**Richtsnoeren 06/2020 over het samenspel van de tweede betaling** **Dienstenrichtlijn en de AVG**

**Versie 1.0**

**Aangenomen op 17 juli 2020**

Inhoudsopgave

[1. 1. Inleiding 4](#_Toc24619)

[1.1 Definities 5](#_Toc24620)

[1.2 Diensten onder de PSD2 6](#_Toc24621)

[2 Wettige gronden en verdere verwerking in het kader van de PSD2 8](#_Toc24622)

[2.1 Wettige gronden voor verwerking 8](#_Toc24623)

[2.2 Artikel 6, lid 1, onder b), van de AVG (verwerking is noodzakelijk voor de uitvoering van een contract) 8](#_Toc24624)

[2.3 Verdere verwerking 10](#_Toc24625)

[2.4 Wettige grond voor het verlenen van toegang tot de rekening (ASPSP's) 10](#_Toc24626)

[3 Expliciete toestemming 12](#_Toc24627)

[3.1 Toestemming in het kader van de AVG 12](#_Toc24628)

[3.2 Toestemming in het kader van de PSD2 12](#_Toc24629)

[3.2.1. Expliciete toestemming krachtens artikel 94, lid 2 PSD2 13](#_Toc24630)

[3.3 Conclusie 14](#_Toc24631)

[4 De verwerking van stilzwijgende partijgegevens 15](#_Toc24632)

[4.1 Stille partijgegevens 15](#_Toc24633)

[4.2 Het rechtmatige belang van de voor de verwerking verantwoordelijke 15](#_Toc24634)

[4.3 Verdere verwerking van persoonsgegevens van de zwijgende partij 15](#_Toc24635)

[5 De verwerking van bijzondere categorieën van persoonsgegevens in het kader van de PSD2 17](#_Toc24636)

[5.1 Bijzondere categorieën van persoonsgegevens 17](#_Toc24637)

[5.2 Mogelijke afwijkingen 17](#_Toc24638)

[5.3 Aanzienlijk algemeen belang 18](#_Toc24639)

[5.4 Expliciete toestemming 18](#_Toc24640)

[5.5 Geen passende afwijking 18](#_Toc24641)

[6 Minimalisatie van gegevens, veiligheid, transparantie, verantwoordingsplicht en profilering 19](#_Toc24642)

[6.1 Gegevensminimalisatie en gegevensbescherming door ontwerp en standaardisering 19](#_Toc24643)

[6.2 Maatregelen om gegevens te minimaliseren 19](#_Toc24644)

[6.3 Veiligheid 20](#_Toc24645)

[6.4 Transparantie en verantwoording 21](#_Toc24646)

[6.5 Profilering 22](#_Toc24647)

**Het Europees Comité voor gegevensbescherming**

Gezien artikel 70, lid 1, onder e), van Verordening 2016/679/EU 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 met name bijlage XI en Protocol 37, zoals gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018[[1]](#footnote-1), Gezien artikel 12 en artikel 22 van zijn reglement van orde,

Terwijl:

1. De algemene verordening inzake gegevensbescherming (AVG) voorziet in een consistente reeks regels voor de verwerking van persoonsgegevens in de hele EU.
2. De tweede betalingsdienstenrichtlijn (Richtlijn 2015/2366/EU van het Europees Parlement en de Raad van 23 december 2015, hierna "PSD2" genoemd) trekt Richtlijn 2007/64/EG in en voorziet in nieuwe regels om de rechtszekerheid voor consumenten, handelaren en ondernemingen in de betalingsketen te waarborgen en het rechtskader voor de markt voor betalingsdiensten te moderniseren.[[2]](#footnote-2) De lidstaten moesten de PSD2 vóór 13 januari 2018 in nationaal recht omzetten.
3. Een belangrijk kenmerk van de PSD2 is de invoering van een wettelijk kader voor nieuwe betalingsinitiëringsdiensten en rekeninginformatiediensten. De PSD2 stelt deze nieuwe betalingsdienstaanbieders in staat om toegang te krijgen tot betaalrekeningen van betrokkenen voor het verlenen van de genoemde diensten.
4. Wat de gegevensbescherming betreft, wordt overeenkomstig artikel 94, lid 1, van de PSD2 elke verwerking van persoonsgegevens, met inbegrip van het verstrekken van informatie over de verwerking, voor de doeleinden van de PSD2 uitgevoerd in overeenstemming met de AVG[[3]](#footnote-3) en Verordening (EU) nr. 2018/1725.
5. In overweging 89 van de PSD2 staat dat wanneer persoonsgegevens voor de doeleinden van de PSD2 worden verwerkt, het precieze doel van de verwerking moet worden gespecificeerd, de toepasselijke rechtsgrondslag moet worden genoemd, de relevante veiligheidsvereisten die in de AVG zijn vastgelegd, ten uitvoer moeten worden gelegd en de beginselen van noodzakelijkheid, evenredigheid, doelbinding en evenredige bewaringstermijnen voor gegevens moeten worden nageleefd. Ook moeten gegevensbescherming door ontwerp en gegevensbescherming standaard worden ingebed in alle gegevensverwerkingssystemen die in het kader van de PSD2worden ontwikkeld en gebruikt. 4
6. Overweging 93 van de PSD2 bepaalt dat de betalingsdienstaanbieders en de betalingsdienstaanbieders voor rekeninginformatie enerzijds en de betalingsdienstaanbieders voor rekeningonderhoud anderzijds zich dienen te houden aan de noodzakelijke gegevensbeschermings- en veiligheidseisen die bij deze richtlijn zijn vastgesteld of waarnaar in deze richtlijn wordt verwezen of die in de technische reguleringsnormen zijn opgenomen.

**HEEFT DE VOLGENDE RICHTSNOEREN VASTGESTELD**

# 1. 1. INLEIDING

 De tweede Richtlijn Betalingsdiensten (hierna "PSD2" genoemd) heeft een aantal nieuwigheden op het gebied van betalingsdiensten geïntroduceerd. Hoewel de toepassing van de PSD2 nieuwe mogelijkheden voor consumenten schept en de transparantie op dit gebied vergroot, doet zij bepaalde vragen en zorgen rijzen met betrekking tot de noodzaak dat de betrokkenen de volledige controle over hun persoonsgegevens behouden. De algemene verordening inzake gegevensbescherming (hierna "de AVG" genoemd) is van toepassing op de verwerking van persoonsgegevens, met inbegrip van verwerkingsactiviteiten in het kader van betalingsdiensten zoals gedefinieerd in de PSD2[[4]](#footnote-4). De voor de verwerking verantwoordelijken die op het door de PSD2 bestreken gebied handelen, moeten dus altijd de vereisten van de AVG in acht nemen, met inbegrip van de in artikel 5 van de AVG neergelegde beginselen inzake gegevensbescherming, alsook de desbetreffende bepalingen van de e-privacyrichtlijn[[5]](#footnote-5). Hoewel de PSD2[[6]](#footnote-6) en de regelgevende technische normen voor sterke klantenauthenticatie en gemeenschappelijke en veilige open communicatienormen (hierna "RTS" genoemd[[7]](#footnote-7)) een aantal bepalingen bevatten met betrekking tot gegevensbescherming en -beveiliging, is er onzekerheid ontstaan over de interpretatie van deze bepalingen en over de wisselwerking tussen het algemene gegevensbeschermingskader en de PSD2.

 Op 5 juli 2018 heeft de EDPB een brief over de PSD2 gepubliceerd, waarin de EDPB toelichting geeft bij vragen over de bescherming van persoonsgegevens in verband met de PSD2, met name over de verwerking van persoonsgegevens van niet-aangeslotenen (zogenaamde "silent party data") door aanbieders van rekeninginformatiediensten (hierna "AISP's" genoemd) en aanbieders van diensten voor het initiëren van betalingen (hierna "PISP's" genoemd), de procedures met betrekking tot het geven en intrekken van toestemming, de RTS en de samenwerking tussen betalingsdienstaanbieders voor rekeningen (hierna "ASPSP's" genoemd) met betrekking tot veiligheidsmaatregelen. Terwijl het voorbereidende werk voor deze richtsnoeren bestond uit het verzamelen van input van belanghebbenden, zowel schriftelijk als op een evenement van belanghebbenden, om de meest urgente uitdagingen vast te stellen.

 Deze richtsnoeren zijn bedoeld om in het kader van de PSD2 verdere richtsnoeren te geven over gegevensbeschermingsaspecten, met name over het verband tussen de relevante bepalingen inzake de AVG en de PSD2. Deze richtsnoeren zijn vooral gericht op de verwerking van persoonsgegevens door AISP's en PISP's. Als zodanig behandelt dit document de voorwaarden voor het verlenen van toegang tot informatie over betaalrekeningen door de ASPSP's en voor de verwerking van persoonsgegevens door PISP’s en AISP's, met inbegrip van de vereisten en waarborgen met betrekking tot de verwerking van persoonsgegevens door PISP’s en AISP's voor andere doeleinden dan de oorspronkelijke doeleinden waarvoor de gegevens zijn verzameld, met name wanneer zij zijn verzameld in het kader van de verstrekking van een rekeninginformatiedienst.[[8]](#footnote-8) Dit document behandelt ook verschillende begrippen van uitdrukkelijke toestemming in het kader van de richtlijn inzake overheidsopdrachten2 en de richtlijn inzake de bescherming van persoonsgegevens (AVG), de verwerking van "derdengegevens", de verwerking van speciale categorieën persoonsgegevens door PISP’s en AISP's, de toepassing van de belangrijkste gegevensbeschermingsbeginselen die in de AVG zijn vastgelegd, met inbegrip van minimalisering van de gegevens, transparantie, verantwoordingsplicht en veiligheidsmaatregelen. De PSD2 brengt multifunctionele verantwoordelijkheden met zich mee op het gebied van onder meer consumentenbescherming en mededingingsrecht. Overwegingen met betrekking tot deze rechtsgebieden vallen buiten het toepassingsgebied van deze richtsnoeren.

 Om het lezen van de richtsnoeren te vergemakkelijken, worden de belangrijkste definities die in dit document worden gebruikt, hieronder vermeld.

## 1.1Definities

*Met "Account Information Service Provider" ("AISP")* wordt de aanbieder van een onlinedienst bedoeld om geconsolideerde informatie te verstrekken over een of meer betaalrekeningen die de betalingsdienstgebruiker bij een andere betalingsdienstaanbieder of bij meer dan een betalingsdienstaanbieder aanhoudt;

*Met "Account Servicing Payment Service Provider" ("ASPSP")* wordt bedoeld een betalingsdienstaanbieder die een betaalrekening voor een betaler aanlevert en onderhoudt*;*

*Gegevensminimalisering"* is een beginsel van gegevensbescherming, volgens hetwelk persoonsgegevens adequaat en relevant moeten zijn en beperkt moeten blijven tot hetgeen noodzakelijk is in verband met de doeleinden waarvoor zij worden verwerkt;

*Betaler"* verwijst naar een natuurlijke of rechtspersoon die een betaalrekening heeft en een betalingsopdracht van die betaalrekening toestaat, of, wanneer er geen betaalrekening is, een natuurlijke of rechtspersoon die een betalingsopdracht geeft;

*Begunstigde"* verwijst naar een natuurlijke of rechtspersoon die de beoogde ontvanger is van de gelden die het voorwerp van een betalingstransactie zijn geweest*;*

*Betalingsrekening"*: een rekening op naam van een of meer betalingsdienstgebruikers die wordt gebruikt voor de uitvoering van betalingstransacties;

*Met "aanbieder van betalingsinitiëringsdiensten" ("PISP")* wordt de aanbieder van een dienst bedoeld die op verzoek van de betalingsdienstgebruiker een betalingsopdracht initieert met betrekking tot een betaalrekening bij een andere betalingsdienstaanbieder;

*Onder "betalingsdienstaanbieder" wordt verstaan* een instantie als bedoeld in artikel 1, lid 1, van de PSD210 of een natuurlijke of rechtspersoon die uit hoofde van artikel 32 of 33 van de PSD2 een vrijstelling geniet;

10 Art. 1 (1) In de PSD2 is bepaald dat de lidstaten bij de vaststelling van de regels een onderscheid moeten maken tussen de volgende categorieën *betalingsdienstaanbieders*:

a) kredietinstellingen in de zin van punt 1) van artikel 2, lid 1, van de richtlijn. 4, lid 1, van Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad ( 1 ), met inbegrip van bijkantoren daarvan in de zin van artikel 17, lid 17, van die verordening. 4, lid 1, van die verordening wanneer dergelijke bijkantoren in de Unie zijn gevestigd, ongeacht of het hoofdkantoor van die bijkantoren in de Unie is gevestigd of, in overeenstemming met artikel 4, lid 1, van die verordening. 47 van Richtlijn 2013/36/EU en met het nationale recht, buiten de Unie; b) instellingen voor elektronisch geld in de zin van punt 1 van artikel 4, lid 1, van die verordening, ongeacht of het hoofdkantoor van die bijkantoren in de Unie is gevestigd of, overeenkomstig artikel 47 van Richtlijn 2013/36/EU en het nationale recht, buiten de Unie; c) instellingen voor elektronisch geld in de zin van artikel 4, lid 1, van die verordening, ongeacht of het hoofdkantoor van die bijkantoren in de Unie is gevestigd. 2 van Richtlijn 2009/110/EG, met inbegrip van, in overeenstemming met artikel 2, lid 1, van die richtlijn; b) instellingen voor elektronisch geld in de zin van artikel 2, lid 1, van Richtlijn 2009/110/EG, met inbegrip van, in overeenstemming met artikel 2, lid 2, van die richtlijn. 8 van die richtlijn en met het nationale recht, bijkantoren daarvan, wanneer deze bijkantoren binnen de Unie zijn gevestigd en hun hoofdkantoor buiten de Unie is gevestigd, voor zover de door deze bijkantoren verrichte betalingsdiensten verband houden met de uitgifte van elektronisch geld;

c) postcheque- en girodiensten die krachtens het nationale recht gerechtigd zijn betalingsdiensten te verlenen; d) betalingsinstellingen;

1. de ECB en de nationale centrale banken wanneer zij niet handelen in hun hoedanigheid van monetaire autoriteit of andere overheidsinstanties;
2. De lidstaten of hun regionale of lokale overheden wanneer zij niet in hun hoedanigheid van overheid optreden.

*Onder "gegevensbescherming door ontwerp"* wordt verstaan: technische en organisatorische maatregelen die in een product of dienst zijn ingebed en die bedoeld zijn om de gegevensbeschermingsbeginselen op doeltreffende wijze toe te passen en de nodige waarborgen in de verwerking te integreren om te voldoen aan de eisen van de AVG en de rechten van de betrokkenen te beschermen;

*Met "standaardgegevensbescherming"* wordt bedoeld passende technische en organisatorische maatregelen die in een product of dienst worden toegepast en die ervoor zorgen dat standaard alleen persoonsgegevens worden verwerkt die voor elk specifiek doel van de verwerking noodzakelijk zijn;

*RTS"* verwijst naar de 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 met betrekking tot technische reguleringsnormen voor een sterke klantenauthenticatie en gemeenschappelijke en veilige open communicatienormen;

*Met "*derde partijen" *("TPP")* worden zowel PISP's als AISP's bedoeld.

## 1.2Diensten onder de PSD2

 De PSD2 introduceert twee nieuwe soorten betalingsdiensten (aanbieders): PISP's en AISP's. Bijlage 1 van de PSD2 bevat de acht betalingsdiensten die onder de PSD2 vallen.

 ISP's bieden diensten aan om op verzoek van een betalingsdienstgebruiker betalingsopdrachten te initiëren met betrekking tot de betaalrekening van de gebruiker die bij een andere betalingsdienstaanbieder wordt aangehouden.[[9]](#footnote-9) Een PISP kan een ASPSP (gewoonlijk een bank) verzoeken een transactie te initiëren in naam van de betalingsdienstgebruiker. De (betalingsdienst)gebruiker kan een natuurlijke persoon (betrokkene) of een rechtspersoon zijn.

 De AISP's bieden onlinediensten aan voor geconsolideerde informatie over een of meer betaalrekeningen die de betalingsdienstgebruiker bij een andere betalingsdienstaanbieder of bij meer dan een betalingsdienstaanbieder aanhoudt. 12 Volgens overweging 28 van de PSD2 kan de betalingsdienstgebruiker op elk moment onmiddellijk een algemeen beeld krijgen van zijn financiële situatie.

 Als het gaat om accountinformatiediensten, kunnen er verschillende soorten diensten worden aangeboden, met de nadruk op verschillende kenmerken en doeleinden. Zo kunnen sommige aanbieders gebruikers diensten aanbieden zoals budgetplanning en toezicht op de uitgaven. De verwerking van persoonsgegevens in het kader van deze diensten valt onder de PSD2. Diensten die kredietwaardigheidsbeoordelingen van de betalingsdienstverlener of auditdiensten op basis van de verzameling van informatie via een rekeninginformatiedienst omvatten, vallen buiten het toepassingsgebied van de PSD2 en vallen daarom onder de AVG. Andere rekeningen dan betaalrekeningen (bv. sparen, beleggen) vallen echter niet onder de PSD2.

Voorbeeld:

HappyPayments is een bedrijf dat een online dienst aanbiedt die bestaat uit het verstrekken van informatie over een of meer betaalrekeningen via een mobiele app om financieel toezicht te houden (een Account Information Service). Met deze dienst kan de gebruiker van de betaaldienst in één oogopslag de saldi en recente transacties op twee of meer betaalrekeningen bij verschillende banken zien. Het biedt ook, wanneer een betalingsdienstgebruiker daarvoor kiest, een categorisering van uitgaven en inkomsten volgens verschillende typologieën (salaris, vrije tijd, energie, hypotheek, enz.), waardoor de betalingsdienstgebruiker wordt geholpen bij de financiële planning. Binnen deze app biedt HappyPayments ook een dienst aan om betalingen rechtstreeks vanuit de aangewezen betaalrekening(en) (een Payment Initiation Service) te initiëren.

 Om deze diensten te kunnen verlenen, regelt de PSD2 de wettelijke voorwaarden waaronder PISP's en AISP's toegang kunnen krijgen tot betaalrekeningen om een dienst te verlenen aan de gebruiker van de betalingsdienst.

 In artikel 66, lid 1, en artikel 67, lid 1, van de richtlijn betalingsdiensten2 wordt bepaald dat de toegang tot en het gebruik van betalings- en rekeninginformatiediensten rechten van de betalingsdienstgebruiker zijn. Dit betekent dat de betalingsdienstgebruiker volledig vrij moet blijven met betrekking tot de uitoefening van een dergelijk recht en niet kan worden gedwongen om van dit recht gebruik te maken.

 De toegang tot betaalrekeningen en het gebruik van informatie over betaalrekeningen is gedeeltelijk geregeld in de artikelen 66 en 67 van de PSD2, die waarborgen bevatten met betrekking tot de bescherming van (persoons)gegevens. Artikel 66, lid 3, onder f), van de PSD2 bepaalt dat de ISP de betalingsdienstgebruiker niet om andere gegevens mag verzoeken dan die welke noodzakelijk zijn om de betalingsinitiëringsdienst te verlenen, en artikel 66, lid 3, onder g), van de PSD2 bepaalt dat ISP's geen gegevens mogen gebruiken, raadplegen of opslaan voor andere doeleinden dan het verrichten van de betalingsinitiëringsdienst waarom uitdrukkelijk door de betalingsdienstgebruiker is verzocht. Voorts bepaalt artikel 67, lid 2, onder d), van de PSD2 dat de toegang van AISP's beperkt is tot de informatie van aangewezen betaalrekeningen en daarmee verband houdende betalingstransacties, terwijl artikel 67, lid 2, onder f), van de PSD2 bepaalt dat AISP's geen gegevens mogen gebruiken, raadplegen of opslaan voor andere doeleinden dan het verrichten van de uitdrukkelijk door de betalingsdienstgebruiker gevraagde rekeninginformatiedienst, in overeenstemming met de gegevensbeschermingsregels. Dit laatste benadrukt dat, in het kader van de rekeninginformatiediensten, persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden kunnen worden verzameld. Een AISP moet daarom in het contract uitdrukkelijk vermelden voor welke specifieke doeleinden de persoonsgegevens zullen worden verwerkt in het kader van de door hem verleende rekeninginformatiedienst. Het contract moet wettig, billijk en transparant zijn in de zin van artikel 5 van de AVG en moet ook in overeenstemming zijn met andere consumentenbeschermingswetten.

 Afhankelijk van de specifieke omstandigheden kunnen betalingsdienstaanbieders een voor de verwerking verantwoordelijke of een verwerker in het kader van de AVG zijn.[[10]](#footnote-10)

# 2 ONRECHTMATIGE GRONDEN EN VERDERE VERWERKING ONDER DE PSD2

## 2.1Wettige redenen voor verwerking

 Volgens de AVG moeten de voor de verwerking verantwoordelijken over een rechtsgrondslag beschikken om persoonsgegevens te kunnen verwerken. Artikel 6, lid 1, van de AVG vormt een uitputtende en restrictieve lijst van zes rechtsgrondslagen voor de verwerking van persoonsgegevens in het kader van de AVG14. Het is aan de voor de verwerking verantwoordelijke om de passende rechtsgrondslag vast te stellen en ervoor te zorgen dat aan alle voorwaarden voor deze rechtsgrondslag wordt voldaan. De vaststelling van de geldige en meest geschikte rechtsgrondslag in een specifieke situatie hangt af van de omstandigheden waaronder de verwerking plaatsvindt, met inbegrip van het doel van de verwerking en de relatie tussen de voor de verwerking verantwoordelijke en de betrokkene.

## 2.2 Artikel 6, lid 1, onder b), van de AVG (verwerking is noodzakelijk voor de uitvoering van een contract)

 Betalingsdiensten worden altijd geleverd op contractuele basis tussen de betalingsdienstgebruiker en de betalingsdienstaanbieder. Zoals in overweging 87 van de PSD2 wordt gesteld, "*mag zijn richtlijn alleen betrekking hebben op contractuele verplichtingen en verantwoordelijkheden 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, onder b), van de AVG, hetgeen betekent dat de verwerking noodzakelijk is voor de uitvoering van een contract waarbij de betrokkene partij is of om op verzoek van de betrokkene stappen te ondernemen alvorens een contract te sluiten.

 De betalingsdiensten in het kader van de PSD2 zijn gedefinieerd in bijlage 1 van de PSD2. Het aanbieden van deze diensten zoals gedefinieerd in de PSD2 is een voorwaarde voor de totstandkoming van een contract waarin partijen toegang hebben tot de gegevens van de betaalrekening van de betalingsdienstgebruiker. Met betrekking tot betalingsinitiëringsdiensten en rekeninginformatiediensten in het kader van de PSD2 kunnen in de contracten voorwaarden worden opgenomen die ook betrekking hebben op aanvullende diensten die niet door de PSD2 worden gereguleerd. De *EDPB-richtsnoeren 2/2019 betreffende de verwerking van persoonsgegevens op grond van artikel 6, lid 1, onder b), van het AVG in het kader van de verlening van onlinediensten aan betrokkenen* maken duidelijk dat de voor de verwerking verantwoordelijken moeten beoordelen welke verwerking van persoonsgegevens objectief gezien noodzakelijk is om het contract uit te voeren. In deze richtsnoeren wordt erop gewezen dat de rechtvaardiging van de noodzaak afhankelijk is van de aard van de dienst, de

14 Volgens artikel 6 is de verwerking slechts rechtmatig indien en voor zover ten minste een van de volgende punten van toepassing is:

1. de betrokkene heeft toestemming gegeven voor de verwerking van zijn of haar persoonsgegevens voor een of meer specifieke doeleinden;
2. de verwerking is noodzakelijk voor de uitvoering van een contract waarbij de betrokkene partij is of om op verzoek van de betrokkene stappen te ondernemen alvorens een contract af te sluiten;
3. de verwerking is noodzakelijk voor de naleving van een wettelijke verplichting waaraan de voor de verwerking verantwoordelijke is onderworpen;
4. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
5. de verwerking is noodzakelijk voor de uitvoering van een taak van algemeen belang of voor de uitoefening van het officiële gezag dat aan de voor de verwerking verantwoordelijke is toegekend;
6. de verwerking is noodzakelijk voor de gerechtvaardigde belangen van de voor de verwerking verantwoordelijke of van een derde, behalve wanneer deze belangen worden overschaduwd door de belangen of fundamentele rechten en vrijheden van de betrokkene die bescherming van persoonsgegevens vereisen, in het bijzonder wanneer de betrokkene een kind is.

wederzijdse perspectieven en verwachtingen van de partijen bij het contract, de grondgedachte van het contract en de essentiële elementen van het contract.

 De EDPB-richtsnoeren 2/2019 maken ook duidelijk dat, in het licht van artikel 7, lid 4, van het AVG, een onderscheid wordt gemaakt tussen verwerkingsactiviteiten die noodzakelijk zijn voor de uitvoering van een contract en voorwaarden die de dienst afhankelijk maken van bepaalde verwerkingsactiviteiten die in feite niet noodzakelijk zijn voor de uitvoering van het contract. Voor "noodzakelijk voor de uitvoering" is duidelijk meer nodig dan een contractuele clausule.[[11]](#footnote-11) De voor de verwerking verantwoordelijke moet kunnen aantonen hoe het hoofddoel van het specifieke contract met de betrokkene in feite niet kan worden uitgevoerd als de specifieke verwerking van de betrokken persoonsgegevens niet plaatsvindt. De loutere verwijzing naar of vermelding van de gegevensverwerking in een contract volstaat niet om de verwerking in kwestie onder het toepassingsgebied van artikel 6, lid 1, onder b), van de AVG te brengen.

 Artikel 5, lid 1, onder b), van de AVG voorziet in het beginsel van doelbinding, op grond waarvan persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verkregen en vervolgens niet mogen worden verwerkt op een wijze die onverenigbaar is met die doeleinden. Bij de beoordeling of artikel 6, lid 1, onder b), een passende rechtsgrondslag is voor een online (betalings)dienst, moet rekening worden gehouden met het specifieke doel, het doel of de doelstelling van de dienst.[[12]](#footnote-12) De doeleinden van de verwerking moeten duidelijk worden gespecificeerd en aan de betrokkene worden meegedeeld, in overeenstemming met de verplichtingen van de voor de verwerking verantwoordelijke inzake doelbinding en transparantie. De beoordeling van wat "noodzakelijk" is, houdt een gecombineerde, op feiten gebaseerde beoordeling in van de verwerking "voor het nagestreefde doel en van de vraag of deze minder indringend is in vergelijking met andere opties om hetzelfde doel te bereiken". Artikel 6, lid 1, onder b), heeft geen betrekking op verwerking die nuttig maar niet objectief gezien noodzakelijk is voor het verrichten van de contractuele dienst of voor het nemen van relevante precontractuele stappen op verzoek van de betrokkene, ook al is deze noodzakelijk voor de andere bedrijfsdoeleinden van de voor de verwerking verantwoordelijke.[[13]](#footnote-13)

 De EDPB-richtsnoeren 2/2019 maken duidelijk dat contracten de categorieën persoonsgegevens of soorten verwerkingsoperaties die de voor de verwerking verantwoordelijke moet uitvoeren voor de uitvoering van het contract in de zin van artikel 6, lid 1, onder b), niet kunstmatig kunnen uitbreiden.[[14]](#footnote-14) Deze richtsnoeren hebben ook betrekking op gevallen waarin "take it or leave it"-situaties kunnen ontstaan voor betrokkenen die mogelijk slechts in een van de diensten geïnteresseerd zijn. Dit kan gebeuren wanneer een voor de verwerking verantwoordelijke verschillende afzonderlijke diensten of elementen van een dienst met verschillende fundamentele doeleinden, kenmerken of redenen wil bundelen in één contract. Wanneer het contract bestaat uit verschillende afzonderlijke diensten of elementen van een dienst die in feite redelijkerwijs onafhankelijk van elkaar kunnen worden verricht, moet de toepasselijkheid van artikel 6, lid 1, onder b), worden beoordeeld in de context van elk van die diensten afzonderlijk, waarbij wordt gekeken naar wat objectief gezien nodig is om elk van de afzonderlijke diensten waarom de betrokkene actief heeft verzocht of waarvoor hij zich heeft aangemeld, te verrichten.[[15]](#footnote-15)

 In overeenstemming met de bovengenoemde richtsnoeren moeten de verwerkingsverantwoordelijken beoordelen wat objectief gezien noodzakelijk is voor de uitvoering van het contract. Wanneer de voor de verwerking verantwoordelijken niet kunnen aantonen dat de verwerking van de gegevens van de persoonlijke betaalrekening objectief noodzakelijk is voor het verrichten van elk van deze diensten afzonderlijk, is artikel 6, lid 1, onder b), van de AVG geen geldige rechtsgrond voor verwerking. In deze gevallen moet de voor de verwerking verantwoordelijke een andere rechtsgrondslag voor de verwerking overwegen.

## 2.3Nadere verwerking

 Artikel 6, lid 4, van de AVG bepaalt de voorwaarden voor de verwerking van persoonsgegevens voor een ander doel dan waarvoor de persoonsgegevens zijn verzameld. Meer in het bijzonder kan een dergelijke verdere verwerking plaatsvinden, wanneer deze is gebaseerd op een wet van de Unie of een lidstaat, die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt om de in artikel 23, lid 1, genoemde doelstellingen te waarborgen, wanneer de betrokkene zijn toestemming heeft gegeven of wanneer de verwerking voor een ander doel dan waarvoor de persoonsgegevens zijn verzameld, verenigbaar is met het oorspronkelijke doel.

 De artikelen 66, lid 3, onder g), en 67, lid 2, onder f), van de PSD2 moeten zorgvuldig in aanmerking worden genomen. Zoals hierboven vermeld, bepaalt artikel 66, lid 3, onder g), van de richtlijn betalingsdiensten2 dat de PISP geen gegevens mag gebruiken, raadplegen of opslaan voor andere doeleinden dan het verlenen van de betalingsinitiëringsdienst waarom de betaler uitdrukkelijk heeft verzocht. In artikel 67, lid 2, onder f), van de PSD2 is bepaald dat de AISP de gegevens niet mag gebruiken, raadplegen of opslaan voor andere doeleinden dan het verrichten van de uitdrukkelijk door de betalingsdienstgebruiker gevraagde rekeninginformatiedienst, met inachtneming van de gegevensbeschermingsregels.

 Bijgevolg beperken artikel 66, lid 3, onder g), en artikel 67, lid 2, onder f), van de PSD2 de mogelijkheden voor verwerking voor andere doeleinden aanzienlijk, wat betekent dat de verwerking voor een ander doel niet is toegestaan, tenzij de betrokkene overeenkomstig artikel 6, lid 1, onder a), van de AVG toestemming heeft gegeven of de verwerking is vastgelegd in het recht van de Unie of in het recht van de lidstaat waaraan de voor de verwerking verantwoordelijke overeenkomstig artikel 6, lid 4, van de AVG is onderworpen. Wanneer de verwerking voor een ander doel dan waarvoor de persoonsgegevens zijn verzameld, niet is gebaseerd op de toestemming van de betrokkene of op het recht van de Unie of de lidstaat, maken de beperkingen in artikel 66, lid 3, onder g), en artikel 67, lid 2, onder f), van de PSD2 duidelijk dat een ander doel niet verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. De verenigbaarheidstoets van artikel 6, lid 4, van de AVG kan niet leiden tot een rechtsgrondslag voor de verwerking.

 Artikel 6, lid 4, van de AVG maakt verdere verwerking op basis van het recht van de Unie of van de lidstaten mogelijk. Zo zijn alle PISP’s en AISP's verplichte entiteiten krachtens artikel 3, lid 2, onder a), van Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of de financiering van terrorisme in het kader van de antiwitwasrichtlijn. Deze verplichte entiteiten zijn derhalve verplicht de in de richtlijn gespecificeerde klantenonderzoeksmaatregelen toe te passen. De persoonsgegevens die in verband met een PSD2-dienst worden verwerkt, worden dus verder verwerkt op basis van ten minste één wettelijke verplichting die op de dienstverrichter rust[[16]](#footnote-16).

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

## 2.4Wettelijke grond voor het verlenen van toegang tot de rekening (ASPSP's)

 Zoals vermeld in punt 10 kunnen betalingsdienstgebruikers hun recht uitoefenen om gebruik te maken van betalingsinitiërings- en rekeninginformatiediensten. De in artikel 66, lid 1, en artikel 67, lid 1, van de PSD2 aan de lidstaten opgelegde verplichtingen moeten in nationaal recht worden omgezet om de effectieve toepassing van het recht van de betalingsdienstgebruiker om van de bovengenoemde betalingsdiensten gebruik te maken, te waarborgen. De effectieve toepassing van dergelijke rechten zou niet mogelijk zijn zonder het bestaan van een overeenkomstige verplichting voor de ASPSP, doorgaans een bank, om de betalingsdienstaanbieder toegang te verlenen tot de rekening, op voorwaarde dat hij aan alle vereisten heeft voldaan om toegang te krijgen tot de rekening van de betalingsdienstgebruiker. Voorts wordt in artikel 66, lid 5, en artikel 67, lid 4, van de richtlijn betalingsdiensten2 duidelijk gesteld dat het verlenen van betalingsinitiëringsdiensten en van rekeninginformatiediensten niet afhankelijk is van het bestaan van een contractuele relatie tussen de PISP/AISP en de ASPSP.

 De verwerking van persoonsgegevens door de ASPSP, bestaande uit het verlenen van toegang tot de persoonsgegevens die door de PISP en de AISP worden opgevraagd om hun betalingsdienst aan de gebruiker van de betalingsdienst uit te voeren, is gebaseerd op een wettelijke verplichting. Om de doelstellingen van de PSD2 te bereiken, moeten de ASPSP's de persoonsgegevens voor de diensten van de ISP's en de AISP's verstrekken, hetgeen een noodzakelijke voorwaarde is om de ISP's en de AISP's in staat te stellen hun diensten te verlenen en aldus de in artikel 66, lid 1, en artikel 67, lid 1, van de PSD2 bedoelde rechten te waarborgen. Daarom is de toepasselijke rechtsgrond in dit geval artikel 6, lid 1, onder c), van de AVG.

 Aangezien de AVG heeft bepaald dat verwerking op basis van een wettelijke verplichting duidelijk moet worden vastgelegd in het recht van de Unie of van de lidstaten (zie artikel 6, lid 3, van de AVG), moet de verplichting voor ASPSP's om toegang te verlenen voortvloeien uit het nationale recht tot omzetting van de PSD2.

# 3 UITDRUKKELIJKE TOESTEMMING

## 3. 1C In het kader van de AVG

 Volgens de AVG is toestemming een van de zes rechtsgronden voor de rechtmatigheid van de verwerking van persoonsgegevens. In artikel 4, lid 11, van het AVG wordt toestemming gedefinieerd als "elke vrijelijk gegeven, specifieke, geïnformeerde en ondubbelzinnige aanduiding van de wensen van de betrokkene waarmee hij of zij, door middel van een verklaring of een duidelijke positieve handeling, instemt met de verwerking van de hem of haar betreffende persoonsgegevens". Deze vier voorwaarden, vrij gegeven, specifiek, geïnformeerd en ondubbelzinnig, zijn essentieel voor de geldigheid van de toestemming. Volgens de EDPB-richtsnoeren 05/2020 inzake toestemming op grond van Verordening 2016/679 kan toestemming alleen een passende wettelijke basis zijn als een betrokkene controle wordt geboden en een reële keuze wordt gemaakt met betrekking tot het aanvaarden of weigeren van de aangeboden of geweigerde voorwaarden zonder dat dit afbreuk doet aan zijn of haar rechten. Wanneer een voor de verwerking verantwoordelijke om toestemming vraagt, heeft hij de plicht om te beoordelen of hij aan alle vereisten voor het verkrijgen van geldige toestemming voldoet. Indien de toestemming wordt verkregen met volledige inachtneming van de AVG, is dit een instrument dat de betrokkenen controle geeft over de vraag of hun persoonsgegevens al dan niet zullen worden verwerkt. Zo niet, dan wordt de controle van de betrokkene illusoir en is de toestemming een ongeldige rechtsgrond voor de verwerking, waardoor de verwerkingsactiviteit onwettig wordt[[17]](#footnote-17).

 De AVG bevat ook verdere waarborgen in artikel 7, waarin wordt bepaald dat de voor de verwerking verantwoordelijke moet kunnen aantonen dat er ten tijde van de verwerking een geldige toestemming was. Ook moet het verzoek om toestemming worden gepresenteerd op een wijze die duidelijk te onderscheiden is van de andere zaken, in een begrijpelijke en gemakkelijk toegankelijke vorm, met gebruikmaking van duidelijke en duidelijke taal. Bovendien moet de betrokkene worden geïnformeerd over het recht om zijn of haar toestemming te allen tijde in te trekken, en wel op een even eenvoudige manier als bij het verlenen van de toestemming.

 Volgens artikel 9 van de AVG is toestemming een van de uitzonderingen op het algemene verbod op de verwerking van bijzondere categorieën van persoonsgegevens. In dat geval moet de toestemming van de betrokkene echter "uitdrukkelijk" zijn.[[18]](#footnote-18)

 Volgens de EDPB-richtsnoeren 05/2020 inzake toestemming in het kader van Verordening 2016/679 verwijst de uitdrukkelijke toestemming in het kader van de AVG naar de wijze waarop de betrokkene zijn toestemming uitspreekt. Dit betekent dat de betrokkene een uitdrukkelijke toestemming moet geven voor specifieke verwerkingsdoeleinden. Een voor de hand liggende manier om ervoor te zorgen dat de toestemming expliciet is, zou zijn om de toestemming uitdrukkelijk te bevestigen in een schriftelijke verklaring. In voorkomend geval kan de voor de verwerking verantwoordelijke ervoor zorgen dat de schriftelijke verklaring door de betrokkene wordt ondertekend, zodat alle mogelijke twijfel en het mogelijke gebrek aan bewijs in de toekomst worden weggenomen.

 In geen geval kan uit potentieel dubbelzinnige verklaringen of handelingen toestemming worden afgeleid. Een voor de verwerking verantwoordelijke moet er ook voor zorgen dat de toestemming niet kan worden verkregen door dezelfde motie als het akkoord gaan met een contract of het aanvaarden van de algemene voorwaarden van een dienst.

## 3.2Consumenten onder de PSD2

 De EDPB merkt op dat het juridische kader met betrekking tot uitdrukkelijke toestemming complex is, aangezien zowel de PSD2 als de AVG het begrip "uitdrukkelijke toestemming" bevatten. Dit leidt tot de vraag of "uitdrukkelijke toestemming" als bedoeld in artikel 94, lid 2, van de PSD2 op dezelfde wijze moet worden geïnterpreteerd als uitdrukkelijke toestemming in het kader van de AVG.

### 3.2.1Expliciete toestemming krachtens artikel 94, lid 2 PSD2

 De PSD2 bevat een aantal specifieke regels betreffende de verwerking van persoonsgegevens, met name in artikel 94, lid 1, van de PSD2, waarin wordt bepaald dat de verwerking van persoonsgegevens voor de doeleinden van de PSD2 in overeenstemming moet zijn met de EU-wetgeving inzake gegevensbescherming. Voorts is in artikel 94, lid 2, van de PSD2 bepaald dat betalingsdienstaanbieders alleen met de uitdrukkelijke toestemming van de betalingsdienstgebruiker toegang hebben tot de persoonsgegevens die nodig zijn voor het aanbieden van hun betalingsdiensten, deze verwerken en bewaren. Overeenkomstig artikel 33, lid 2, van de PSD2 is dit vereiste van uitdrukkelijke toestemming van de betalingsdienstgebruiker niet van toepassing op de AISP's. Artikel 67, lid 2, onder a), van de PSD2 voorziet echter nog steeds in uitdrukkelijke toestemming van de AISP's voor de verlening van de dienst.

 Zoals hierboven vermeld, is de lijst van wettige grondslagen voor de verwerking in het kader van de AVG uitputtend. Zoals vermeld in punt 14 is de rechtsgrondslag voor de verwerking van persoonsgegevens voor het verlenen van betalingsdiensten in beginsel artikel 6, lid 1, onder b), van de AVG, wat betekent dat de verwerking noodzakelijk is voor de uitvoering van een contract waarbij de betrokkene partij is of om op verzoek van de betrokkene maatregelen te nemen voordat een contract wordt gesloten. Hieruit volgt dat artikel 94, lid 2, van de PSD2 niet kan worden beschouwd als een aanvullende rechtsgrondslag voor de verwerking van persoonsgegevens. De EDPB is van mening dat dit lid, gelet op het voorgaande, enerzijds moet worden geïnterpreteerd in samenhang met het toepasselijke rechtskader voor gegevensbescherming en anderzijds op een wijze die het nuttig effect ervan behoudt. De uitdrukkelijke toestemming uit hoofde van artikel 94, lid 2, van de PSD2 moet derhalve worden beschouwd als een aanvullend vereiste van contractuele aard met betrekking[[19]](#footnote-19) tot de toegang tot en de daaropvolgende verwerking en opslag van persoonsgegevens met het oog op het aanbieden van betalingsdiensten en is derhalve niet hetzelfde als (uitdrukkelijke) toestemming uit hoofde van de AVG.

 "Uitdrukkelijke toestemming" als bedoeld in artikel 94, lid 2 PSD2 is een contractuele toestemming. Dit houdt in dat artikel 94, lid 2, van de richtlijn betalingsdiensten2 in die zin moet worden geïnterpreteerd dat de betrokkenen bij het sluiten van een contract met een betalingsdienstaanbieder in het kader van de richtlijn betalingsdiensten2 volledig op de hoogte moeten worden gebracht van de specifieke categorieën persoonsgegevens die zullen worden verwerkt. Voorts moeten zij op de hoogte worden gebracht van het specifieke (betalingsdienst)doel waarvoor hun persoonsgegevens zullen worden verwerkt en moeten zij uitdrukkelijk met deze clausules instemmen. Dergelijke clausules moeten duidelijk te onderscheiden zijn van de andere zaken die in het contract worden behandeld en moeten uitdrukkelijk door de betrokkene worden aanvaard.

 Centraal in het begrip "uitdrukkelijke toestemming" in het kader van artikel 94, lid 2, van de richtlijn betalingsdiensten2 staat het verkrijgen van toegang tot persoonsgegevens om deze vervolgens te verwerken en op te slaan met het oog op het aanbieden van betalingsdiensten. Dit houdt in dat de betalingsdienstaanbieder de persoonsgegevens nog niet verwerkt, maar toegang moet krijgen tot persoonsgegevens die onder de verantwoordelijkheid van een andere voor de verwerking verantwoordelijke zijn verwerkt. Indien een betalingsdienstgebruiker een contract afsluit met bijvoorbeeld een betalingsdienstaanbieder, moet deze aanbieder toegang krijgen tot de persoonsgegevens van de betalingsdienstgebruiker die worden verwerkt onder de verantwoordelijkheid van de betalingsdienstaanbieder die de rekening onderhoudt. Het doel van de uitdrukkelijke toestemming op grond van artikel 94, lid 2, van de richtlijn betalingsdiensten2 is het verkrijgen van toegang tot die persoonsgegevens, om deze persoonsgegevens die nodig zijn voor het aanbieden van de betalingsdienst, te kunnen verwerken en opslaan. Indien de betrokkene uitdrukkelijk toestemming verleent, is de betalingsdienstaanbieder van de rekening verplicht toegang te verlenen tot de aangegeven persoonsgegevens.

 Hoewel de toestemming van artikel 94, lid 2, van de PSD2 geen wettelijke grond is voor de verwerking van persoonsgegevens, houdt deze toestemming specifiek verband met persoonsgegevens en gegevensbescherming en zorgt zij voor transparantie en een zekere mate van controle voor de betalingsdienstgebruiker24. Hoewel in de PSD2 de materiële voorwaarden voor toestemming op grond van artikel 94, lid 2, van de PSD2 niet worden gespecificeerd, moet zij, zoals hierboven is vermeld, worden opgevat in samenhang met het toepasselijke rechtskader inzake gegevensbescherming en op een wijze die het nuttige effect ervan behoudt.

 Met betrekking tot de door de voor de verwerking verantwoordelijken te verstrekken informatie en de eis van transparantie wordt in de richtsnoeren van de Groep voor transparantie van artikel 29 het volgende bepaald: "*Een centrale overweging van het in deze bepalingen uiteengezette transparantiebeginsel is dat de betrokkene van tevoren moet kunnen bepalen wat de omvang en de gevolgen van de verwerking zijn en dat hij niet op een later tijdstip mag worden verrast over de wijze waarop zijn persoonsgegevens zijn gebruikt*".[[20]](#footnote-20)

 Voorts moeten, overeenkomstig het beginsel van doelbinding, persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld (artikel 5, lid 1, onder b), van de AVG). Wanneer persoonsgegevens voor meer dan één doel worden verzameld, "*moeten de voor de verwerking verantwoordelijken vermijden slechts één algemeen doel te identificeren om verschillende verdere verwerkingsactiviteiten te rechtvaardigen die in feite slechts op afstand verband houden met het eigenlijke oorspronkelijke doel*".[[21]](#footnote-21) De EDPB heeft, onlangs nog in het kader van contracten voor onlinediensten, gewezen op het risico dat algemene verwerkingsvoorwaarden in contracten worden opgenomen en heeft verklaard dat het doel van de verzameling duidelijk en specifiek moet worden vastgesteld: het moet voldoende gedetailleerd zijn om te bepalen wat voor soort verwerking wel en niet onder het gespecificeerde doel valt, en om te kunnen beoordelen of de wet wordt nageleefd en of er waarborgen voor de gegevensbescherming worden toegepast.[[22]](#footnote-22)

 In het kader van het aanvullende vereiste van uitdrukkelijke toestemming overeenkomstig artikel 94, lid 2, van de PSD2 houdt dit in dat de voor de verwerking verantwoordelijken de betrokkenen specifieke en uitdrukkelijke informatie moeten verstrekken over de specifieke doeleinden die door de voor de verwerking verantwoordelijke zijn vastgesteld en waarvoor hun persoonsgegevens worden opgevraagd, verwerkt en bewaard. Overeenkomstig artikel 94, lid 2, van de PSD2 moeten de betrokkenen deze specifieke doeleinden uitdrukkelijk aanvaarden.

 Bovendien benadrukt de EDPB, zoals hierboven in punt 9 is uiteengezet, dat de betalingsdienstgebruiker moet kunnen kiezen of hij al dan niet van de dienst gebruik wil maken en niet kan worden gedwongen dit te doen. Daarom moet de toestemming op grond van artikel 94, lid 2, van de PSD2 ook een vrij gegeven toestemming zijn.

## 3.3Conclusie

 Expliciete toestemming in het kader van de PSD2 is anders dan (expliciete) toestemming in het kader van de AVG. Expliciete toestemming op grond van artikel 94, lid 2, van de PSD2 is een aanvullend vereiste van contractuele aard. Wanneer een betalingsdienstaanbieder voor de verlening van een betalingsdienst toegang tot persoonsgegevens nodig heeft, is uitdrukkelijke toestemming overeenkomstig artikel 94, lid 2, van de PSD2 van de betalingsdienstgebruiker vereist.

# 4 DE VERWERKING VAN GEGEVENS VAN STILLE PARTIJEN

## 4.1Stille partijgegevens

 Een kwestie van gegevensbescherming die zorgvuldig moet worden overwogen, is de verwerking van zogenaamde 'silent party data'. In de context van dit document zijn gegevens van stille partijen persoonsgegevens van een betrokkene die niet de gebruiker van een specifieke betalingsdienstaanbieder is, maar wiens persoonsgegevens door die specifieke betalingsdienstaanbieder worden verwerkt voor de uitvoering van een contract tussen de aanbieder en de betalingsdienstgebruiker. Dit is bijvoorbeeld het geval wanneer een betalingsdienstgebruiker, betrokkene A, gebruik maakt van de diensten van een AISP, en betrokkene B een reeks betalingstransacties heeft verricht op de betaalrekening van betrokkene A. In dit geval wordt betrokkene B beschouwd als de "stille partij" en worden de persoonsgegevens (zoals het rekeningnummer van betrokkene B en het geldbedrag dat met deze transacties gemoeid was) die betrekking hebben op betrokkene B, beschouwd als "stille partijgegevens".

## 4.2Het rechtmatige belang van de voor de verwerking verantwoordelijke

 Artikel 5, lid 1, onder b), van het AVG vereist dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en niet verder worden verwerkt op een wijze die onverenigbaar is met die doeleinden. Bovendien vereist de AVG dat elke verwerking van persoonsgegevens zowel noodzakelijk als proportioneel is en in overeenstemming met de andere beginselen van gegevensbescherming, zoals de beginselen van doelbinding en gegevensminimalisering.

 De AVG kan de verwerking van gegevens van derden toestaan wanneer deze verwerking noodzakelijk is voor de gerechtvaardigde belangen van een voor de verwerking verantwoordelijke of een derde (artikel 6, lid 1, onder f), van de AVG). Een dergelijke verwerking kan echter alleen plaatsvinden wanneer het gerechtvaardigde belang van de voor de verwerking verantwoordelijke niet "zwaarder weegt dan de belangen of de fundamentele rechten en vrijheden van de betrokkene die de bescherming van persoonsgegevens vereisen".

 Een rechtmatige basis voor de verwerking van gegevens van derden door PISP’s en AISP's - in het kader van de verlening van betalingsdiensten in het kader van de PSD2 - zou dus het rechtmatige belang van een voor de verwerking verantwoordelijke of een derde kunnen zijn om het contract met de gebruiker van de betalingsdienst uit te voeren. De noodzaak om persoonsgegevens van de stille partij te verwerken is beperkt en wordt bepaald door de redelijke verwachtingen van deze betrokkenen. In het kader van het verlenen van betalingsdiensten die onder de PSD2 vallen, moeten door alle betrokken partijen doeltreffende en passende maatregelen worden genomen om te waarborgen dat de belangen of fundamentele rechten en vrijheden van de stille partijen niet worden overruled en om ervoor te zorgen dat de redelijke verwachtingen van deze betrokkenen ten aanzien van de verwerking van hun persoonsgegevens worden gerespecteerd. In dit verband moet de voor de verwerking verantwoordelijke de nodige waarborgen voor de verwerking vaststellen om de rechten van de betrokkenen te beschermen. Dit omvat technische maatregelen om ervoor te zorgen dat gegevens van stille partijen niet worden verwerkt voor een ander doel dan het doel waarvoor de persoonsgegevens oorspronkelijk door de PISP’s en de AISP's zijn verzameld. Indien mogelijk moeten ook encryptie- of andere technieken worden toegepast om een passend niveau van beveiliging en minimalisering van de gegevens te bereiken.

## 4.3Nadere verwerking van persoonsgegevens van de zwijgende partij

 Zoals vermeld in paragraaf 29 kunnen persoonsgegevens die worden verwerkt in verband met een door de PSD2 gereguleerde betalingsdienst, verder worden verwerkt op basis van wettelijke verplichtingen die op de dienstverlener rusten. Deze wettelijke verplichtingen kunnen betrekking hebben op persoonsgegevens van de stille partij.

 Met betrekking tot de verdere verwerking van gegevens van stille partijen op basis van rechtmatige belangen is de EDPB van mening dat deze gegevens niet kunnen worden gebruikt voor een ander doel dan waarvoor de persoonsgegevens zijn verzameld, andere op basis van de wetgeving van de EU of de lidstaten. Toestemming van de zwijgende partij is juridisch niet haalbaar, omdat voor het verkrijgen van toestemming persoonsgegevens van de zwijgende partij zouden moeten worden verzameld of verwerkt, waarvoor geen rechtsgrond kan worden gevonden op grond van artikel 6 van het AVG. De verenigbaarheidstoets van artikel 6, lid 4, van de AVG kan evenmin een grond bieden voor de verwerking voor andere doeleinden (bv. direct-marketingactiviteiten). De rechten en vrijheden van deze stille partijen worden niet gerespecteerd indien de nieuwe verantwoordelijke voor de verwerking de persoonsgegevens voor andere doeleinden gebruikt, rekening houdend met de context waarin de persoonsgegevens zijn verzameld, met name het ontbreken van enige relatie met de stille partijen[[23]](#footnote-23); het ontbreken van enig verband tussen enig ander doel en het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld (i.e. het feit dat betalingsdienstaanbieders de gegevens van de stille partij alleen nodig hebben voor de uitvoering van een overeenkomst met de andere contractpartij); de aard van de betrokken persoonsgegevens[[24]](#footnote-24), de omstandigheid dat de betrokkenen redelijkerwijs geen verdere verwerking kunnen verwachten of zelfs maar weten welke voor de verwerking verantwoordelijke hun persoonsgegevens verwerkt en gelet op de wettelijke beperkingen op de verwerking die in artikel 66, lid 3, onder g), en artikel 67, lid 2, onder f), van de richtlijn betalingsdiensten2 zijn vastgesteld.

# 5 DE VERWERKING VAN BIJZONDERE CATEGORIEËN VAN PERSOONSGEGEVENS IN HET KADER VAN DE PSD2

## 5.1Speciale categorieën van persoonsgegevens

 Artikel 9, lid 1, van het AVG verbiedt de verwerking van "persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijkt, alsmede de verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, gegevens over de gezondheid of gegevens over het seksleven of de seksuele geaardheid van een natuurlijke persoon".

 Er moet worden benadrukt dat elektronische betalingen in sommige lidstaten alomtegenwoordig zijn en door veel mensen worden bevoordeeld ten opzichte van contante betalingen in hun dagelijkse transacties. Tegelijkertijd kunnen financiële transacties gevoelige informatie over individuele personen aan het licht brengen, met inbegrip van informatie over speciale categorieën van persoonsgegevens. Zo kunnen bijvoorbeeld politieke meningen en religieuze overtuigingen worden onthuld door donaties aan politieke partijen of organisaties, kerken of parochies. Vakbondslidmaatschap kan worden onthuld door het in mindering brengen van een jaarlijkse lidmaatschapsbijdrage op iemands bankrekening. Persoonlijke gegevens over de gezondheid kunnen worden verzameld uit de analyse van medische rekeningen die door een betrokkene zijn betaald. Ten slotte kan informatie over bepaalde aankopen informatie over het seksleven of de seksuele geaardheid van een persoon onthullen. Zoals uit deze voorbeelden blijkt, kunnen zelfs afzonderlijke transacties speciale categorieën van persoonsgegevens bevatten. Bovendien kunnen door de som van de financiële transacties verschillende soorten gedragspatronen aan het licht komen, waaronder speciale categorieën persoonsgegevens en aanvullende diensten die worden gefaciliteerd door rekeninginformatiediensten, die kunnen berusten op profilering zoals gedefinieerd in artikel 4, lid 4, van de AVG. De kans is dan ook groot dat een dienstverlener die informatie over financiële transacties van betrokkenen verwerkt, ook speciale categorieën persoonsgegevens verwerkt.

 Met betrekking tot de term "gevoelige betalingsgegevens" merkt de EDPB het volgende op. De definitie van gevoelige betalingsgegevens in de PSD2 verschilt aanzienlijk van de manier waarop de term "gevoelige persoonsgegevens" gewoonlijk wordt gebruikt in het kader van de AVG en de gegevensbescherming (wet). Waar de PSD2 "gevoelige betalingsgegevens" definieert als "gegevens, met inbegrip van gepersonaliseerde veiligheidsgegevens die kunnen worden gebruikt om fraude te plegen", benadrukt de AVG de noodzaak van specifieke bescherming van speciale categorieën van persoonsgegevens die krachtens artikel 9 van de AVG door hun aard bijzonder gevoelig zijn met betrekking tot de fundamentele rechten en vrijheden, zoals speciale categorieën van persoonsgegevens.[[25]](#footnote-25) In dit verband wordt aanbevolen om ten minste in kaart te brengen en te categoriseren wat voor soort persoonsgegevens er precies zullen worden verwerkt. Waarschijnlijk zal een effectbeoordeling voor gegevensbescherming (DPIA) nodig zijn overeenkomstig artikel 35 van het AVG, wat zal helpen bij het in kaart brengen van de gegevens.

## 5.2Mogelijke afwijkingen

 Het verbod van artikel 9 van het AVG is niet absoluut. Hoewel de afwijkingen van artikel 9, lid 2, onder b) tot en met f) en h) tot en met j), duidelijk niet van toepassing zijn op de verwerking van persoonsgegevens in het kader van de PSD2 , kunnen met name de volgende twee afwijkingen van artikel 9, lid 2, van de AVG worden overwogen:

 Het verbod is niet van toepassing indien de betrokkene uitdrukkelijk toestemming heeft gegeven voor de verwerking van die persoonsgegevens voor een of meer specifieke doeleinden (artikel 9, lid 2, onder a), van het AVG).

 Het verbod is niet van toepassing indien de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang, op grond van het recht van de Unie of van de lidstaten, dat in verhouding moet staan tot het nagestreefde doel, de essentie van het recht op gegevensbescherming moet eerbiedigen en moet voorzien in passende en specifieke maatregelen ter bescherming van de grondrechten en de belangen van de betrokkene (artikel 9, lid 2, onder g), van het AVG).

 Er zij op gewezen dat de lijst van afwijkingen in artikel 9, lid 2, van het AVG uitputtend is. De mogelijkheid dat speciale categorieën persoonsgegevens worden opgenomen in de persoonsgegevens die worden verwerkt voor het verlenen van een van de diensten die onder de PSD2 vallen, moet door de dienstverlener worden erkend. Aangezien het verbod van artikel 9, lid 1, van de AVG op deze dienstverleners van toepassing is, moeten zij ervoor zorgen dat een van de uitzonderingen van artikel 9, lid 2, van de AVG op hen van toepassing is. Benadrukt moet worden dat wanneer de dienstverlener niet kan aantonen dat aan een van de uitzonderingen is voldaan, het verbod van artikel 9, lid 1, van toepassing is.

## 5.3Aanzienlijk algemeen belang

 Betalingsdiensten mogen om redenen van zwaarwegend algemeen belang bijzondere categorieën persoonsgegevens verwerken, maar alleen als aan alle voorwaarden van artikel 9, lid 2, onder g), van de AVG is voldaan. Dit betekent dat de verwerking van de speciale categorieën persoonsgegevens moet worden geregeld in een specifieke afwijking van artikel 9, lid 1, van de AVG in de wetgeving van de Unie of van de lidstaten. Deze bepaling moet betrekking hebben op de evenredigheid met het nagestreefde doel van de verwerking en moet passende en specifieke maatregelen bevatten om de grondrechten en de belangen van de betrokkene te beschermen. Voorts zal deze bepaling in het recht van de Unie of van de lidstaten de essentie van het recht op gegevensbescherming moeten eerbiedigen. Ten slotte moet ook worden aangetoond dat de verwerking van de speciale categorieën gegevens noodzakelijk is in verband met het wezenlijke openbare belang, met inbegrip van het belang van het systeem. Pas als aan al deze voorwaarden is voldaan, kan deze afwijking van toepassing worden verklaard op aangewezen soorten betalingsdiensten.

## 5.4Expliciete toestemming

 In gevallen waarin de afwijking van artikel 9, lid 2, onder g), van het AVG niet van toepassing is, lijkt het verkrijgen van uitdrukkelijke toestemming overeenkomstig de voorwaarden voor geldige toestemming in het AVG de enige mogelijke wettelijke afwijking te blijven voor de verwerking van bijzondere categorieën van persoonsgegevens door TPP's. In de EDPB-richtsnoeren 05/2020 inzake toestemming op grond van Verordening 2016/679 staat[[26]](#footnote-26) dat: "Artikel 9, lid 2, erkent niet "noodzakelijk voor de uitvoering van een overeenkomst" als een uitzondering op het algemene verbod om bijzondere categorieën van gegevens te verwerken. Daarom moeten de voor de verwerking verantwoordelijken en de lidstaten die zich met deze situatie bezighouden, de specifieke uitzonderingen van artikel 9, lid 2, onder b) tot en met j), onderzoeken. Wanneer dienstverleners zich beroepen op artikel 9, lid 2, onder a), van het AVG, moeten zij zich ervan vergewissen dat hun uitdrukkelijke toestemming is verleend voordat zij met de verwerking beginnen". De uitdrukkelijke toestemming als bedoeld in artikel 9, lid 2, onder a), van de AVG moet aan alle eisen van de AVG voldoen. Dit geldt ook voor gegevens van stille partijen.

## 5.5Geen passende afwijking

 Zoals hierboven is opgemerkt, is het verbod van artikel 9, lid 1, van toepassing wanneer de dienstverlener niet kan aantonen dat aan een van de afwijkingen is voldaan. In dat geval moeten technische maatregelen worden genomen om de verwerking van bijzondere categorieën van persoonsgegevens te voorkomen, bijvoorbeeld door de verwerking van bepaalde gegevenspunten te verhinderen. In dit verband kunnen betalingsdienstaanbieders de technische mogelijkheden onderzoeken om bijzondere categorieën van persoonsgegevens uit te sluiten en een geselecteerde toegang toe te staan, waardoor de verwerking van bijzondere categorieën van persoonsgegevens met betrekking tot stille partijen door betalingsdienstaanbieders zou worden voorkomen.

# 6 GEGEVENS MINIMALISEREN, BEVEILIGING, TRANSPARANTIE, VERANTWOORDING EN PROFILERING

## 6. 1Gegevensminimalisatie en gegevensbescherming door ontwerp en standaard

 Het beginsel van gegevensminimalisatie is vastgelegd in artikel 5, lid 1, onder c), van het AVG: "Persoonsgegevens zijn [...] adequaat, ter zake dienend en beperkt tot hetgeen noodzakelijk is in verband met de doeleinden waarvoor zij worden verwerkt". Op grond van het beginsel van minimalisering van de hoeveelheid gegevens mogen de voor de verwerking verantwoordelijken niet meer persoonsgegevens verwerken dan nodig is om het specifieke doel in kwestie te bereiken. Zoals in hoofdstuk 2 is aangegeven, worden de hoeveelheid en het soort persoonsgegevens dat nodig is om de betalingsdienst te verlenen, bepaald door het objectieve en wederzijds begrepen contractuele doel[[27]](#footnote-27). De minimalisering van de gegevens is van toepassing op elke verwerking (bv. elke verzameling van of toegang tot en elk verzoek om persoonsgegevens). In de EDPB-richtsnoeren 4/2019 over artikel 25 "Gegevensbescherming door ontwerp en standaard" staat dat "verwerkers en aanbieders van technologie zich er ook van bewust moeten zijn dat de voor de verwerking verantwoordelijken alleen persoonsgegevens moeten verwerken met systemen en technologieën die een ingebouwde gegevensbescherming hebben".[[28]](#footnote-28)

 Artikel 25 van de AVG bevat de verplichtingen tot toepassing van de gegevensbescherming bij wijze van ontwerp en bij gebrek aan beter. Deze verplichtingen zijn van bijzonder belang voor het beginsel van minimalisering van de gegevens. In dit artikel wordt bepaald dat de voor de verwerking verantwoordelijke zowel bij de vaststelling van de middelen voor de verwerking als bij de verwerking zelf passende technische en organisatorische maatregelen ten uitvoer moet leggen om de gegevensbeschermingsbeginselen op doeltreffende wijze ten uitvoer te leggen en de nodige waarborgen in de verwerking te integreren om aan de eisen van de AVG te voldoen en de rechten van de betrokkenen te beschermen. De voor de verwerking verantwoordelijke voert passende technische en organisatorische maatregelen uit om ervoor te zorgen dat standaard alleen persoonsgegevens worden verwerkt die voor elk specifiek doel van de verwerking noodzakelijk zijn. Deze verplichting geldt voor de hoeveelheid verzamelde persoonsgegevens, de omvang van de verwerking ervan, de duur van de opslag en de toegankelijkheid ervan. Deze maatregelen kunnen encryptie, pseudonimisering en andere technische maatregelen omvatten.

 Bij de toepassing van de verplichting van artikel 25 van de AVG moet rekening worden gehouden met de stand van de techniek, de kosten van de uitvoering, de aard, de omvang, de context en de doeleinden van de verwerking, alsmede met de risico's van wisselende waarschijnlijkheid en ernst van de rechten en vrijheden van natuurlijke personen die de verwerking met zich meebrengt. Verdere verduidelijkingen van deze verplichting worden gegeven in de bovengenoemde EDPB-richtsnoeren 4/2019 betreffende artikel 25 Gegevensbescherming door ontwerp en door wanbetaling.

## 6. 2D-gegevensminimalisatiemaatregelen

 De TPP die toegang heeft tot de gegevens van de betaalrekening om de gevraagde diensten te verlenen, moet ook rekening houden met het beginsel van gegevensminimalisatie en mag alleen persoonsgegevens verzamelen die nodig zijn om de specifieke betalingsdiensten te verlenen waarom de betalingsdienstgebruiker heeft verzocht. In beginsel moet de toegang tot de persoonsgegevens worden beperkt tot hetgeen noodzakelijk is voor het aanbieden van betalingsdiensten. Zoals in hoofdstuk 2 is aangetoond, vereist de PSD2 dat ASPSP's op verzoek van de PSU informatie over de PSU delen wanneer de PSU een betalingsinitiëringsdienst of een rekeninginformatiedienst wenst te gebruiken.

 Wanneer niet alle gegevens van de betaalrekening nodig zijn voor de levering van de overeenkomst, moet de AISP een selectie van de relevante gegevenscategorieën maken voordat de gegevens worden verzameld. Zo kunnen de gegevenscategorieën die niet noodzakelijk zijn, bijvoorbeeld de identiteit van de stille partij en de transactiekenmerken omvatten. Ook is het mogelijk dat het IBAN van de bankrekening van de stille partij niet hoeft te worden weergegeven, tenzij dit op grond van de wetgeving van de lidstaat of van de EU vereist is.

 In dit verband kan, in het kader van de uitvoering van een passend gegevensbeschermingsbeleid, in overeenstemming met artikel 24, lid 2, van het AVG worden overwogen om technische maatregelen toe te passen die de PTB's in staat stellen of ondersteunen bij hun verplichting om alleen de persoonsgegevens te raadplegen en op te vragen die nodig zijn voor het verlenen van hun diensten. In dit verband beveelt de EDPB het gebruik van digitale filters aan om de AISP's te ondersteunen bij hun verplichting om alleen persoonsgegevens te verzamelen die nodig zijn voor de doeleinden waarvoor zij worden verwerkt. Wanneer een dienstverlener bijvoorbeeld de transactiekenmerken (in het beschrijvingsveld van de transactieregisters) niet nodig heeft voor het verlenen van zijn dienst, zou een filter kunnen fungeren als een hulpmiddel voor TPP's om dit veld uit te sluiten van de algemene verwerkingsoperaties door de TPP.

 In dit verband moet ook worden opgemerkt dat volgens de PSD2 ASPSP's alleen toegang mogen verlenen tot informatie over betaalrekeningen. In het kader van de PSD2 is er geen rechtsgrondslag om toegang te verlenen met betrekking tot persoonsgegevens die op andere rekeningen staan, zoals spaar-, hypotheek- of beleggingsrekeningen. Daarom moeten in het kader van de PSD2 technische maatregelen worden genomen om ervoor te zorgen dat de toegang wordt beperkt tot de noodzakelijke informatie over betaalrekeningen.

 Naast het verzamelen van zo weinig mogelijk gegevens moet de dienstverlener ook een beperkte bewaartermijn hanteren. Persoonlijke gegevens mogen door de dienstverlener niet langer worden bewaard dan nodig is in verband met de door de betalingsdienstgebruiker gevraagde doeleinden.

 Indien het contract tussen de betrokkene en de AISP de overdracht van persoonsgegevens aan derden vereist, kunnen alleen die persoonsgegevens worden overgedragen die noodzakelijk zijn voor de uitvoering van het contract. De betrokkenen moeten ook specifiek worden geïnformeerd over de overdracht en de persoonsgegevens die aan deze derde partij zullen worden doorgegeven.

## 6.3 Veiligheid

 De EDPB heeft er al op gewezen dat de schending van financiële persoonsgegevens *"duidelijk ernstige gevolgen heeft voor het dagelijks leven van de betrokkene*" en noemt als voorbeeld de risico's van betalingsfraude.[[29]](#footnote-29)

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

 De voor de verwerking verantwoordelijken zijn verplicht passende maatregelen te nemen om de persoonsgegevens van de betrokkenen te beschermen.

(Artikel 24, lid 1, AVG). Hoe hoger de risico's die verbonden zijn aan de door de voor de verwerking verantwoordelijke uitgevoerde activiteit, hoe hoger de veiligheidsnormen die moeten worden toegepast. Aangezien de verwerking van financiële gegevens met verschillende ernstige risico's gepaard gaat, moeten de beveiligingsmaatregelen dienovereenkomstig hoog zijn.

 Dienstverleners moeten worden gehouden aan hoge normen, waaronder sterke klantenauthenticatiemechanismen en hoge veiligheidsnormen voor de technische apparatuur.[[30]](#footnote-30) Ook andere procedures, zoals het doorlichten van de verwerkers van de veiligheidsnormen en het uitvoeren van procedures tegen ongeoorloofde toegang, zijn van belang.

## 6.4Transparantie en verantwoording

 Transparantie en verantwoordingsplicht zijn twee fundamentele beginselen van de AVG.

 Met betrekking tot de transparantie (artikel 5, lid 1, onder a), van de AVG) wordt in artikel 12 van de AVG bepaald dat de voor de verwerking verantwoordelijken passende maatregelen moeten nemen om de in de artikelen 13 en 14 van de AVG bedoelde informatie te verstrekken. Voorts moet de informatie of mededeling over de verwerking van persoonsgegevens beknopt, transparant, begrijpelijk en gemakkelijk toegankelijk zijn. De informatie moet in duidelijke en duidelijke taal en schriftelijk worden verstrekt "of op een andere wijze, waaronder, in voorkomend geval, langs elektronische weg". De Groep artikel 29 "Richtsnoeren inzake transparantie in het kader van Verordening 2016/679", zoals bekrachtigd door de EDPB, biedt specifieke richtsnoeren voor de naleving van het beginsel van transparantie in digitale omgevingen.

 Voor de diensten in het kader van de PSD2 is artikel 13 van de AVG van toepassing op de persoonsgegevens die van de betrokkene worden verzameld en artikel 14 op de persoonsgegevens die niet van de betrokkene zijn verkregen.

 De betrokkene moet met name worden geïnformeerd over de periode waarin de persoonsgegevens zullen worden opgeslagen of, indien dat niet mogelijk is, over de criteria die worden gehanteerd om die periode vast te stellen en, indien van toepassing, over de gerechtvaardigde belangen die door de voor de verwerking verantwoordelijke of door een eventuele derde worden nagestreefd. Wanneer de verwerking gebaseerd is op toestemming als bedoeld in artikel 6, lid 1, onder a), van het AVG of op uitdrukkelijke toestemming als bedoeld in artikel 9, lid 2, onder a), van het AVG, moet de betrokkene worden geïnformeerd over het bestaan van het recht om zijn of haar toestemming te allen tijde in te trekken.

 De voor de verwerking verantwoordelijke verstrekt de informatie aan de betrokkene, rekening houdend met de specifieke omstandigheden waarin de persoonsgegevens worden verwerkt. Indien de persoonsgegevens worden gebruikt voor de communicatie met de betrokkene[[31]](#footnote-31), wat waarschijnlijk het geval zal zijn voor AISP's, moet de informatie uiterlijk op het moment van de eerste communicatie aan de betrokkene worden verstrekt. Indien persoonsgegevens aan een andere ontvanger moeten worden verstrekt, dient de informatie uiterlijk op het moment van de eerste verstrekking van de persoonsgegevens te worden verstrekt.

 Met betrekking tot onlinebetalingsdiensten wordt in de bovengenoemde richtsnoeren verduidelijkt dat de voor de verwerking verantwoordelijken een gelaagde aanpak kunnen volgen wanneer zij ervoor kiezen een combinatie van methoden te gebruiken om de transparantie te waarborgen. Met name wordt aanbevolen om gelaagde privacyverklaringen/-kennisgevingen te gebruiken om een verband te leggen met de verschillende categorieën informatie die aan de betrokkene moeten worden verstrekt, in plaats van al deze informatie in één enkele kennisgeving op een scherm weer te geven, teneinde informatiemoeheid te voorkomen en tegelijkertijd de doeltreffendheid van de informatie te waarborgen.

 In de bovengenoemde richtsnoeren wordt ook verduidelijkt dat de voor de verwerking verantwoordelijken ervoor kunnen kiezen aanvullende instrumenten te gebruiken om informatie te verstrekken aan de individuele betrokkene, zoals privacydashboards. Een privacydashboard is een enkel punt van waaruit betrokkenen "privacyinformatie" kunnen bekijken en hun privacyvoorkeuren kunnen beheren door toe te staan of te voorkomen dat hun gegevens op bepaalde manieren door de voor de verwerking verantwoordelijke in kwestie worden gebruikt.[[32]](#footnote-32) Een privacydashboard zou een overzicht kunnen geven van de TPP's die de betrokkenen uitdrukkelijk toestemming hebben gekregen en zou ook relevante informatie kunnen bieden over de aard en de hoeveelheid persoonsgegevens die door TPP's zijn opgevraagd. In principe kan een ASPSP de gebruiker de mogelijkheid bieden om[[33]](#footnote-33) via het overzicht een specifieke uitdrukkelijke toestemming van PSD2 in te trekken, wat zou resulteren in een weigering van toegang tot zijn betaalrekeningen aan een of meer TPPs. De gebruiker zou een ASPSP ook kunnen verzoeken de toegang tot zijn betaalrekening(en) te weigeren aan een of meer specifieke TPP's39 , aangezien de gebruiker het recht heeft om (geen) gebruik te maken van een rekeninginformatiedienst. Indien privacydashboards worden gebruikt om een expliciete toestemming te geven of in te trekken, moeten deze op legale wijze worden ontworpen en toegepast en moet met name worden voorkomen dat er belemmeringen ontstaan voor het recht van de TPP's om diensten te verlenen in overeenstemming met de PSD2. In dit verband en in overeenstemming met de toepasselijke bepalingen van de PSD2 heeft een TPP de mogelijkheid om na intrekking van deze toestemming opnieuw uitdrukkelijke toestemming van de gebruiker te verkrijgen.

 Het verantwoordingsbeginsel vereist dat de voor de verwerking verantwoordelijke passende technische en organisatorische maatregelen vaststelt om te waarborgen en aan te kunnen tonen dat de verwerking wordt uitgevoerd in overeenstemming met de AVG, in het bijzonder met de belangrijkste gegevensbeschermingsbeginselen als bedoeld in artikel 5, lid 1. Deze maatregelen moeten rekening houden met de aard, de omvang, de context en de doeleinden van de verwerking en het risico voor de rechten en vrijheden van natuurlijke personen, en moeten indien nodig worden herzien en bijgewerkt. 40

## 6.5Profilering

 De verwerking van persoonsgegevens door betalingsdienstaanbieders kan "profilering" als bedoeld in artikel 4, lid 4, van de AVG met zich meebrengen. De AISP's zouden bijvoorbeeld kunnen vertrouwen op een geautomatiseerde verwerking van persoonsgegevens om bepaalde persoonlijke aspecten met betrekking tot een natuurlijke persoon te beoordelen. De persoonlijke financiële situatie van de betrokkene zou kunnen worden geëvalueerd, afhankelijk van de specifieke kenmerken van de dienst. Rekeninginformatiediensten, die op verzoek van de gebruikers moeten worden verstrekt, kunnen een uitgebreide evaluatie van de gegevens van persoonlijke betaalrekeningen omvatten.

 De voor de verwerking verantwoordelijke moet ook transparant zijn voor de betrokkene over het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering. In die gevallen moet de voor de verwerking verantwoordelijke zinvolle informatie verstrekken over de betrokken logica, alsmede over de betekenis en de beoogde gevolgen van een dergelijke verwerking voor de betrokkene (artikel 13, lid 2, onder f), en artikel 14, lid 2, onder g), en overweging 60).[[34]](#footnote-34)Evenzo heeft de betrokkene krachtens artikel 15 van de verordening inzake de bescherming van de persoonlijke levenssfeer het recht om bij de voor de verwerking verantwoordelijke informatie op te vragen en te verkrijgen over het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, de betrokken logica en de gevolgen daarvan 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.[[35]](#footnote-35)

 Wat in dit verband ook relevant is, is het recht van de betrokkene om niet te worden onderworpen aan een besluit dat uitsluitend gebaseerd is op geautomatiseerde verwerking, met inbegrip van profilering, die voor hem of haar rechtsgevolgen heeft of die hem of haar in aanzienlijke mate treft, zoals bepaald in artikel 22 van het AVG. Deze norm houdt ook in dat de voor de verwerking verantwoordelijken in bepaalde omstandigheden passende maatregelen moeten nemen om de rechten van de betrokkene te waarborgen, zoals specifieke informatieverstrekking aan de betrokkene, het recht op menselijk ingrijpen in de besluitvorming en het recht om zijn of haar standpunt kenbaar te maken en het besluit te betwisten. Zoals ook in overweging 71 van het AVG wordt gesteld, betekent dit onder meer dat de betrokkenen het recht hebben om niet aan een besluit te worden onderworpen, zoals de automatische weigering van een onlinekredietaanvraag zonder enige menselijke tussenkomst. 43

 Geautomatiseerde besluitvorming, met inbegrip van het opstellen van profielen met speciale categorieën persoonsgegevens, is alleen toegestaan onder de cumulatieve voorwaarden van artikel 22, lid 4, van het AVG:

* er is een vrijstelling op grond van artikel 22, lid 2, van toepassing;
* en artikel 9, lid 2, onder a) of g), van het AVG is van toepassing. In beide gevallen moet de voor de verwerking verantwoordelijke passende maatregelen nemen om de rechten en vrijheden en de gerechtvaardigde belangen van de betrokkene te beschermen.[[36]](#footnote-36)

 De eisen voor verdere verwerking, zoals vermeld in deze richtlijnen, moeten ook in acht worden genomen. De verduidelijkingen en instructies inzake geautomatiseerde individuele besluitvorming en profilering die de Werkgroep 29 Richtsnoeren inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening 2016/679 heeft gegeven, zoals bekrachtigd door de EDPB, zijn volledig relevant in de context van betalingsdiensten en moeten daarom naar behoren in overweging worden genomen.

Voor het Europees Comité voor gegevensbescherming

De voorzitter

(Andrea Jelinek)

1. Verwijzingen naar "lidstaten" in dit document moeten worden opgevat als verwijzingen naar "EER-lidstaten". [↑](#footnote-ref-1)
2. Overweging 6 PSD2. [↑](#footnote-ref-2)
3. Aangezien de PSD2 dateert van vóór de AVG, verwijst zij nog steeds naar Richtlijn 95/46. In artikel 94 van de AVG is bepaald dat verwijzingen naar de ingetrokken Richtlijn 95/46 moeten worden opgevat als verwijzingen naar de AVG. 4 Overweging 89, PSD2. [↑](#footnote-ref-3)
4. Kunst. 1 (1) AVG. [↑](#footnote-ref-4)
5. 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. 37 - 0047. [↑](#footnote-ref-5)
6. Kunst. 94 PSD etc. [↑](#footnote-ref-6)
7. Gedelegeerde Verordening (EU) nr. 2018/389 van de Commissie van 27 november 2017 tot aanvulling van Richtlijn (EU) nr. 2015/2366 van het Europees Parlement en de Raad met betrekking tot technische reguleringsnormen voor een sterke klantenauthenticatie en gemeenschappelijke en veilige open communicatienormen (Voor de EER relevante tekst); C/2017/7782; PB L 69 van 13.3.2018, blz. 23-43; beschikbaar op https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN . [↑](#footnote-ref-7)
8. Een rekeninginformatiedienst is een onlinedienst om geconsolideerde informatie te verstrekken over een of meer betaalrekeningen die de betalingsdienstgebruiker bij een andere betalingsdienstaanbieder of bij meer dan een betalingsdienstaanbieder aanhoudt. [↑](#footnote-ref-8)
9. Kunst. 4 (15) PSD2. 12 Art. 4 (16) PSD2. [↑](#footnote-ref-9)
10. De EDPB werkt momenteel aan richtsnoeren voor de begrippen "voor de verwerking verantwoordelijke" en "verwerker" in het kader van de AVG. [↑](#footnote-ref-10)
11. Richtsnoeren 2/2019 betreffende de verwerking van persoonsgegevens uit hoofde van artikel 6, lid 1, onder b), van het AVG in het kader van de verlening van onlinediensten aan betrokkenen, EDPB, blz. 9. [↑](#footnote-ref-11)
12. Idem. [↑](#footnote-ref-12)
13. Idem, pagina 8. [↑](#footnote-ref-13)
14. Idem, pagina 10. [↑](#footnote-ref-14)
15. Idem, pagina 11. [↑](#footnote-ref-15)
16. Merk op dat een grondig onderzoek naar de vraag of de anti-witwasrichtlijn voldoet aan de norm van de kunst. 6 (4) AVG valt buiten het toepassingsgebied van dit document. [↑](#footnote-ref-16)
17. Richtsnoeren 05/2020 inzake toestemming op grond van Verordening 2016/679, EDPB, alinea. 3. [↑](#footnote-ref-17)
18. Zie ook Advies 15/2011 over de definitie van toestemming (WP 187), blz. 6-8, en/of Advies 06/2014 over het begrip "rechtmatige belangen van de voor de verwerking verantwoordelijke" in de zin van artikel 7 van Richtlijn 95/46/EG (WP 217), blz. 9, 10, 13 en 14. [↑](#footnote-ref-18)
19. Brief van de EDPB met betrekking tot de PSD2-richtlijn, 5 juli 2018, blz. 4. 24 Art. 94 (2) PSD2 valt onder hoofdstuk 4 "Gegevensbescherming". [↑](#footnote-ref-19)
20. Artikel 29-werkgroep, richtsnoeren inzake transparantie in het kader van Verordening 2016/679, lid 10 (goedgekeurd op 11 april 2018) - bekrachtigd door de EDPB. [↑](#footnote-ref-20)
21. Artikel 29 Werkgroep Advies 03/2013 over doelbinding (WP203), blz. 16. [↑](#footnote-ref-21)
22. Richtsnoeren 2/2019 betreffende de verwerking van persoonsgegevens uit hoofde van artikel 6, lid 1, onder b), van het AVG in het kader van de verlening van onlinediensten aan betrokkenen, paragraaf 16 (versie openbare raadpleging) en advies 03/2013 van de Groep artikel 29 over doelbinding (WP203), blz. 15-16. [↑](#footnote-ref-22)
23. In overweging 87 van PSD2 staat dat PSD2 alleen betrekking heeft op "contractuele verplichtingen en verantwoordelijkheden tussen de betalingsdienstgebruiker en de betalingsdienstaanbieder". Gegevens van stille partijen vallen derhalve niet onder het toepassingsgebied van PSD2. [↑](#footnote-ref-23)
24. Er moet bijzondere aandacht worden besteed aan de verwerking van financiële persoonsgegevens, aangezien de verwerking kan worden beschouwd als een verhoging van het mogelijke risico voor de rechten en vrijheden van personen, overeenkomstig de richtsnoeren voor de effectbeoordeling van de gegevensbescherming (DPIA). [↑](#footnote-ref-24)
25. Zo worden in overweging 10 van de AVG speciale categorieën van persoonsgegevens aangeduid als "gevoelige gegevens". [↑](#footnote-ref-25)
26. Richtsnoeren 05/2020 inzake toestemming op grond van Verordening 2016/679, EDPB, alinea. 99 [↑](#footnote-ref-26)
27. Richtsnoeren 2/2019 betreffende de verwerking van persoonsgegevens uit hoofde van artikel 6, lid 1, onder b), van het bbp in het kader van de verlening van onlinediensten aan betrokkenen, EDPB, punt 32. [↑](#footnote-ref-27)
28. Richtsnoeren 4/2019 betreffende artikel 25 Gegevensbescherming naar ontwerp en standaard - versie voor openbare raadpleging, blz. 25. [↑](#footnote-ref-28)
29. Richtsnoeren van de Groep artikel 29 voor de effectbeoordeling van gegevensbescherming (DPIA) en het bepalen of verwerking "waarschijnlijk tot een hoog risico zal leiden" voor de toepassing van Verordening 2016/679, WP248 rev.01 - bekrachtigd door het EDPB. [↑](#footnote-ref-29)
30. Zie de RTS. [↑](#footnote-ref-30)
31. Kunst. 14, lid 3, onder b), van het AVG. [↑](#footnote-ref-31)
32. Volgens de richtsnoeren van de Groep artikel 29 inzake transparantie in het kader van Verordening 2016/679, WP 260 rev.01 - goedgekeurd door de EDPB - zijn privacydashboards bijzonder nuttig wanneer dezelfde dienst door de betrokkenen op verschillende apparaten wordt gebruikt, aangezien zij hen toegang geven tot en controle hebben over hun persoonsgegevens, ongeacht de wijze waarop zij de dienst gebruiken. Door de betrokkenen de mogelijkheid te bieden hun privacyinstellingen handmatig aan te passen via een privacydashboard, kan het ook gemakkelijker worden om een privacyverklaring/kennisgeving te personaliseren door alleen de soorten verwerking weer te geven die voor die specifieke betrokkene plaatsvinden. [↑](#footnote-ref-32)
33. Zie bijvoorbeeld de in artikel 67, lid 2, onder a), van de AVG genoemde "uitdrukkelijke toestemming"2. 39 Zie ook EBA/OP/2020/10, paragraaf 45 40 Art. 5, lid 2, en artikel 5, lid 1, onder a), van de PSD2. 24 AVG. [↑](#footnote-ref-33)
34. Artikel 29 Richtsnoeren van de werkgroep inzake transparantie in het kader van Verordening 2016/679, WP 260 rev.01 - bekrachtigd door de EDPB. [↑](#footnote-ref-34)
35. Artikel 29 Richtsnoeren van de werkgroep inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening 2016/679, WP251rev.01 43 Overweging 71 AVG. [↑](#footnote-ref-35)
36. Artikel 29 Richtsnoeren van de werkgroep inzake geautomatiseerde individuele besluitvorming en profilering voor de toepassing van Verordening 2016/679, WP251rev.01, blz. 24. [↑](#footnote-ref-36)