn eveneens belangrijk.

6.4 Transparantie en de verantwoordingsplicht

72. Transparantie en de verantwoordingsplicht zijn twee grondbeginselen van de AVG.

73. Met betrekking tot transparantie (artikel 5, lid 1, punt a), AVG), is in artikel 12 AVG gespecificeerd dat verwerkingsverantwoordelijken passende maatregelen nemen om de in de artikelen 13 en 14 AVG bedoelde informatie te verstrekken. Daarnaast is in dit artikel bepaald dat de informatie of communicatie over de verwerking van persoonsgegevens beknopt, transparant, begrijpelijk en gemakkelijk toegankelijk moet zijn. De informatie wordt in duidelijke en eenvoudige taal opgesteld en schriftelijk "of met andere middelen, met inbegrip van, indien dit passend is, elektronische middelen", verstrekt. De "Richtsnoeren inzake transparantie overeenkomstig Verordening 2016/679" van Groep artikel 29, zoals bekrachtigd door het EDPB, bevat specifieke richtsnoeren voor de naleving van het transparantiebeginsel in digitale omgevingen.

74. Volgens voornoemde Richtsnoeren inzake transparantie overeenkomstig Verordening 2016/679 moet artikel 11 AVG worden gezien als een middel om echte gegevensminimalisatie af te dwingen zonder de uitoefening van rechten door betrokkenen te belemmeren en moet de uitoefening van die rechten mogelijk worden gemaakt met behulp van door de betrokkene te verstrekken aanvullende informatie. Er kunnen situaties zijn waarin een verwerkingsverantwoordelijke persoonsgegevens verwerkt waarvoor de identificatie van een betrokkene niet nodig is (bijvoorbeeld bij gepseudonimiseerde gegevens). In dergelijke gevallen kan ook artikel 11, lid 1, relevant zijn, aangezien daarin wordt bepaald dat een verwerkingsverantwoordelijke niet verplicht is om, uitsluitend om aan de AVG te voldoen, aanvullende gegevens ter identificatie van de betrokkene bij te houden, te verkrijgen of te verwerken.

75. Voor diensten in het kader van de RBD2 is artikel 13 AVG van toepassing voor de persoonsgegevens die bij de betrokkene worden verzameld en is artikel 14 van toepassing wanneer de persoonsgegevens niet bij de betrokkene zijn verkregen.

76. De betrokkene moet meer in het bijzonder in kennis worden gesteld van de periode gedurende welke de persoonsgegevens zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria ter bepaling van die termijn en, in voorkomend geval, de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een eventuele derde. Wanneer de verwerking gebaseerd is op toestemming als bedoeld in artikel 6, lid 1, punt a), AVG of op uitdrukkelijke toestemming als bedoeld in artikel 9, lid 2, punt a), AVG, moet de betrokkene in kennis worden gesteld van het bestaan van het recht de toestemming te allen tijde in te trekken.

77. De verwerkingsverantwoordelijke verstrekt de informatie aan de betrokkene afhankelijk van de concrete omstandigheden waarin de persoonsgegevens worden verwerkt. Indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene[38], hetgeen waarschijnlijk het geval zal zijn voor rekeninginformatiedienstaanbieders, moet de informatie uiterlijk op het moment van het eerste contact met de betrokkene worden verstrekt. Wanneer de persoonsgegevens aan een andere ontvanger zullen worden verstrekt, moet de informatie uiterlijk worden verstrekt wanneer de persoonsgegevens voor het eerst worden bekendgemaakt.

78. Wat onlinebetalingsdiensten betreft, wordt in bovengenoemde richtsnoeren verduidelijkt dat verwerkingsverantwoordelijken een gelaagde aanpak kunnen volgen wanneer zij ervoor kiezen om

[38] Artikel 14, lid 3, punt b), AVG.

een combinatie van methoden te gebruiken om transparantie te waarborgen. Teneinde informatiemoeheid te voorkomen en tegelijkertijd de doeltreffendheid van de informatie te waarborgen is het in het bijzonder aanbevolen om gelaagde privacyverklaringen/mededelingen te gebruiken en daarin links te plaatsen naar de verschillende categorieën informatie die aan de betrokkene moeten worden verstrekt, in plaats van alle informatie in één enkele mededeling op het scherm weer te geven.

79. In voornoemde richtsnoeren is ook verduidelijkt dat verwerkingsverantwoordelijken aanvullende manieren kunnen hanteren om informatie te verstrekken aan de individuele betrokkene, zoals privacydashboards. Een privacydashboard is één enkel punt waar de betrokkene "privacy-informatie" kan inzien en zijn of haar privacyvoorkeuren kan beheren door toe te staan of te voorkomen dat zijn of haar gegevens door de verwerkingsverantwoordelijke in kwestie op bepaalde manieren worden gebruikt[39]. Een privacydashboard zou een overzicht kunnen geven van de derde-aanbieders die de uitdrukkelijke toestemming van de betrokkene hebben verkregen en zou ook relevante informatie kunnen bieden over de aard van en de hoeveelheid persoonsgegevens die door derde-aanbieders zijn geraadpleegd. In beginsel kan een rekeninghoudende betalingsdienstaanbieder de gebruiker de mogelijkheid bieden om een specifieke uitdrukkelijke toestemming in het kader van de RBD2 in te trekken[40] via het overzicht, waardoor een of meer derde-aanbieders de toegang tot hun betaalrekening zou worden ontzegd. De gebruiker zou een rekeninghoudende betalingsdienstaanbieder ook kunnen verzoeken om de toegang tot hun betaalrekening(en) te ontzeggen aan een of meer specifieke derde-aanbieders[41], aangezien het recht van de gebruiker is om al dan niet gebruik te maken van een rekeninginformatiedienst. Indien privacydashboards worden gebruikt om uitdrukkelijke toestemming te geven of in te trekken, moeten zij op rechtmatige wijze worden ontworpen en toegepast en in het bijzonder vermijden belemmeringen op te werpen voor het recht van derde-aanbieders om diensten te verlenen in overeenstemming met de RBD2. In dat verband en overeenkomstig de toepasselijke bepalingen van de RBD2 heeft een derde-aanbieder de mogelijkheid om opnieuw de uitdrukkelijke toestemming van de gebruiker te verkrijgen nadat die toestemming is ingetrokken.

80. De beginselen van verantwoordingsplicht schrijven voor dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen vaststelt om te waarborgen dat de verwerking plaatsvindt in overeenstemming met de AVG, in het bijzonder met de belangrijkste gegevensbeschermingsbeginselen van artikel 5, lid 1. Bij die maatregelen moet rekening worden gehouden met de aard, de omvang, de context en het doel van de verwerking en het risico voor de rechten en vrijheden van natuurlijke personen, en de maatregelen moeten worden geëvalueerd en indien nodig geactualiseerd[42].

[39] Volgens de Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679 van Groep artikel 29, zoals bekrachtigd door het EDPB, zijn privacydashboards met name zinvol wanneer de betrokkene dezelfde dienst gebruikt op verschillende apparaten, omdat de betrokkene zo toegang tot en controle over zijn of haar persoonsgegevens krijgt, ongeacht hoe hij of zij de dienst gebruikt. Toestaan dat betrokkenen hun privacy-instellingen kunnen aanpassen via een privacydashboard kan het ook gemakkelijker maken om een privacyverklaring/mededeling te personaliseren door daarin alleen de soorten verwerkingen op te nemen die op een betrokkene van toepassing zijn.

[40] Zie bijvoorbeeld de in artikel 67, lid 2, punt a), RBD2 vermelde "uitdrukkelijke toestemming".

[41] Zie ook EBA/OP/2020/10, punt 45

[42] Artikel 5, lid 2, en artikel 24 AVG.

6.5 Profilering

81. De verwerking van persoonsgegevens door betalingsdienstaanbieders kan gepaard gaan met "profilering" als bedoeld in artikel 4, punt 4, AVG. Zo kunnen rekeninginformatiedienstaanbieders gebruikmaken van de geautomatiseerde verwerking van persoonsgegevens om bepaalde persoonlijke aspecten van een natuurlijke persoon te beoordelen. Naargelang van de specifieke kenmerken van de dienst kan de persoonlijke financiële situatie van een betrokkene worden beoordeeld. Rekeninginformatiediensten die op verzoek van gebruikers moeten worden verstrekt, kunnen gepaard gaan met een uitgebreide beoordeling van persoonlijke betaalrekeninggegevens.

82. De verwerkingsverantwoordelijke moet tegenover de betrokkene ook transparant zijn over het bestaan van geautomatiseerde besluitvorming, waaronder profilering. In die gevallen moet de verwerkingsverantwoordelijke nuttige informatie verstrekken over de onderliggende logica en over het belang en de verwachte gevolgen van die verwerking voor de betrokkene (artikel 13, lid 2, punt f), en artikel 14, lid 2, punt g), en overweging 60)[43]. Evenzo heeft de betrokkene krachtens artikel 15 AVG het recht om van de verwerkingsverantwoordelijke informatie te ontvangen over het bestaan van geautomatiseerde besluitvorming, waaronder profilering, de onderliggende logica en de gevolgen voor de betrokkene en, in bepaalde omstandigheden, het recht om bezwaar te maken tegen profilering, ongeacht of er uitsluitend geautomatiseerde individuele besluitvorming op basis van profilering plaatsvindt[44].

83. Wat in deze context voorts relevant is, is het in artikel 22 AVG opgenomen recht van de betrokkene niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft. Die norm houdt onder bepaalde omstandigheden ook in dat de verwerkingsverantwoordelijken passende maatregelen moeten treffen om de rechten van de betrokkene te waarborgen, waaronder specifieke informatie aan de betrokkene, het recht op menselijke tussenkomst en het recht om zijn standpunt kenbaar te maken en om het besluit aan te vechten. Zoals ook vermeld in overweging 71 AVG betekent dit onder meer dat betrokkenen het recht hebben niet te worden onderworpen aan een besluit, zoals de automatische weigering van een online ingediende kredietaanvraag of van verwerking van sollicitaties via internet zonder menselijke tussenkomst[45].

84. Geautomatiseerde besluitvorming, waaronder profilering, waarbij bijzondere categorieën van persoonsgegevens betrokken zijn, is uitsluitend toegestaan onder de cumulatieve voorwaarden van artikel 22, lid 4, AVG:

- er geldt een uitzondering op grond van artikel 22, lid 2;
- en artikel 9, lid 2, punten a) tot en met g), AVG zijn van toepassing. In beide gevallen neemt de verwerkingsverantwoordelijke passende maatregelen om de rechten en vrijheden en het gerechtvaardigde belang van de betrokkene te waarborgen[46].

85. De vereisten voor verdere verwerking, zoals vermeld in deze richtsnoeren, moeten eveneens in acht worden genomen. De verduidelijkingen en instructies inzake geautomatiseerde individuele

[43] Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679, WP 260 — bekrachtigd door het EDPB.
[44] Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679 van de Groep artikel 29, WP251rev.01.
[45] Overweging 71 AVG.
[46] Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679 van de Groep artikel 29, WP251rev.01, blz. 24.

besluitvorming en profilering in de Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening (EU) 2016/679 van de Groep artikel 29, zoals bekrachtigd door het EDPB, zijn volledig relevant in de context van betalingsdiensten en moeten derhalve naar behoren in overweging worden genomen.

Voor het Europees Comité voor gegevensbescherming

De voorzitter

(Andrea Jelinek)