



Advies Raad van State inzake het voorstel van wet tot wijziging van de Wet op het financieel toezicht in verband met het via een centraal elektronisch systeem geautomatiseerd ontsluiten van identificerende gegevens door banken en andere betaaldienstverleners (Wet verwijzingsportaal bankgegevens)

Nader Rapport

2019-0000088919

Directie Financiële Markten

Aan de Koning

Nader rapport inzake het voorstel van wet tot wijziging van de Wet op het financieel toezicht in verband met het via een centraal elektronisch systeem geautomatiseerd ontsluiten van identificerende gegevens door banken en andere betaaldienstverleners (Wet verwijzingsportaal bankgegevens)

Blijkens de mededeling van de Directeur van Uw kabinet van 24 april 2019, nr. 2019000843, machtigde Uwe Majesteit de Afdeling advisering van de Raad van State haar advies inzake het bovenvermelde voorstel van wet rechtstreeks aan mij te doen toekomen. Dit advies, gedateerd 29 mei 2019, nr. W06.19.0106/III, bied ik U hierbij aan. De tekst van het advies is tevens hieronder opgenomen, voorzien van mijn reactie.

Bij Kabinetsmissive van 24 april 2019, no.2019000843, heeft Uwe Majesteit, op voordracht van de Minister van Financiën, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het voorstel van wet tot wijziging van de Wet op het financieel toezicht in verband met het via een centraal elektronisch systeem geautomatiseerd verstrekken en ontsluiten van identificerende gegevens door banken en betaaldienstverleners (Wet verwijzingsportaal bankgegevens), met memorie van toelichting.

Het voorstel regelt de inrichting van een Verwijzingsportaal bankgegevens (hierna: VB). Het doel hiervan is het proces van het verstrekken van bepaalde identificerende gegevens¹ door banken en andere betaaldienstverleners aan bepaalde overheidsinstanties efficiënter te laten verlopen.

De Afdeling advisering van de Raad van State vestigt de aandacht op de waarborgen voor gegevensverwerking bij de introductie van deze digitale techniek, de beveiligingsrisico's voor banken, betaaldienstverleners en overheidsinstanties, de implementatie van de Europese ontsluitverplichting en de kosten van het VB. In verband daarmee is aanpassing wenselijk van het wetsvoorstel en de toelichting.

1. Inleiding

Het voorstel regelt de inrichting van een VB. Het VB is een technische koppeling die het voor aangesloten banken en betaaldienstverleners mogelijk maakt om geautomatiseerd identificerende gegevens te verstrekken op verzoek of na vordering van overheidsinstanties. De politie, de Bijzondere opsporingsdiensten, het Openbaar Ministerie, de Financiële inlichtingeneenheid (hierna: FIU) en de Belastingdienst hebben voor de uitoefening van hun wettelijke taken deze gegevens nodig van cliënten van banken en andere betaaldienstverleners. Deze overheidsinstanties hebben de wettelijke bevoegdheid om identificerende gegevens te vorderen of te verzoeken bij banken en betaaldienstverleners. Op dit moment vindt deze gegevensverstrekking handmatig plaats. Deze wijze van verstrekking sluit niet meer aan bij het huidige betalingsverkeer, dat snel, digitaal en grensoverschrijdend is, aldus de toelichting.²

¹ Het gaat daarbij dus niet om informatie over het gebruik van de rekening of het product zelf (bijvoorbeeld welke transacties hebben plaatsgevonden of de hoogte van het saldo).

² Memorie van Toelichting, paragraaf 2.1.



Het VB maakt het daarom voor overheidsdiensten mogelijk om bijna real-time identificerende gegevens te vorderen of op te vragen. Voor banken en andere betaaldienstverleners die rekeningen aanbieden wordt het mogelijk deze gegevens vervolgens geautomatiseerd te verstrekken. Het verwijzingsportaal is geen database, maar een koppeling; het zoekt, op aanvraag, gegevens op in administraties van aangesloten banken en betaaldienstverleners. Het slaat de gegevens die het heeft opgezocht slechts enkele minuten op ten behoeve van de verwerking door de aangesloten overheidsinstanties. Daarna worden de gegevens vernietigd.³

Met het wetsvoorstel wordt daarnaast de Europese verplichting geïmplementeerd om te voorzien in een centraal elektronisch systeem voor gegevensontsluiting dat tijdige identificatie mogelijk maakt van natuurlijke personen of rechtspersonen die houder zijn van of zeggenschap hebben over bank- en betaalrekeningen met een IBAN⁴-identificatienummer of over een kluis bij de bank (hierna kortgezegd: Europese ontsluitverplichting).⁵

2. Waarborgen tegen onnodige gegevensverstrekking

Het wetsvoorstel beoogt de reeds bestaande wettelijke bevoegdheden voor de genoemde overheidsinstanties om identificerende gegevens te vorderen of op te vragen niet te wijzigen, in te perken of te verruimen. Niettemin leidt het VB wel tot verlaging van de drempel voor gegevensverstrekking. Het voorstel is dan ook niet alleen technisch van aard. Het gebruik van digitale techniek is weliswaar begrijpelijk, maar vergt wel dat de gevolgen daarvan voor burgers en rechtspersonen uitdrukkelijk worden onderkend.⁶

Het VB maakt het mogelijk dat identificerende gegevens door banken automatisch worden verstrekt op verzoek van bepaalde overheidsinstanties. Interne procedures bij de overheidsinstanties moeten waarborgen dat een dergelijk verzoek bevoegd wordt gedaan en aan alle overige (wettelijke) voorwaarden wordt voldaan. Daarnaast worden alleen gegevens uit het VB aan de verzoekende instanties teruggezonden indien een zoekvraag in het VB tot maximaal drie personen leidt. Dit laatste geldt niet voor zoekvragen op basis van een product,⁷ deze kunnen wel tot meer personen leiden.⁸

Tot nu toe worden de identificerende gegevens handmatig verstrekt door de bank. De introductie van het VB zorgt ervoor dat deze gegevens na invoering van het verzoek in het VB automatisch en dus zonder mogelijkheid van controle op de juistheid van het verzoek of de vordering door de bank worden verstrekt. De gegevensverstrekking wordt daardoor sneller en efficiënter. De richtlijn beoogt dit ook voor zover het de gegevensverstrekking betreft tussen banken, andere betaaldienstverleners en de Financiële inlichtingeneenheden.

Keerzijde daarvan is echter dat de kans op onnodige gegevensverstrekking wordt verhoogd. Het had in de rede gelegen om met het oog daarop, binnen de eisen die de richtlijn aan de gegevensontsluiting stelt, te voorzien in extra waarborgen in het VB om het risico daarop zoveel mogelijk te verkleinen. In dat verband wijst de Afdeling erop dat bijvoorbeeld uitdrukkelijk niet is gekozen voor de mogelijkheid tot fiatting.⁹ Dat fiatting leidt tot vertraging, zoals opgemerkt in de gegevensbeschermingsbeoordeling,¹⁰ acht de Afdeling onvoldoende om daarvan af te zien, gelet op het belang van bescherming van de gegevens van betrokkenen. Bovendien blijkt uit de toelichting ook niet of en welke andere waarborgen in het VB zijn overwogen.

Dit klemt te meer gelet op de bestaande (ruime) vorderingsgrondslagen die in het voorstel zijn overgenomen voor de Belastingdienst.¹¹ De Belastingdienst, zijnde de inspecteur, heeft immers de mogelijkheid om identificerende gegevens op te vragen ten behoeve van het voorkomen van misbruik met toeslagen en ten behoeve van de belastingheffing en -inning. Uit de toelichting wordt echter niet duidelijk welke waarborgen worden gerealiseerd om het risico van onnodige gegevensverstrekking aan de Belastingdienst, zoveel mogelijk te verkleinen. De toelichting¹² verwijst enkel naar een beoogde

³ Memorie van Toelichting, paragraaf 2.3.

⁴ International Bank Account Number.

⁵ Artikel 32bis zoals gewijzigd met inwerkingtreding van de richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU (PbEU2018, L 156).

⁶ Zie ook in die zin het ongevraagd advies van de Afdeling inzake digitalisering, Kamerstukken II 2017/18, 26 643, nr. 557.

⁷ Financieel product in de zin van de Wet op het financieel toezicht.

⁸ Gegevensbeschermingseffectbeoordeling Rijksdienst, bijlage bij de Memorie van Toelichting, paragraaf 14.

⁹ Memorie van Toelichting, paragraaf 4.4.

¹⁰ Gegevensbeschermingseffectbeoordeling Rijksdienst, bijlage bij de Memorie van Toelichting, paragraaf 3.

¹¹ Op grond van artikel 53 van de Algemene wet inzake rijksbelastingen, de artikelen 62 en 62bis van de Invorderingswet 1990 en artikel 38 van de Algemene wet inkomensafhankelijke regelingen.

¹² Memorie van Toelichting, artikelsgewijze toelichting, onderdeel D.



aanpassing van het zogenoemde Voorschrift informatie fiscus/banken,¹³ zonder in te gaan op de benodigde aanpassingen.

Daarnaast had het in de rede gelegen om expliciet toe te lichten hoe de rechten van betrokkenen ten aanzien van het VB kunnen worden uitgeoefend. De toelichting gaat slechts in algemene zin in op de afspraken tussen de verwerker (de Justitiële informatiedienst) en de verwerkingsverantwoordelijken (respectievelijk banken, betaaldienstverleners en de betreffende overheidsinstanties).¹⁴

De Afdeling adviseert in de toelichting op het voorgaande nader in te gaan, daarbij in het bijzonder aandacht te besteden aan de Belastingdienst en het wetsvoorstel aan te passen.

2. Naar aanleiding van de opmerkingen van de Afdeling op dit punt alsmede op het punt van de gegevensverstrekking aan de Belastingdienst, is paragraaf 4.4 van de memorie van toelichting aangevuld met een passage over een aantal extra waarborgen waarin zal worden voorzien in verband met de beoogde werkwijze van fiattering buiten het verwijzingsportaal bankgegevens. In paragraaf 4.9 van de memorie van toelichting is ingegaan op de wijze waarop de rechten van betrokkenen kunnen worden uitgeoefend.

3. Veiligheidsrisico's gegevenssystemen banken en overheidsinstanties

In de toelichting wordt niet zonder reden uitgebreid ingegaan op de beveiligingsmaatregelen die zijn getroffen ten aanzien van het VB. Zo is het systeem niet toegankelijk via het internet om ongeoorloofde toegang tot het systeem te voorkomen. Het VB heeft een eigen fysieke infrastructuur, die met een firewall is afgeschermd van het netwerk van het ministerie van Justitie en Veiligheid. Ook is er een autorisatie en inlogvoorziening voor medewerkers die bevoegd zijn gegevens op te vragen en worden de beheerders van het systeem door de AIVD gescreend. Daarnaast wordt een penetratietest uitgevoerd voordat het VB in gebruik wordt genomen. In reactie op het advies van het Bureau ICT-toetsing zijn bovendien aanvullende maatregelen getroffen.¹⁵ Hiermee is gekozen voor een oplossing die zo min mogelijk risico's met zich brengt, aldus de toelichting.¹⁶

Het VB leidt er echter ook toe dat via een koppeling van het VB aan de klantenadministratie van een bank of betaaldienstverlener, de klantadministratie wordt ontsloten. Daarnaast wordt een verbinding gelegd van het VB naar de overheidsinstanties. Deze ontsluiting brengt als zodanig risico's met zich voor de beveiliging van de klantadministraties van banken en betaaldienstverleners en de gegevensbestanden van de betreffende overheidsinstanties.

De Afdeling merkt op dat, in tegenstelling tot de uitvoerige toelichting op de vereiste beveiligingsmaatregelen ten aanzien van het VB, in de toelichting niet wordt ingegaan op de mogelijke consequenties van de koppeling met het VB voor de beveiliging van de klantenadministraties van de banken en betaaldienstverleners en de gegevensbestanden van de betrokken overheidsinstanties.

De Afdeling adviseert op het voorgaande in de toelichting nader in te gaan.

3. Bovenstaande opmerkingen van de Afdeling zijn aanleiding geweest om paragraaf 4.8 van de memorie van toelichting aan te vullen met een beschrijving van de beveiligingsmaatregelen die genomen zijn ten aanzien van de koppeling van het VB met de klantadministraties van aangesloten banken en andere betaaldienstverleners en met de gegevensbestanden van de betrokken overheidsinstanties.

4. Implementatie overige onderdelen van Europese ontsluitverplichting

De voorbereiding van een nationale wettelijke regeling voor de inrichting van het VB is ingehaald door Europeesrechtelijke ontwikkelingen, zo blijkt uit de toelichting. Op 19 juni 2018 is de richtlijn tot wijziging van de vierde anti-witwasrichtlijn¹⁷ in werking getreden, waarin voornoemde Europese ontsluitverplichting is opgenomen. Het wetsvoorstel beoogt daarom ook de hiervoor genoemde Europese ontsluitverplichting te implementeren.

De Afdeling heeft er begrip voor dat de voorbereidingen van een op nationaal beleid ingericht VB zijn voortgezet, op het moment dat de Europese ontsluitverplichting in werking trad. Dit leidt er echter toe dat het wetsvoorstel niet geheel aansluit bij hetgeen waartoe de richtlijn de EU-lidstaten verplicht. Zo

¹³ Besluit van de Staatssecretaris van Financiën van 13 december 2012 (Staatscourant 2012, 26782).

¹⁴ Memorie van Toelichting, paragraaf 4.5 en 4.9.

¹⁵ Kamerstukken II 2018/19, 26 643, nr. 592.

¹⁶ Memorie van Toelichting, paragraaf 4.8.

¹⁷ De vierde anti-witwasrichtlijn (EU) 2015/849 strekt tot het voorkomen van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering voor de aan deze misdrijven ten grondslag liggende delicten zoals corruptie of voor fiscale misdrijven, waaronder belastingontduiking en -fraude.



geeft het VB naast de FIU ook het Openbaar Ministerie, de Politie, de Bijzondere opsporingsdiensten en de Belastingdienst toegang tot het VB. Uit de transponeringstabel valt op te maken dat andere onderdelen van de Europese ontsluitverplichting echter nog zullen worden geïmplementeerd, zonder dat duidelijk wordt wanneer dit het geval zal zijn en of de in het voorstel opgenomen wettelijke vorderingsgrondslagen daarvoor toereikend zullen zijn.¹⁸

De Afdeling adviseert op het voorgaande in de toelichting nader in te gaan.

4. De Afdeling merkt terecht op dat het wetsvoorstel thans niet geheel aansluit bij de Europese ontsluitverplichting uit de richtlijn tot wijziging van de vierde anti-witwasrichtlijn. Dit heeft ertoe geleid dat het wetsvoorstel is aangevuld met een vorderingsgrondslag voor gegevens over de uiteindelijk belanghebbende en de openings- en sluitingsdatum van een rekening en kluis. Omdat er meer tijd nodig is voor de technische implementatie van deze vorderingsmogelijkheid is deze wijziging opgenomen in een afzonderlijk wijzigingsartikel (artikel II). Zowel het algemene deel als de artikelsgewijze toelichting zijn met betrekking tot deze uitbreiding van de vorderingsgrondslag aangevuld.

5. Kosten VB

Ten slotte wijst de Afdeling erop dat de banken de kosten voor de aansluiting op het VB zelf moeten dragen. Reden daarvoor is dat marktpartijen de kosten die direct voortkomen uit Europese voorschriften zelf dragen, aldus de toelichting.¹⁹ Het wetsvoorstel heeft echter een bredere strekking dan implementatie van de Europese ontsluitverplichting. Niet nader wordt toegelicht waarom de kosten niettemin volledig door de banken gedragen zouden moeten worden.

De Afdeling adviseert op het voorgaande in de toelichting nader in te gaan.

5. Naar aanleiding van deze opmerking van de Afdeling is in paragraaf 7.2 van de memorie van toelichting, naar aanleiding van een consultatiereactie van de NVB, nader ingegaan op de vraag waarom de kosten niettemin volledig door de banken gedragen moeten worden. Uiteengezet is dat het wetsvoorstel met de bredere strekking beoogt te voorkomen dat banken en aangesloten overheidsdiensten voor vorderingen/bevragingen die onder de scope van de Europese richtlijn vallen gebruik kunnen maken van het verwijzingsportaal en voor andere bevragingen niet. Dit zou voor alle partijen extra kosten met zich meebrengen, omdat anders een deel van het proces nog op handmatige wijze zou moeten worden voortgezet. Daarnaast vindt momenteel ook geen vergoeding van investerings-, exploitatie- en onderhoudskosten plaats bij zowel bepaalde strafrechtelijke vorderingen als informatieverzoeken van de Belastingdienst en FIU-Nederland.

De Afdeling advisering van de Raad van State heeft een aantal opmerkingen bij het voorstel en adviseert daarmee rekening te houden voordat het voorstel bij de Tweede Kamer der Staten-Generaal wordt ingediend.

*De waarnemend vice-president van de Raad van State,
S.F.M. Wortmann*

Ik moge U, mede namens mijn ambtgenoot van Justitie en Veiligheid, verzoeken het hierbij gevoegde gewijzigde voorstel van wet en de gewijzigde memorie van toelichting aan de Tweede Kamer der Staten-Generaal te zenden.

*De Minister van Financiën,
W.B. Hoekstra.*

¹⁸ Transponeringstabel artikel 32bis, derde lid.

¹⁹ Memorie van Toelichting, paragraaf 7.2.



Advies Raad van State

No. W06.19.0106/III

's-Gravenhage, 29 mei 2019

Aan de Koning

Bij Kabinetsmissive van 24 april 2019, no.2019000843, heeft Uwe Majesteit, op voordracht van de Minister van Financiën, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het voorstel van tot wijziging van de Wet op het financieel toezicht in verband met het via een centraal elektronisch systeem geautomatiseerd verstrekken en ontsluiten van identificerende gegevens door banken en betaaldienstverleners (Wet verwijzingsportaal bankgegevens), met memorie van toelichting.

Het voorstel regelt de inrichting van een Verwijzingsportaal bankgegevens (hierna: VB). Het doel hiervan is het proces van het verstrekken van bepaalde identificerende gegevens¹ door banken en andere betaaldienstverleners aan bepaalde overheidsinstanties efficiënter te laten verlopen.

De Afdeling advisering van de Raad van State vestigt de aandacht op de waarborgen voor gegevensverwerking bij de introductie van deze digitale techniek, de beveiligingsrisico's voor banken, betaaldienstverleners en overheidsinstanties, de implementatie van de Europese ontsluitverplichting en de kosten van het VB. In verband daarmee is aanpassing wenselijk van het wetsvoorstel en de toelichting.

1. Inleiding

Het voorstel regelt de inrichting van een VB. Het VB is een technische koppeling die het voor aangesloten banken en betaaldienstverleners mogelijk maakt om geautomatiseerd identificerende gegevens te verstrekken op verzoek of na vordering van overheidsinstanties. De politie, de Bijzondere opsporingsdiensten, het Openbaar Ministerie, de Financiële inlichtingeneenheid (hierna: FIU) en de Belastingdienst hebben voor de uitoefening van hun wettelijke taken deze gegevens nodig van cliënten van banken en andere betaaldienstverleners. Deze overheidsinstanties hebben de wettelijke bevoegdheid om identificerende gegevens te vorderen of te verzoeken bij banken en betaaldienstverleners. Op dit moment vindt deze gegevensverstrekking handmatig plaats. Deze wijze van verstrekking sluit niet meer aan bij het huidige betalingsverkeer, dat snel, digitaal en grensoverschrijdend is, aldus de toelichting.²

Het VB maakt het daarom voor overheidsdiensten mogelijk om bijna real-time identificerende gegevens te vorderen of op te vragen. Voor banken en andere betaaldienstverleners die rekeningen aanbieden wordt het mogelijk deze gegevens vervolgens geautomatiseerd te verstrekken. Het verwijzingsportaal is geen database, maar een koppeling; het zoekt, op aanvraag, gegevens op in administraties van aangesloten banken en betaaldienstverleners. Het slaat de gegevens die het heeft opgezocht slechts enkele minuten op ten behoeve van de verwerking door de aangesloten overheidsinstanties. Daarna worden de gegevens vernietigd.³

Met het wetsvoorstel wordt daarnaast de Europese verplichting geïmplementeerd om te voorzien in een centraal elektronisch systeem voor gegevensontsluiting dat tijdige identificatie mogelijk maakt van natuurlijke personen of rechtspersonen die houder zijn van of zeggenschap hebben over bank- en betaalrekeningen met een IBAN⁴-identificatienummer of over een kluis bij de bank (hierna kortgezegd: Europese ontsluitverplichting).⁵

2. Waarborgen tegen onnodige gegevensverstrekking

Het wetsvoorstel beoogt de reeds bestaande wettelijke bevoegdheden voor de genoemde overheidsinstanties om identificerende gegevens te vorderen of op te vragen niet te wijzigen, in te perken of te verruimen. Niettemin leidt het VB wel tot verlaging van de drempel voor gegevensverstrekking. Het voorstel is dan ook niet alleen technisch van aard. Het gebruik van digitale techniek is weliswaar

¹ Het gaat daarbij dus niet om informatie over het gebruik van de rekening of het product zelf (bijvoorbeeld welke transacties hebben plaatsgevonden of de hoogte van het saldo).

² Memorie van Toelichting, paragraaf 2.1.

³ Memorie van Toelichting, paragraaf 2.3.

⁴ International Bank Account Number.

⁵ Artikel 32bis zoals gewijzigd met inwerkingtreding van de richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU (PbEU2018, L 156).



begrijpelijk, maar vergt wel dat de gevolgen daarvan voor burgers en rechtspersonen uitdrukkelijk worden onderkend.⁶

Het VB maakt het mogelijk dat identificerende gegevens door banken automatisch worden verstrekt op verzoek van bepaalde overheidsinstanties. Interne procedures bij de overheidsinstanties moeten waarborgen dat een dergelijk verzoek bevoegd wordt gedaan en aan alle overige (wettelijke) voorwaarden wordt voldaan. Daarnaast worden alleen gegevens uit het VB aan de verzoekende instanties teruggezonden indien een zoekvraag in het VB tot maximaal drie personen leidt. Dit laatste geldt niet voor zoekvragen op basis van een product,⁷ deze kunnen wel tot meer personen leiden.⁸

Tot nu toe worden de identificerende gegevens handmatig verstrekt door de bank. De introductie van het VB zorgt ervoor dat deze gegevens na invoering van het verzoek in het VB automatisch en dus zonder mogelijkheid van controle op de juistheid van het verzoek of de vordering door de bank worden verstrekt. De gegevensverstrekking wordt daardoor sneller en efficiënter. De richtlijn beoogt dit ook voor zover het de gegevensverstrekking betreft tussen banken, andere betaaldienstverleners en de Financiële inlichtingeneenheden.

Keerzijde daarvan is echter dat de kans op onnodige gegevensverstrekking wordt verhoogd. Het had in de rede gelegen om met het oog daarop, binnen de eisen die de richtlijn aan de gegevensontsluiting stelt, te voorzien in extra waarborgen in het VB om het risico daarop zoveel mogelijk te verkleinen. In dat verband wijst de Afdeling erop dat bijvoorbeeld uitdrukkelijk niet is gekozen voor de mogelijkheid tot fiatting.⁹ Dat fiatting leidt tot vertraging, zoals opgemerkt in de gegevensbeschermingsbeoordeling,¹⁰ acht de Afdeling onvoldoende om daarvan af te zien, gelet op het belang van bescherming van de gegevens van betrokkenen. Bovendien blijkt uit de toelichting ook niet of en welke andere waarborgen in het VB zijn overwogen.

Dit klemmt te meer gelet op de bestaande (ruime) vorderingsgrondslagen die in het voorstel zijn overgenomen voor de Belastingdienst.¹¹ De Belastingdienst, zijnde de inspecteur, heeft immers de mogelijkheid om identificerende gegevens op te vragen ten behoeve van het voorkomen van misbruik met toeslagen en ten behoeve van de belastingheffing en -inning. Uit de toelichting wordt echter niet duidelijk welke waarborgen worden gerealiseerd om het risico van onnodige gegevensverstrekking aan de Belastingdienst, zoveel mogelijk te verkleinen. De toelichting¹² verwijst enkel naar een beoogde aanpassing van het zogenoemde Voorschrift informatie fiscus/banken,¹³ zonder in te gaan op de benodigde aanpassingen.

Daarnaast had het in de rede gelegen om expliciet toe te lichten hoe de rechten van betrokkenen ten aanzien van het VB kunnen worden uitgeoefend. De toelichting gaat slechts in algemene zin in op de afspraken tussen de verwerker (de Justitiële informatiedienst) en de verwerkingsverantwoordelijken (respectievelijk banken, betaaldienstverleners en de betreffende overheidsinstanties).¹⁴

De Afdeling adviseert in de toelichting op het voorgaande nader in te gaan, daarbij in het bijzonder aandacht te besteden aan de Belastingdienst en het wetsvoorstel aan te passen.

3. Veiligheidsrisico's gegevenssystemen banken en overheidsinstanties

In de toelichting wordt niet zonder reden uitgebreid ingegaan op de beveiligingsmaatregelen die zijn getroffen ten aanzien van het VB. Zo is het systeem niet toegankelijk via het internet om ongeoorloofde toegang tot het systeem te voorkomen. Het VB heeft een eigen fysieke infrastructuur, die met een firewall is afgeschermd van het netwerk van het ministerie van Justitie en Veiligheid. Ook is er een autorisatie en inlogvoorziening voor medewerkers die bevoegd zijn gegevens op te vragen en worden de beheerders van het systeem door de AIVD gescreend. Daarnaast wordt een penetratietest uitgevoerd voordat het VB in gebruik wordt genomen. In reactie op het advies van het Bureau ICT-toetsing zijn bovendien aanvullende maatregelen getroffen.¹⁵ Hiermee is gekozen voor een oplossing die zo min mogelijk risico's met zich brengt, aldus de toelichting.¹⁶

⁶ Zie ook in die zin het ongevraagd advies van de Afdeling inzake digitalisering, Kamerstukken II 2017/18, 26 643, nr. 557.

⁷ Financieel product in de zin van de Wet op het financieel toezicht.

⁸ Gegevensbeschermingseffectbeoordeling Rijksdienst, bijlage bij de Memorie van Toelichting, paragraaf 14.

⁹ Memorie van Toelichting, paragraaf 4.4.

¹⁰ Gegevensbeschermingseffectbeoordeling Rijksdienst, bijlage bij de Memorie van Toelichting, paragraaf 3.

¹¹ Op grond van artikel 53 van de Algemene wet inzake rijksbelastingen, de artikelen 62 en 62bis van de Invorderingswet 1990 en artikel 38 van de Algemene wet inkomensafhankelijke regelingen.

¹² Memorie van Toelichting, artikelsgewijze toelichting, onderdeel D.

¹³ Besluit van de Staatssecretaris van Financiën van 13 december 2012 (Staatscourant 2012, 26782).

¹⁴ Memorie van Toelichting, paragraaf 4.5 en 4.9.

¹⁵ Kamerstukken II 2018/19, 26 643, nr. 592.

¹⁶ Memorie van Toelichting, paragraaf 4.8.



Het VB leidt er echter ook toe dat via een koppeling van het VB aan de klantenadministratie van een bank of betaaldienstverlener, de klantadministratie wordt ontsloten. Daarnaast wordt een verbinding gelegd van het VB naar de overheidsinstanties. Deze ontsluiting brengt als zodanig risico's met zich voor de beveiliging van de klantadministraties van banken en betaaldienstverleners en de gegevensbestanden van de betreffende overheidsinstanties.

De Afdeling merkt op dat, in tegenstelling tot de uitvoerige toelichting op de vereiste beveiligingsmaatregelen ten aanzien van het VB, in de toelichting niet wordt ingegaan op de mogelijke consequenties van de koppeling met het VB voor de beveiliging van de klantenadministraties van de banken en betaaldienstverleners en de gegevensbestanden van de betrokken overheidsinstanties.

De Afdeling adviseert op het voorgaande in de toelichting nader in te gaan.

4. Implementatie overige onderdelen van Europese ontsluitverplichting

De voorbereiding van een nationale wettelijke regeling voor de inrichting van het VB is ingehaald door Europeesrechtelijke ontwikkelingen, zo blijkt uit de toelichting. Op 19 juni 2018 is de richtlijn tot wijziging van de vierde anti-witwasrichtlijn¹⁷ in werking getreden, waarin voornoemde Europese ontsluitverplichting is opgenomen. Het wetsvoorstel beoogt daarom ook de hiervoor genoemde Europese ontsluitverplichting te implementeren.

De Afdeling heeft er begrip voor dat de voorbereidingen van een op nationaal beleid ingericht VB zijn voortgezet, op het moment dat de Europese ontsluitverplichting in werking trad. Dit leidt er echter toe dat het wetsvoorstel niet geheel aansluit bij hetgeen waartoe de richtlijn de EU-lidstaten verplicht. Zo geeft het VB naast de FIU ook het Openbaar Ministerie, de Politie, de Bijzondere opsporingsdiensten en de Belastingdienst toegang tot het VB. Uit de transponeringstabel valt op te maken dat andere onderdelen van de Europese ontsluitverplichting echter nog zullen worden geïmplementeerd, zonder dat duidelijk wordt wanneer dit het geval zal zijn en of de in het voorstel opgenomen wettelijke vorderingsgrondslagen daarvoor toereikend zullen zijn.¹⁸

De Afdeling adviseert op het voorgaande in de toelichting nader in te gaan.

5. Kosten VB

Ten slotte wijst de Afdeling erop dat de banken de kosten voor de aansluiting op het VB zelf moeten dragen. Reden daarvoor is dat marktpartijen de kosten die direct voortkomen uit Europese voorschriften zelf dragen, aldus de toelichting.¹⁹ Het wetsvoorstel heeft echter een bredere strekking dan implementatie van de Europese ontsluitverplichting. Niet nader wordt toegelicht waarom de kosten niettemin volledig door de banken gedragen zouden moeten worden.

De Afdeling adviseert op het voorgaande in de toelichting nader in te gaan.

De Afdeling advisering van de Raad van State heeft een aantal opmerkingen bij het voorstel en adviseert daarmee rekening te houden voordat het voorstel bij de Tweede Kamer der Staten-Generaal wordt ingediend.

*De waarnemend vice-president van de Raad van State,
S.F.M. Wortmann.*

¹⁷ De vierde anti-witwasrichtlijn (EU) 2015/849 strekt tot het voorkomen van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering voor de aan deze misdrijven ten grondslag liggende delicten zoals corruptie of voor fiscale misdrijven, waaronder belastingontduiking en -fraude.

¹⁸ Transponeringstabel artikel 32bis, derde lid.

¹⁹ Memorie van Toelichting, paragraaf 7.2.



Tekst zoals toegezonden aan de Raad van State: Wijziging van de Wet op het financieel toezicht in verband met het via een centraal elektronisch systeem geautomatiseerd ontsluiten van identificerende gegevens door banken en andere betaaldienstverleners (Wet verwijzingsportaal bankgegevens)

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben, dat het wenselijk is om regels te stellen over het via een centraal systeem geautomatiseerd verstrekken van identificerende gegevens door banken en andere betaaldienstverleners, zodat deze verstrekking efficiënter verloopt en dat het stellen van regels daarnaast noodzakelijk is ter implementatie van Richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU (PbEU 2018, L 156);

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

ARTIKEL I

De **Wet op het financieel toezicht** wordt als volgt gewijzigd:

A

In artikel 1:1 wordt in de alfabetische volgorde de volgende definitie ingevoegd:

SEPA-verordening: Verordening (EU) nr. 260/2012 van het Europees Parlement en de Raad van 14 maart 2012 tot vaststelling van technische en bedrijfsmatige vereisten voor overmakingen en automatische afschrijvingen in euro en tot wijziging van Verordening (EG) nr. 924/2009 (PbEU 2012, L94);

B

Na artikel 1:49 wordt een artikel ingevoegd, luidende:

Artikel 1:49a

De Nederlandsche Bank en Onze Minister van Justitie en Veiligheid werken samen met het oog op de vervulling van de aan de Nederlandsche Bank in deze wet opgedragen taak met betrekking tot de in artikel 3:267i opgenomen verplichtingen voor banken en andere betaaldienstverleners.

C

Na artikel 1:93g wordt een artikel ingevoegd, luidende:

Artikel 1:93h

1. De Nederlandsche Bank kan, in afwijking van artikel 1:89, eerste lid, vertrouwelijke gegevens of inlichtingen, met uitzondering van persoonsgegevens, verkregen bij de vervulling van de haar in deze wet opgedragen taak met betrekking tot de in artikel 3:267i opgenomen verplichtingen voor banken en andere betaaldienstverleners, verstrekken aan Onze Minister van Justitie en Veiligheid, voor zover de gegevens of inlichtingen naar het oordeel van de Nederlandsche Bank noodzakelijk zijn voor de vervulling van die taak en dienstig zijn voor de samenwerking op grond van artikel 1:49a.
2. Onze Minister van Justitie en Veiligheid is verplicht tot geheimhouding van de op grond van het eerste lid ontvangen vertrouwelijke gegevens of inlichtingen.
3. Artikel 1:93, tweede lid, is van overeenkomstige toepassing.

D

Na afdeling 3.5.9 wordt een afdeling ingevoegd, luidende:



Afdeling 3.5.10. Verwijzingsportaal bankgegevens

Artikel 3:267i

1. Banken en andere betaaldienstverleners die rekeningen aanbieden met een IBAN identificatienummer als bedoeld in de SEPA-verordening dat de landcode NL bevat, en banken die in Nederland kluizen aanbieden, zijn ter voldoening van vorderingen en verzoeken van aangewezen instanties en functionarissen, aangesloten op een door Onze Minister van Justitie en Veiligheid beheerd centraal elektronisch systeem voor het geautomatiseerd ontsluiten van identificerende gegevens betreffende hun cliënten.
2. In dit artikel en de daarop gebaseerde bepalingen wordt onder cliënten verstaan: personen die financiële producten of kluizen afnemen van de banken en betaaldienstverleners, bedoeld in het eerste lid, en personen die als gemachtigde namens hen zeggenschap kunnen uitoefenen over deze financiële producten of kluizen.
3. Banken en andere betaaldienstverleners verstrekken gegevens door middel van het centraal elektronisch systeem, bedoeld in het eerste lid, ter voldoening aan vorderingen of verzoeken om identificerende gegevens bij of krachtens:
 - a. de artikelen 126a, 126nc, 126uc, 126zk, 126ii of 577bb van het Wetboek van Strafvordering;
 - b. artikel 19 van de Wet op de economische delicten;
 - c. artikel 17 van de Wet ter voorkoming van witwassen en financieren van terrorisme;
 - d. artikel 53, eerste lid, aanhef en onderdeel a, van de Algemene wet inzake rijksbelastingen;
 - e. de artikelen 62 of 62bis van de Invorderingswet 1990;
 - f. artikel 38 van de Algemene wet inkomensafhankelijke regelingen.
4. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over het beheer van het centraal elektronisch systeem, de instanties en functionarissen die het systeem gebruiken, de identificerende gegevens die door middel van het systeem worden ontsloten en de technische eisen waaraan het systeem en de aansluiting daarop moeten voldoen. Ook kunnen bij of krachtens die maatregel van bestuur regels worden gesteld over de wijze waarop vorderingen of verzoeken als bedoeld in het eerste lid worden gedaan en de wijze waarop de gevorderde of verzochte identificerende gegevens worden aangeboden.
5. Voor het opvragen van gegevens uit de eigen administratie ten behoeve van de verstrekking van identificerende gegevens, bedoeld in het eerste lid, maken banken en andere betaaldienstverleners gebruik van het burgerservicenummer voor zover zij daarover beschikken.

E

In de bijlagen behorende bij de artikelen 1:79 en 1:80 wordt in de opsomming van de artikelen in het Deel Prudentieel toezicht financiële ondernemingen in de numerieke volgorde telkens ingevoegd: artikel 3:267i, eerste lid.

ARTIKEL II

Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip.

ARTIKEL III

Deze wet wordt aangehaald als: Wet verwijzingsportaal bankgegevens.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren die zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

De Minister van Financiën,

De Minister van Justitie en Veiligheid,



MEMORIE VAN TOELICHTING

Algemeen

1. Inleiding

Dit wetsvoorstel strekt ertoe het proces van het verstrekken van bepaalde identificerende gegevens door banken en andere betaaldienstverleners, alsmede het door bepaalde overheidsinstanties vorderen en opvragen van die identificerende gegevens bij die banken en andere betaaldienstverleners, te automatiseren en daarmee efficiënter te laten verlopen. Hiertoe wordt de Wet op het financieel toezicht (Wft) gewijzigd door de afdeling Verwijzingsportaal bankgegevens op te nemen, die partijen die rekeningen aanbieden met een Nederlands IBAN identificatienummer verplicht om aan te sluiten op een verwijzingsportaal bankgegevens. Dit verwijzingsportaal bankgegevens is een technische koppeling die het voor aangesloten banken en betaaldienstverleners mogelijk maakt om geautomatiseerd te voldoen aan bepaalde vorderingen of verzoeken van overheidsinstanties. Hiermee wordt ook de verplichting geïmplementeerd voor elke lidstaat van de Europese Unie (EU-lidstaat) om te voorzien in een centraal elektronisch systeem ter identificatie van cliënten van banken en andere betaaldienstverleners. Deze verplichting vloeit voort uit artikel 32bis van Richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU (PbEU 2018, L 156) (hierna: de richtlijn tot wijziging van de vierde anti-witwasrichtlijn).

2. Aanleiding en doel van het wetsvoorstel

2.1 Wenselijkheid van geautomatiseerde ontsluiting

Verschillende overheidsinstanties, in het bijzonder die zich bezighouden met het aanpakken en bestrijden van witwassen en terrorismefinanciering, alsmede de daaraan ten grondslag liggende delicten zoals corruptie en fiscale misdrijven waaronder belastingontduiking en -fraude, hebben daarvoor identificerende gegevens nodig van cliënten van banken en andere betaaldienstverleners. Datzelfde geldt voor de Belastingdienst voor haar taken op het gebied van belastingheffing en -inning. Het gaat dan bijvoorbeeld om de naam, het registratienummer bij de Kamer van Koophandel, het adres en bij natuurlijke personen de geboortedatum. De politie, de bijzondere opsporingsdiensten, het Openbaar Ministerie (OM), de Financiële inlichtingen eenheid (hierna: FIU-Nederland) en de Belastingdienst hebben voor het uitvoeren van bepaalde taken de bevoegdheid om die identificerende gegevens te vorderen of op te vragen op grond van het Wetboek van Strafvordering (Sv), de Wet op de economische delicten (Wed), de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft), de Algemene wet inzake rijksbelastingen (AWR), de Invorderingswet 1990 (IW 1990) en de Algemene wet inkomensafhankelijke regelingen (Awir). Banken en andere betaaldienstverleners dienen de gevorderde of gevraagde identificerende gegevens op grond van de genoemde wetgeving te verstrekken.

Momenteel gebeurt het vorderen of opvragen van identificerende gegevens bij banken door overheidsinstanties veelal handmatig en op individuele basis. Dit heeft verschillende nadelen. Een belangrijk nadeel is dat de levering en verwerking van de gegevens vertraging kan oplopen, waardoor de gevraagde gegevens reeds kunnen zijn gewijzigd voordat de betreffende instantie ze ontvangt. Dit beperkt de genoemde instanties steeds meer bij de uitvoering van hun taken. Het betalingsverkeer verloopt namelijk steeds sneller, het is in toenemende mate digitaal en niet gebonden aan grenzen. Ook zijn er meer soorten diensten beschikbaar en is het eenvoudiger om producten van verschillende banken en andere betaaldienstverleners af te nemen en om gegevens snel (online) te wijzigen. Al deze ontwikkelingen, die in de toekomst nog zullen doorzetten, maken het moeilijker en in veel gevallen onmogelijk om geldstromen in kaart te brengen zonder actuele gegevens. Het is daarom voor een goede taakuitoefening essentieel dat identificerende gegevens snel en volledig bij de genoemde overheidsinstanties bekend zijn. Ook is het nodig dat de gegevens digitaal worden aangeleverd, zodat ze direct verwerkt kunnen worden. Er is geïnventariseerd op welke wijze het proces van vorderen en opvragen van identificerende gegevens bij banken en andere betaaldienstverleners, alsmede het daaropvolgend door hen verstrekken van die identificerende gegevens, beter kan worden vormgegeven. Dit heeft geleid tot het voorstel om voor bepaalde overheidsinstanties voor bepaalde identificerende gegevens te gaan werken met een centraal elektronisch systeem.

Het zogenoemde verwijzingsportaal bankgegevens voorziet in het betrouwbaar, veilig, snel, gericht en efficiënt vorderen, opvragen en verstrekken van identificerende gegevens op een (in beginsel) uniforme wijze. Met de verplichte aansluiting van in de wet aangewezen banken en andere betaaldienstverleners op het verwijzingsportaal bankgegevens wordt voorkomen dat overheidsinstanties

buiten het portaal om bij sommige partijen alsnog handmatig een vordering moeten indienen. Daarmee is het systeem zo effectief mogelijk.

2.2. Europese verplichting

Inmiddels heeft het wetsvoorstel niet meer alleen een nationale achtergrond. Op 19 juni 2018 is de hiervoor genoemde richtlijn tot wijziging van de vierde anti-witwasrichtlijn in werking getreden. Deze richtlijn wijzigt de vierde anti-witwasrichtlijn¹. De vierde anti-witwasrichtlijn en de wijziging van die richtlijn strekken tot het voorkomen van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering voor de aan deze misdrijven ten grondslag liggende delicten zoals corruptie of voor fiscale misdrijven, waaronder belastingontduiking en -fraude. De richtlijn tot wijziging van de vierde anti-witwasrichtlijn bevat daartoe verschillende maatregelen, waaronder in artikel 32bis de verplichting voor elke EU-lidstaat om te voorzien in een centraal elektronisch systeem voor gegevensontsluiting, dat de tijdige identificatie mogelijk maakt van natuurlijke personen of rechtspersonen die houder zijn van of zeggenschap hebben over bank- en betaalrekeningen met een IBAN-identificatienummer² of over een kluis bij een bank. Deze richtlijnverplichting valt in belangrijke mate samen met de nationale beleidsmatige wens om het verstrekken van identificerende gegevens door banken en andere betaaldienstverleners te automatiseren. Het beoogde verwijzingsportaal bankgegevens is immers een dergelijk geautomatiseerd centraal systeem en voldoet grotendeels aan de eisen van de richtlijn. Wel heeft het verwijzingsportaal bankgegevens een enerzijds breder toepassingsgebied dan de richtlijn voorschrijft en voldoet het anderzijds niet aan alle vereisten van de richtlijn. Het toepassingsbereik is breder doordat er meer overheidsinstanties zijn aangesloten en meer soorten identificerende gegevens kunnen worden opgevraagd dan de richtlijn voorschrijft. Dit is in de eerste plaats te verklaren doordat het opzetten van het verwijzingsportaal bankgegevens niet uitsluitend dient ter implementatie van de richtlijn, maar ook om te voldoen aan de nationale beleidsmatige wens om slagvaardiger op te kunnen treden bij het bestrijden van criminaliteit. Daarnaast is bij de keuze voor de gegevens die via het verwijzingsportaal bankgegevens verstrekt moeten worden aangesloten bij de reeds bestaande wettelijke bevoegdheden en de huidige praktijk van het handmatig vorderen van identificerende gegevens. Als in het onderhavige wetsvoorstel strikt zou zijn aangesloten bij de in de richtlijn genoemde gegevens, zou dat betekenen dat de aangesloten overheidsinstanties de overige gegevens, die zij op grond van de huidige Nederlandse wetgeving kunnen vorderen of opvragen, alsnog op de – inefficiënte – handmatige manier zouden moeten vorderen of opvragen. Dat zou het voordeel van het portaal teniet doen. Het verwijzingsportaal bankgegevens dat door het wetsvoorstel wordt geregeld voldoet niet aan alle vereisten van artikel 32bis van de richtlijn (zie ook de transponeringstabel in paragraaf 8). De overige vereisten zullen op een later moment worden geïmplementeerd.

De richtlijn tot wijziging van de vierde anti-witwasrichtlijn verplicht EU-lidstaten om uiterlijk op 10 september 2020 artikel 32bis, inhoudende de verplichting tot het opzetten van een centraal elektronisch geautomatiseerd systeem voor het ontsluiten van identificerende gegevens door banken en andere betaaldienstverleners, geïmplementeerd te hebben. De overige bepalingen van de richtlijn worden separaat geïmplementeerd, te weten in de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft), afgezien van de onderdelen van artikel 32bis die met dit wetsvoorstel nog niet geïmplementeerd zijn. Deze onderdelen worden geïmplementeerd in de algemene maatregel van bestuur behorend bij onderhavig wetsvoorstel.

2.3 Het verwijzingsportaal bankgegevens

Het verwijzingsportaal bankgegevens is een technische voorziening die het mogelijk maakt om identificerende bankgegevens van natuurlijke personen en rechtspersonen alsmede identificerende gegevens behorend bij financiële producten, bijna real-time te vorderen of op te vragen, op basis van de huidige bevoegdheden van opsporingsambtenaren, de FIU-Nederland en van de Belastingdienst. Het verwijzingsportaal bankgegevens maakt het voor banken en andere betaaldienstverleners die rekeningen aanbieden tevens mogelijk om deze gevraagde of gevorderde gegevens vervolgens geautomatiseerd te verstrekken. Het verwijzingsportaal bankgegevens is daarmee te kwalificeren als een koppeling: het zoekt, op aanvraag, gegevens op in administraties van aangesloten banken en betaaldienstverleners en is geen database. Het slaat de gegevens die het heeft opgezocht slechts kort op (enkele minuten) ten behoeve van de verwerking door de aangesloten overheidsinstanties. Daarna worden de gegevens vernietigd. Aangesloten overheidsinstanties kunnen een vordering of verzoek

¹ 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, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie (PbEU 2015, L 141)

² International Bank Account Number.

gelijktijdig aan meerdere of aan alle banken en betaaldienstverleners richten. Het verwijzingsportaal bankgegevens stuurt de identificerende gegevens, zo nodig gebundeld, aan de vragende overheidsinstantie. Dit gehele proces is binnen enkele minuten afgerond. De technische inrichting van het verwijzingsportaal bankgegevens zorgt er verder voor dat de identificerende gegevens die worden ontsloten van goede kwaliteit zijn en dat er minder gegevens worden ontsloten van personen waarop de vordering of het verzoek geen betrekking heeft.

De manier waarop het verwijzingsportaal bankgegevens is ingericht brengt mee dat het wetsvoorstel de reeds bestaande wettelijke bevoegdheden voor de genoemde overheidsinstanties om identificerende gegevens te vorderen of op te vragen niet wijzigt, inperkt of verruimt. Het wetsvoorstel schrijft alleen voor bepaalde partijen en bepaalde gegevens voor dat het verwijzingsportaal bankgegevens wordt gebruikt als middel voor verstrekking, voor zover er een wettelijke plicht daartoe bestaat.

2.4 Identificerende gegevens

In het portaal kunnen identificerende gegevens van personen die in Nederland financiële producten, in de zin van de Wet op het financieel toezicht, afnemen van banken en andere betaaldienstverleners worden ontsloten. Ook kunnen gegevens van personen, die als gemachtigde namens een cliënt zeggenschap kunnen uitoefenen over financiële producten, bijvoorbeeld op basis van een volmacht, worden opgevraagd. Bij of krachtens algemene maatregel van bestuur behorend bij dit wetsvoorstel zal worden uitgewerkt welke soorten identificerende gegevens via het verwijzingsportaal bankgegevens beschikbaar en opvraagbaar zullen zijn. Welke gegevens een aangesloten overheidsinstantie in een concreet geval kan opvragen of vorderen hangt af van de grondslag die daarvoor wordt gebruikt. De volgende identificerende gegevens zullen via het portaal beschikbaar zijn:

- in geval van een natuurlijk persoon: naam, tenaamstelling van de rekening, de kluis of het financiële product, adres, woonplaats, postadres, geboortedatum, en administratieve kenmerken (is het product actief of beëindigd, is de betreffende persoon zelf cliënt of kan hij als gemachtigde namens een ander zeggenschap uitoefenen);
- in geval van een rechtspersoon: naam, tenaamstelling van de rekening, de kluis of het financiële product, adres, vestigingsplaats, postadres, nummer van inschrijving bij de Kamer van Koophandel en administratieve kenmerken.

Zoals hierboven beschreven zijn deze identificerende gegevens gekozen om aan te sluiten bij de reeds bestaande bevoegdheden van de aangesloten overheidsinstanties en op basis van de bestaande praktijk tussen de overheidsinstanties en banken. Via het verwijzingsportaal bankgegevens wordt geen informatie verstrekt over het gebruik van de financiële producten. Er kan bijvoorbeeld via het portaal geen informatie worden opgevraagd over transacties die vanaf een bepaalde rekening zijn uitgevoerd of over het saldo op een bepaalde rekening. Voor zover de aangesloten overheidsinstanties andere gegevens dan de genoemde identificerende gegevens vorderen of opvragen bij aangesloten banken en betaaldienstverleners, of identificerende gegevens van andere partijen dan van aangesloten partijen vorderen of verzoeken, blijven de bestaande, handmatige, procedures van kracht en verloopt de verstrekking dus niet via het verwijzingsportaal bankgegevens. Het is niet mogelijk deze gegevens via het verwijzingsportaal bankgegevens op te vragen.

De wijze waarop banken en andere betaaldienstverleners de bovenstaande identificerende gegevens geautomatiseerd dienen te verstrekken, zal worden uitgewerkt bij of krachtens algemene maatregel van bestuur behorend bij dit wetsvoorstel. Wel voorziet het wetsvoorstel in een grondslag voor de aangesloten private partijen om bij het opvragen van gegevens uit de eigen administratie, ten behoeve van verstrekking via het verwijzingsportaal bankgegevens, het burgerservicenummer te gebruiken. Het gebruik van dit nummer is noodzakelijk om snel en efficiënt gegevens te verzamelen, het helpt om de hoeveelheid uitgewisselde informatie te beperken en het voorkomt dat onnodig identificerende gegevens worden verstrekt van personen waar de vordering of het verzoek geen betrekking op heeft.

2.5 Aansluiting op het verwijzingsportaal bankgegevens: private partijen

Dit wetsvoorstel verplicht banken en andere betaaldienstverleners die rekeningen aanbieden met een IBAN-identificatienummer dat de landcode 'NL' bevat, alsmede banken die kluizen aanbieden, aangesloten te zijn op het verwijzingsportaal bankgegevens. Deze afbakening vloeit voort uit de verplichting uit de richtlijn tot wijziging van de vierde anti-witwasrichtlijn om ervoor te zorgen dat in het verwijzingsportaal bankgegevens identificerende gegevens zijn op te vragen van natuurlijke personen en rechtspersonen die een rekening met een IBAN identificatienummer hebben en van personen die kluizen aanhouden bij banken in Nederland. Via het verwijzingsportaal bankgegevens dienen die banken en andere betaaldienstverleners identificerende gegevens betreffende hun cliënten bij een verzoek of vordering van de genoemde overheidsinstanties geautomatiseerd te verstrekken. Voor de aangesloten banken en betaaldienstverleners betekent dit concreet dat zij een automatische

koppeling tussen het eigen (klant)systeem en het verwijzingsportaal bankgegevens dienen te realiseren. Hoe de aansluiting op het verwijzingsportaal bankgegevens dient plaats te vinden en welke gegevens via het verwijzingsportaal worden gevorderd en verstrekt, zal worden uitgewerkt bij of krachtens algemene maatregel van bestuur.

2.6 Aansluiting op het verwijzingsportaal bankgegevens: bevoegde overheidsinstanties

Via het verwijzingsportaal bankgegevens kunnen identificerende gegevens worden opgevraagd op grond van artikelen uit het Wetboek van Strafvordering (Sv), de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft), de Wet op de economische delicten (Wed), de Algemene wet inzake rijksbelastingen (AWR), de Invorderingswet 1990 (IW 1990) en de Algemene wet inkomensafhankelijke regelingen (Awir). Deze wetgeving bepaalt ook welke overheidsinstanties bevoegd zijn om via het portaal identificerende gegevens op te vragen. Niet elke organisatie die op grond van deze artikelen bevoegd is om identificerende gegevens te vorderen of op te vragen, is aangesloten op het portaal. Aangesloten zijn de Nationale Politie, het Openbaar Ministerie, de Koninklijke Marechaussee, de Rijksrecherche, de Fiscale Inlichtingen- en Opsporingsdienst, de Inlichtingen- en Opsporingsdienst van de Nederlandse Voedsel- en Warenautoriteit, de directie Opsporing van de Inspectie Sociale Zaken en Werkgelegenheid, de Inlichtingen- en Opsporingsdienst van de Inspectie Leefomgeving en Transport, de Belastingdienst (BD-heffing), Douane (heffing), BD (inning), Douane (inning), BD (Toeslagen/heffing) en BD (Toeslagen/ inning) en de FIU-Nederland. Deze partijen zijn geselecteerd vanwege hun rol bij de aanpak en het bestrijden van witwassen en terrorismefinanciering en de daaraan ten grondslag liggende delicten zoals corruptie en fiscale misdrijven waaronder belastingontduiking en -fraude. Deze partijen mogen het verwijzingsportaal bankgegevens ook gebruiken voor andere verzoeken en vorderingen op basis van de genoemde wettelijke grondslagen. Bij of krachtens algemene maatregel van bestuur zullen functionarissen van deze organisaties of de organisaties zelf aangewezen worden als bevoegde autoriteiten.

2.7 Het beheer van het portaal

Het portaal wordt beheerd door de Justitiële Informatiedienst. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over dit beheer. Onderwerpen als de inrichting van het portaal en de manier waarop er wordt gerapporteerd over het gebruik en de werking van het verwijzingsportaal bankgegevens kunnen bij of krachtens deze algemene maatregel van bestuur worden uitgewerkt.

3. Wet op het financieel toezicht (Wft)

3.1 Motivering keuze

Hoewel de aansluitverplichting voor banken en andere betaaldienstverleners op het verwijzingsportaal bankgegevens op zich een nieuw element vormt in de Wft in de zin dat dit geen prudentieel of gedragsvereiste is zoals die nu zijn opgenomen in de Wft, is er toch voor gekozen om deze verplichting in de Wft op te nemen. Daarbij is in de eerste plaats van belang dat de Wft de primaire vindplaats is van eisen die aan banken en andere betaaldienstverleners worden gesteld. De aansluitverplichting ligt in het verlengde van de bedrijfsvoeringseisen die reeds in de Wft aan banken en andere betaaldienstverleners worden gesteld. Daarnaast heeft de aansluitverplichting ook raakvlakken met eisen inzake integere bedrijfsvoering, zoals gesteld in de artikelen 3.10 en 3.17 van de Wft. Zo is artikel 3.17, tweede lid, onderdeel b, Wft gericht op het tegengaan van gebruik van het financieel stelsel voor witwassen en terrorismefinanciering. Onderzocht is evenwel of het verwijzingsportaal bankgegevens in andere wetten zou kunnen worden geregeld, te weten in de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft), in het Wetboek van Strafvordering (Sv) of een van de andere wetten op grond waarvan gegevens via het verwijzingsportaal bankgegevens kunnen worden gevorderd of opgevraagd. Ten aanzien van de Wwft is geoordeeld dat de scope van die wet te beperkt is, waardoor de suggestie zou worden gewekt dat het verwijzingsportaal bankgegevens alleen van belang is voor de bestrijding van witwassen en terrorismefinanciering. De systematiek van en het soort normen in Sv vormen geen logisch kader om daarin bedrijfsvoeringsverplichtingen voor banken en andere betaaldienstverleners op te nemen. Dit geldt ook voor de andere wetten op grond waarvan gegevens bij deze instellingen kunnen worden gevorderd. Daar komt bij dat het verwijzingsportaal bankgegevens voor verschillende doeleinden zal worden gebruikt. Het opnemen van een verplichting tot aansluiting op het verwijzingsportaal bankgegevens in sectorale wetgeving ligt niet voor de hand, aangezien dan in de verschillende wetten een bepaling zou moeten worden opgenomen, hetgeen de kenbaarheid en toegankelijkheid van de regelgeving omtrent het verwijzingsportaal niet ten goede komt. Verder is van belang dat bestuursrechtelijke handhaving van de aansluitverplichting op het verwijzingsportaal (zie hieronder) in dit geval het meest voor de hand ligt.

3.2 Wettelijke grondslagen voor vorderen en opvragen gegevens

De bevoegdheden van de aangesloten overheidsinstanties om door middel van het verwijzingsportaal bankgegevens gegevens te vorderen of op te vragen zijn geregeld in het Wetboek van Strafvordering (Sv), de Wet op de economische delicten (WED), de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft), de Algemene wet inzake rijksbelastingen (AWR), de Invorderingswet 1990 (IW 1990) en de Algemene wet inkomensafhankelijke regelingen (Awir). Deze wetgeving en de daarop gebaseerde regels bepalen onder meer welke functionarissen gegevens kunnen opvragen, welke gegevens zij kunnen opvragen, met welk doel en welke procedures er bestaan voor het geven van goedkeuring voor een vordering of verzoek, voor zover nodig. Het wetsvoorstel brengt daar geen wijziging in. Voor een toelichting op de achtergrond van de bevoegdheden, het doel van de inzet daarvan, de gegevens die opgevraagd kunnen worden, de inrichting van de procedure van vorderen of verzoeken en andere genoemde aspecten wordt daarom verwezen naar de toelichting bij de betreffende wetgeving. Voor de inzichtelijkheid wordt in de artikelsgewijze toelichting wel kort op de verschillende bevoegdheden ingegaan.

3.3 Toezicht

In het wetsvoorstel is ervoor gekozen om de aansluitverplichting op het verwijzingsportaal bankgegevens neer te leggen in de Wft en voor het toezicht op de naleving daarvan alsmede voor de handhaving aan te sluiten bij de Wft. De Wft kent hoofdzakelijk een bestuursrechtelijk handavingskarakter. Bij de keuze hiervoor speelt in de eerste plaats een rol dat door het niet voldoen aan de aansluitverplichting de rechtsorde niet bijzonder geschokt zal zijn. Ook aan het criterium van de gesloten context wordt voldaan, aangezien sprake is van een bestaande relatie tussen DNB en de banken en andere betaaldienstverleners. Gelet hierop ligt het voor de hand DNB te vragen ook dit deel van het toezicht uit te oefenen. Daardoor wordt tevens een situatie voorkomen van bestuurlijke drukte als gevolg van veel verschillende toezichthouders. Bij de keuze voor DNB als toezichthouder is onderkend dat DNB deze taak alleen kan uitoefenen als zij beschikt over informatie van de Minister van Justitie en Veiligheid (Justid). Justid heeft een belangrijke rol in het toezicht, aangezien Justid als eerste signaleert of in voorkomende gevallen een instelling niet aan de aansluitverplichting voldoet. Deze informatie geeft Justid door aan DNB, waarna DNB onderzoek kan doen. Met het oog hierop is in Deel 1 van de Wft een bepaling opgenomen die DNB en de Minister van Justitie en Veiligheid, als verantwoordelijke voor Justid, verplicht om samen te werken ten behoeve van de goede uitoefening van het toezicht en de handhaving door DNB. Dit houdt onder meer in dat de Minister van Justitie en Veiligheid verplicht is om DNB tijdig te voorzien van de juiste informatie. Daarnaast kan het noodzakelijk zijn dat DNB met het oog op haar toezicht- en handhavingstaak inzake de aansluitverplichting in voorkomende gevallen ook toezichtvertrouwelijke informatie deelt met Justid. Ook daartoe zal een bepaling worden opgenomen in de Wft die dit mogelijk maakt.

Naar verwachting is met het opzetten van het toezicht en de handhaving van de aansluitverplichting door DNB gedurende het eerste jaar 1 fte extra gemoeid en is daarnaast een structurele capaciteitstoename van 1 fte nodig voor het uitvoeren van het toezicht en de handhaving. De extra toezichtskosten hiervan worden binnen het kostenkader van DNB opgevangen en via de systematiek van de Wet bekostiging financieel toezicht 2019 aan de sector doorberekend.

De Autoriteit Persoonsgegevens houdt op grond van bestaande wetgeving toezicht op de rechtmatigheid van de verwerking van persoonsgegevens die met het gebruik van het verwijzingsportaal bankgegevens is gemoeid.

4. Gegevensbescherming

Een gedeelte van de bedoelde identificerende gegevens zijn persoonsgegevens.³ Onder een persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.⁴ Op het gebruik (de verwerking) van persoonsgegevens is privacyregelgeving van toepassing. Omdat de voorgestelde bepaling voor een belangrijk deel betrekking heeft op de verwerking van persoonsgegevens, wordt hierna op de toepasselijke privacyregelgeving ingegaan en is de Autoriteit

³ Niet alle gegevens die via het portaal worden verstrekt zijn persoonsgegevens. Via het portaal kunnen ook identificerende gegevens over rechtspersonen worden opgevraagd.

⁴ Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon. Dit volgt uit de zogenoemde AVG (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 (algemene verordening gegevensbescherming)) (PbEU 2016, L 119)).

Persoonsgegevens op grond van artikel 36, vierde lid, algemene verordening gegevensbescherming gevraagd te adviseren of het wetsvoorstel voldoet aan de geldende wet- en regelgeving met betrekking tot de verwerking van persoonsgegevens. Op dit advies wordt in paragraaf 7.4 ingegaan.

4.1 Verwerking van persoonsgegevens in het portaal

Ten opzichte van de huidige praktijk, wijzigt het verwijzingsportaal bankgegevens op een paar punten de manier waarop persoonsgegevens worden verwerkt bij het voldoen aan vorderingen en verzoeken van aangesloten overheidsinstanties. Vanuit het oogpunt van bescherming van persoonsgegevens heeft dit zowel voordelen voor de betrokkenen als nadelen.

- Gegevens van cliënten van banken en betaaldienstverleners
Zoals in paragraaf 2.3 van deze toelichting is beschreven is het verwijzingsportaal bankgegevens te kenmerken als een koppeling en bevat het maar gedurende zeer beperkte tijd – enkele minuten – gegevens van cliënten van banken en andere betaaldienstverleners. Wel zullen identificerende gegevens van cliënten in plaats van direct van de vorderende of verzoekende overheidsinstantie naar de aangesloten private partijen en andersom, door tussenkomst van een technische voorziening, worden verstrekt. Dit betekent dat er een extra verwerking van persoonsgegevens aan het huidige proces wordt toegevoegd. Het systeem maakt het mogelijk om sneller en efficiënter gegevens op te vragen. Gezien de ervaringen in andere landen met een geautomatiseerd systeem moet er rekening mee worden gehouden dat het automatiseren leidt tot meer bevragingen. Ook dit levert extra verwerkingen op. Hier staat tegenover dat het verwijzingsportaal bankgegevens het gebruik van persoonsgegevens beperkt, doordat persoonsgegevens gericht kunnen worden opgevraagd en verstrekt. Hiertoe dient onder meer het gebruik van het burgerservicenummer, teneinde een vordering of verzoek van een overheidsinstantie te kunnen koppelen aan de betrokkene in het klantsysteem van de aangesloten bank of betaaldienstverlener. Hierdoor neemt het aantal verwerkingen af. Daarnaast neemt ook het aantal medewerkers van aangesloten private partijen, dat inzage heeft in de vorderingen, af. Ten opzichte van de huidige situatie levert het gebruik van het verwijzingsportaal bankgegevens daarnaast een vermindering van risico's per verwerking op, doordat de praktijk van vorderen of opvragen per e-mail vervalt met de daarbij behorende risico's voor de bescherming van persoonsgegevens en doordat minder medewerkers van de aangesloten banken en betaaldienstverleners bij de verwerkingen betrokken zijn.
- Gegevens ten behoeve van de beoordeling van de werking van het verwijzingsportaal bankgegevens
Het gebruik van het verwijzingsportaal bankgegevens brengt verder mee dat persoonsgegevens worden opgeslagen van de gebruikers van het portaal. Zo registreert het verwijzingsportaal bankgegevens van elk verzoek wie dit heeft gedaan. Dit gebeurt om te kunnen controleren dat het verwijzingsportaal rechtmatig wordt gebruikt, alsmede om de werking van het portaal te kunnen beoordelen.

4.2 Toepasselijke regelgeving bescherming persoonsgegevens

Op de verwerking van persoonsgegevens in het verwijzingsportaal zijn artikel 8 van het Handvest van de grondrechten van de Europese Unie, artikel 16 van het Verdrag betreffende de werking van de Europese Unie, artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en fundamentele vrijheden en artikel 10 van de Grondwet van toepassing. Op grond van deze bepalingen bestaat een recht op bescherming van persoonsgegevens dat alleen kan worden ingeperkt voor zover dat noodzakelijk is.

Deze regels worden verder uitgewerkt in de algemene verordening gegevensbescherming (AVG)⁵ en de Uitvoeringswet algemene verordening gegevensbescherming (UAVG). Op een deel van de gegevens die via het verwijzingsportaal bankgegevens worden verwerkt, is daarnaast de Wet politiegegevens van toepassing. Het gaat daarbij om de gegevens die de politie opneemt in de vordering die via het verwijzingsportaal bankgegevens banken en betaaldienstverleners wordt gericht. De Wet politiegegevens is herzien in verband met de implementatie van de richtlijn gegevensbescherming opsporing en vervolging⁶. Voor zover relevant, stelt deze wet vergelijkbare eisen aan de

⁵ De AVG heeft met ingang van 25 mei 2018 de EU-Privacyrichtlijn vervangen. Die richtlijn was in Nederland geïmplementeerd in de Wet bescherming persoonsgegevens (Wbp). De Uitvoeringswet Algemene verordening gegevensbescherming voorziet in de nationale regels die nodig zijn ter uitvoering van de AVG.

⁶ richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PbEU 2016, L119). Deze richtlijn is geïmplementeerd middels een wijziging van de Wet politiegegevens. Deze wijziging is grotendeels op 1 januari 2019 in werking getreden. Zie ook: Kamerstukken II 2017/18, 34 889, nrs. 1–7, Kamerstukken I 2017/18, 34 889, nr. A.

verwerking van deze gegevens als de AVG en de UAVG.

Persoonsgegevens moeten op grond van deze wetgeving worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Voorts mogen persoonsgegevens slechts worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen ze vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt (doelbinding). Ook moet degene die verantwoordelijk is voor een verwerking bij het ontwikkelen van werkwijzen en systemen rekening houden met de gevolgen daarvan voor de bescherming van persoonsgegevens en de risico's zoveel mogelijk beperken.

Op het gebruik van het burgerservicenummer door de aangesloten overheidsinstanties is verder de Wet algemene bepalingen burgerservicenummer van toepassing (Wabb).

4.3 Gegevensbeschermingseffectbeoordeling (PIA)

Voor het verwijzingsportaal bankgegevens is een zogenoemde gegevensbeschermingseffectbeoordeling (PIA) uitgevoerd. De PIA is er op gericht de noodzaak van de voorgenomen verwerking van persoonsgegevens te onderzoeken en de gevolgen en risico's van het systeem op gestructureerde wijze in kaart te brengen. Hierbij is in het bijzonder aandacht besteed aan de beginselen van transparantie, gegevensminimalisering, doelbinding, het vereiste van een goede beveiliging en de rechten van de betrokkenen. De risico's voor dit systeem zijn in drie categorieën in te delen: risico's die te maken hebben met legitimiteit, risico's die te maken hebben met privacy en risico's die te maken hebben met informatiebeveiliging. Onder risico's die te maken hebben met legitimiteit moet onder andere worden verstaan de kans dat via het verwijzingsportaal bankgegevens een vordering of verzoek wordt ingevoerd terwijl hieraan voorafgaand geen toetsing van de formele vereisten voor het indienen van een vordering of verzoek heeft plaatsgevonden. In de categorie privacy is een risico dat, indien een vordering of verzoek aan meerdere banken of betaaldienstverleners tegelijk wordt gericht, via het verwijzingsportaal ook persoonsgegevens van personen die niet in het klantenbestand van een aangesloten bank of betaaldienstverlener voorkomen, toch bij die partij terechtkomen. Risico's met betrekking tot informatiebeveiliging hebben te maken met de toegang tot het systeem, door derden of door onbevoegde medewerkers van de aangesloten partijen. Deze risicoanalyse heeft gevolgen voor de eisen die aan het systeem worden gesteld en voor de werkwijze bij gebruik van het systeem. Een verslag van de PIA is als bijlage bij deze memorie van toelichting gevoegd. Hieronder wordt een aantal bevindingen besproken.

4.4 Algemeen

De rechtsgrond voor de verwerking van persoonsgegevens in het kader van het gebruik van het verwijzingsportaal bankgegevens verschilt per betrokken partij. Hieronder een overzicht.

Organisatie	Rechtsgrond
Nationale Politie	art. 8,9 en 10 Wet politiegegevens
OM	art. 39b Wet justitiële en strafvorderlijke gegevens
Koninklijke Marechaussee	art. 8,9 en 10 Wet politiegegevens
Rijksrecherche	art. 8,9 en 10 Wet politiegegevens
Fiscale Inlichtingen- en Opsporingsdienst	art. 46 jo. art. 10 en 12 Wet politiegegevens art. 10 Besluit politiegegevens bijzondere opsporingsdiensten in combinatie met 8 en 9 Wet politiegegevens
Inlichtingen- en Opsporingsdienst van de Nederlandse Voedsel- en Warenautoriteit	art. 46 jo. art. 10 en 12 Wet politiegegevens art. 10 Besluit politiegegevens bijzondere opsporingsdiensten in combinatie met 8 en 9 Wet politiegegevens
directie Opsporing van de Inspectie Sociale Zaken en Werkgelegenheid	art. 46 jo. art. 10 en 12 Wet politiegegevens art. 10 Besluit politiegegevens bijzondere opsporingsdiensten in combinatie met 8 en 9 Wet politiegegevens
Inlichtingen- en Opsporingsdienst van de Inspectie Leefomgeving en Transport	art. 46 jo. art. 10 en 12 Wet politiegegevens art. 10 Besluit politiegegevens bijzondere opsporingsdiensten in combinatie met 8 en 9 Wet politiegegevens
Belastingdienst (BD-heffing, BD-inning, Toeslagen heffing, Toeslagen-inning, Douane-heffing en Douane-inning)	art. 6, eerste lid, onder e, jo. artikel 6, derde lid, AVG
FIU-Nederland	art. 6:6 van het Besluit politiegegevens
Banken en betaaldienstverleners	art. 6, eerste lid, onder c jo. Art. 6, derde lid, AVG

Het doel van de verzoeken die via het verwijzingsportaal bankgegevens worden ingediend, rechtvaardigt de inbreuk op de persoonlijke levenssfeer van de betrokkene. Gegevens worden immers opgevraagd ten behoeve van het voorkomen en opsporen van fraude en andere vormen van criminaliteit, het opsporen van (criminele) vermogens, het opleggen van financiële maatregelen en

sancties door de daarvoor bevoegde opsporingsdiensten, het voorkomen van misbruik met toeslagen door de Belastingdienst en de belastingheffing en -inning. De actualiteit, kwaliteit en de volledigheid van de gegevens die worden verstrekt, zal met de komst van het verwijzingsportaal bankgegevens toenemen. Het elektronisch opvragen gaat namelijk sneller, het systeem bevat verschillende waarborgen om te zorgen dat degene die de gegevens opvraagt bij het opvragen de juiste gegevens gebruikt en het opvragen kan makkelijker bij verschillende banken of betaaldienstverleners tegelijk gebeuren, zodat een volledig beeld wordt verkregen. Hierdoor kunnen de aangesloten overheidsinstanties beter en sneller hun werkzaamheden uitvoeren. Dat betekent dat het verwijzingsportaal noodzakelijk is in het belang van de openbare veiligheid en het economisch welzijn, zodat een beperking van de rechten van betrokkenen op grond van wetgeving op het gebied van privacy is toegestaan.⁷ In het portaal kunnen alleen vorderingen of verzoeken worden ingediend als daar op basis van de reeds bestaande wetgeving een bevoegdheid voor bestaat. De bevoegdheden worden met de komst van het systeem niet uitgebreid. Door de efficiëntere werking van het verwijzingsportaal ten opzichte van de huidige handmatige werkwijze zal het aantal vorderingen of verzoeken naar verwachting wel toenemen, maar altijd plaatsvinden binnen de wettelijke kaders.

De voorgestelde bepaling is verder voldoende duidelijk en nauwkeurig, zodat de toepassing ervan voldoende voorspelbaar is. Hierdoor is het voor betrokkenen transparant dat en in hoeverre de hen betreffende persoonsgegevens (kunnen) worden vastgelegd, geraadpleegd of anderszins (verder) verwerkt. In de voorgestelde bepaling zijn de doeleinden waarvoor de persoonsgegevens kunnen worden verwerkt expliciet opgenomen in de vorm van een omschrijving van de grondslagen waarop vorderingen of verzoeken, die via het portaal worden gedaan, gegrond moeten zijn. Voor wat betreft het gebruik van het burgerservicenummer is opgenomen dat banken en betaaldienstverleners dit op grond van het wetsvoorstel alleen mogen gebruiken om gegevens in de administratie op te zoeken in het kader van het gebruik van het verwijzingsportaal bankgegevens.

Bij het gebruik van het verwijzingsportaal bankgegevens blijven de bestaande waarborgen in stand om te verzekeren dat vorderingen van overheidsinstanties rechtmatig zijn. De hiervoor geldende procedures vinden plaats voordat het systeem wordt gebruikt voor het vorderen of opvragen van gegevens. Zo is de vordering door opsporingsambtenaren altijd schriftelijk. Daaraan voorafgaand bespreekt de opsporingsambtenaar dit met een (hulp)officier van justitie. In geval van een bijzondere opsporingsdienst wordt dit besproken met een teamleider. De (hulp)officier/teamleider toetst het voornemen op basis van proportionaliteit en subsidiariteit (is er sprake van een misdrijf, is er een noodzaak voor het opsporingsonderzoek, wat is de omvang en reikwijdte van bevraging én zijn er andere opsporingsmogelijkheden om aan de benodigde informatie te komen). Als de (hulp)officier/teamleider akkoord is met de inzet van de opsporingsbevoegdheid wordt de vordering opgemaakt (door een opsporingsambtenaar of de (hulp)officier/teamleider zelf). De opgemaakte vordering wordt door de (hulp)officier/teamleider ondertekend. Met deze vordering kan een opsporingsambtenaar de beschikking krijgen over identificerende gegevens. In het verwijzingsportaal bankgegevens wordt geen mogelijkheid tot fiatting opgenomen; de vordering is immers de exponent van de voorafgaande toetsing en de accordering door de hulpofficier/teamleider. In het verwijzingsportaal bankgegevens wordt wel de naam van de hulpofficier/teamleider en de naam van degene die vordering in het verwijzingsportaal bankgegevens heeft ingevoerd, opgenomen/gelogd. De opsporingsambtenaar moet bovendien verplicht invullen wat de wettelijke grondslag is van de vordering. Over deze werkwijze wordt een vorderingsprotocol ondertekend door de aangesloten opsporingsdiensten en de Minister van Justitie en Veiligheid. Ook voor andere vorderingen of verzoeken via het portaal geldt dat het proces van vorderen, tot aan het moment van het versturen van de vordering – nu op papier of via e-mail, of soms elektronisch straks in het portaal –, ongewijzigd blijft. Voor de Belastingdienst zal dit worden vastgelegd in het Voorschrift informatie fiscus-banken.

De minister van Justitie en Veiligheid zal in het kader van het beheer van het systeem laten beoordelen of het verwijzingsportaal bankgegevens op de juiste manier wordt gebruikt. Daarbij zal ook aan de orde komen of de aangesloten overheidsinstanties het portaal bevoegd gebruiken en of zij de juiste procedures in acht nemen.

4.5 Verwerkingsverantwoordelijkheid en relatie met verwerker

Verzenden verzoek of vordering om informatie:

Het verwijzingsportaal bankgegevens is een centrale voorziening waarlangs vragen van de respectievelijke bevragende organisaties bij de banken worden uitgezet conform de reeds bestaande en ongewijzigde wettelijke bevoegdheden. De bevragende organisaties zijn elk afzonderlijk verwerkingsverantwoordelijke voor het verzenden van hun verzoek of vordering om informatie aan het verwijzings-

⁷ Zie onder meer artikel 8, tweede lid, EVRM en artikel 6, eerste lid, onderdeel e, en derde lid, AVG.



zingsportaal bankgegevens. De gegevens die in het verwijzingsportaal bankgegevens worden opgeslagen (voor ongeveer drie minuten) vallen onder de verwerkingsverantwoordelijkheid van de bevragende organisatie. Hieronder een overzicht:

Bevragende organisatie	Verwerkingsverantwoordelijke
Nationale Politie	de korpschef (artikel 22 Richtlijn (EU) 2016/680 en artikel 1, aanhef en onderdeel f, onder 1, en artikel 6c Wet politiegegevens)
OM	niet van toepassing, want doet zelf geen bevestigingen
Koninklijke Marechaussee	de minister van Defensie (artikel 22 Richtlijn (EU) 2016/680 en artikel 1, aanhef en onderdeel f, onder 3, Wet politiegegevens)
Rijksrecherche	het College van procureurs-generaal (artikel 22 Richtlijn (EU) 2016/680 en artikel 1, aanhef en onderdeel f, onder 2, en artikel 6c Wet politiegegevens)
Fiscale Inlichtingen- en Opsporingsdienst	Directeur FIOD (artikel 22 Richtlijn (EU) 2016/680)
Inlichtingen- en Opsporingsdienst van de Nederlandse Voedsel- en Warenautoriteit	Directeur NVWA-IOD (artikel 22 Richtlijn (EU) 2016/680)
Directie Opsporing van de Inspectie Sociale Zaken en Werkgelegenheid	Directeur Opsporing (artikel 22 Richtlijn (EU) 2016/680)
Inlichtingen- en Opsporingsdienst van de Inspectie Leefomgeving en Transport	De minister van Infrastructuur en Waterstaat (artikel 22 Richtlijn (EU) 2016/680)
Belastingdienst	DG Belastingdienst namens de minister van Financiën
FIU-Nederland	Voor verwerking gegevens betreffende ongebruikelijke transacties: het hoofd FIU namens de minister van Justitie & Veiligheid (artikel 12, derde lid, Wwft) Voor verwerking gegevens betreffende verdachte transacties: de korpschef (artikel 22 Richtlijn (EU) 2016/680 en artikel 1, aanhef en onderdeel f, onder 1, en artikel 6c Wet politiegegevens)

De Justitiële Informatiedienst (Justid), vallend onder de verantwoordelijkheid van de minister van Justitie en Veiligheid, is verwerker voor deze partijen (zie hieronder).

Ontvangst verzoek of vordering en verstrekking door banken en andere betaaldienstverleners:

Banken kijken vervolgens in hun eigen klantsystemen of de gevraagde persoonsgegevens bij hen bekend zijn. Als dat het geval is worden de resultaten via het verwijzingsportaal bankgegevens naar de bevragende organisaties gestuurd. De verstrekking partijen (banken en andere betaaldienstverleners) zijn steeds verwerkingsverantwoordelijke als het gaat om de ontvangst van het verzoek of de vordering van het verwijzingsportaal en het naar aanleiding daarvan verstrekken van gegevens aan het verwijzingsportaal. Vanaf het moment dat de vraag via het verwijzingsportaal bankgegevens bij het koppelveld van de bank is aangekomen en de bank gegevens verwerkt waarmee de vraag kan worden beantwoord, is de bank verwerkingsverantwoordelijke. Dit koppelveld, waarmee de bank op het verwijzingsportaal bankgegevens wordt aangesloten, wordt onder verantwoordelijkheid van de bank ontwikkeld. Verzoeken en vorderingen worden via het koppelveld automatisch gekoppeld aan de gegevens uit de klantadministratie van de bank. Indien de bank over gegevens van de betrokkene beschikt, worden deze automatisch verstuurd. Dit betekent dat de bank als verwerkingsverantwoordelijke enkel achteraf kan controleren of het proces goed is verlopen. Daarom is het portaal zo ingericht dat enkel verzoeken en vorderingen die aan alle vereisten voldoen, aan de bank kunnen worden gestuurd. Daarnaast wordt, in overleg met de banken, een auditproces vormgegeven waarmee onder andere wordt getoetst of alle processtappen juist worden doorlopen. Bank krijgen periodiek inzage in de uitkomst van de audit.

De bank stuurt (persoons)gegevens als antwoord op een zoekopdracht naar het verwijzingsportaal bankgegevens. Vanaf het moment dat deze gegevens worden ontvangen door het verwijzingsportaal bankgegevens, is de bevragende organisatie ten aanzien van de persoonsgegevens die zijn opgenomen in de vordering of het verzoek verwerkingsverantwoordelijke, dus ook verantwoordelijk voor de verdere verwerking van deze gegevens in de eigen systemen.

Loggingsgegevens:

Ten aanzien van de loggingsgegevens die door het verwijzingsportaal bankgegevens worden bewaard, is de minister van Justitie en Veiligheid verwerkingsverantwoordelijke. Deze gegevens worden beheerd door Justid-IBO.

Beheer verwijzingsportaal bankgegevens:

Het beheer van het verwijzingsportaal bankgegevens wordt uitgevoerd door de Justitiële Informatiedienst, met instemming van de minister van Justitie en Veiligheid (Justid in de rol van systeembeheerder, en derhalve verwerker in de zin van artikel 4, onderdeel 8, van de AVG, en verwerker in de zin van artikel 1, onderdeel i, van de Wet politiegegevens). Het verwijzingsportaal wordt beheerd door de Justitiële Informatiedienst, afdeling IBO (Justid-IBO). Aangezien Justid-IBO onder verantwoordelijkheid valt van de minister van Justitie en Veiligheid en er geen sprake is van een gezagsverhouding tussen ministeries onderling, maakt Justid-IBO per aangesloten partij (bevragende organisatie) verwerkersafspraken over onder meer de rechten en plichten van de verschillende partijen ten aanzien van de gegevens, het melden van een datalek, het toegang geven van personen tot het verwijzingsportaal bankgegevens binnen Justid (medewerkers hebben alleen in zeer uitzonderlijke gevallen volgens vastgestelde procedures toegang tot persoonsgegevens), uitvoeren van audits en feitelijke werkplekken van beheerders. Justid-IBO heeft kortom de rol om de gegevens technisch te verbinden en bij de in beheer name de taken uit te voeren die zijn opgenomen in de verwerkersafspraken.

4.6 Dataminimalisatie

Gegevensverwerking moet worden beperkt tot wat noodzakelijk is voor de doeleinden waarvoor persoonsgegevens worden verwerkt.⁸ Dit heeft betrekking op de hoeveelheid verzamelde gegevens, de mate waarin zij worden verwerkt, de termijn waarvoor zij worden opgeslagen (en vervolgens vernietigd) en de toegankelijkheid daarvan.

Mede vanuit het oogpunt van dataminimalisatie is gekozen voor een systeem in de vorm van een koppeling, in plaats van bijvoorbeeld een database die wordt gevuld met klantgegevens van banken waarin overheidsinstanties kunnen zoeken. Een dergelijke database vergt een regelmatige overdracht van een bestand met alle klantgegevens van banken, zodat de gegevens die worden opgevraagd steeds actueel zijn. Binnen de gekozen oplossing wordt daarentegen enkel naar aanleiding van een specifieke vordering of verzoek de noodzakelijke informatie verstrekt. Ook wordt bij het gebruik van het verwijzingsportaal bankgegevens telkens zo veel mogelijk informatie over de betrokkene ingevuld, zodat zo gericht mogelijk vragen kunnen worden gesteld en de kans zo klein mogelijk is dat gegevens worden verstrekt over personen waarop het verzoek geen betrekking heeft. Een uitzondering hierop is het opvragen van gegevens met behulp van het burgerservicenummer. Als dat nummer beschikbaar is wordt er, vanwege de beperkte foutgevoeligheid, juist voor gekozen om geen andere gegevens toe te voegen bij het opvragen van informatie. Aan het systeem zijn verder enkele technische eisen gesteld die ertoe dienen het verstrekken van onnodig veel persoonsgegevens te voorkomen. Zo is er bijvoorbeeld een maximaal aantal zoekresultaten per bank en worden vorderingen en verzoeken die betrekking hebben op personen die niet bij de bank bekend zijn direct vernietigd.

Gelet hierop draagt het verwijzingsportaal bankgegevens ook bij aan een effectievere (snellere), kwalitatief betere (minder fouten) en veiligere manier van gegevensverstrekking van banken aan de bevragende organisaties.⁹

4.7 Gebruik burgerservicenummer

Het wetsvoorstel maakt mogelijk dat het burgerservicenummer wordt gebruikt om de koppeling te maken van een vordering of een verzoek in het portaal met de administratie van een aangesloten bank of betaaldienstverlener. Vanwege het unieke karakter van het burgerservicenummer en het brede gebruik van het nummer binnen de overheid, zijn aan het gebruik van het burgerservicenummer door private partijen risico's verbonden voor de betrokkenen. In het onderhavige geval zijn deze risico's voor betrokkenen afgewogen tegen de risico's voor betrokkenen die bestaan als in het portaal geen burgerservicenummer zou worden gebruikt. De uitkomst hiervan is dat de risico's van het gebruik van het burgerservicenummer opwegen tegen de risico's als geen burgerservicenummer zou worden gebruikt.

Het gebruik van het burgerservicenummer is noodzakelijk om gericht en snel informatie uit de administratie van aangesloten banken en betaaldienstverleners te kunnen opvragen ten behoeve van verstrekking via het verwijzingsportaal. Voor het gebruik van het burgerservicenummer is gekozen in het kader van dataminimalisatie: naarmate gericht gezocht kan worden, worden de zoekresultaten specifiekier. Indien wordt gezocht met gebruik van een uniek nummer, het burgerservicenummer, dat ook een beveiliging bevat tegen typefouten, is er maximaal kans op één uniek zoekresultaat. Dit betekent dat alleen gegevens van die betrokkene door de bank aan de vragende instantie worden

⁸ Artikel 5, eerste lid, onderdeel c, AVG en artikel 4, eerste lid, onderdeel c, Richtlijn (EU) 2016/680.

⁹ Artikel 5, eerste lid, onderdelen d en f, AVG en artikel 4, eerste lid, onderdelen d en f, Richtlijn (EU) 2016/680.

verstrekt. In het wetsvoorstel is uitdrukkelijk beschreven dat het burgerservicenummer op grond van dit wetsvoorstel aan de kant van banken en betaalinstellingen alleen mag worden gebruikt om identificerende gegevens geautomatiseerd in de eigen administratie op te zoeken ten behoeve van een vordering of verzoek op grond van het verwijzingsportaal bankgegevens. Banken en betaaldienstverleners kunnen het burgerservicenummer hiervoor alleen gebruiken als zij daarover al beschikken op grond van een andere wettelijk voorschrift. Daarbij dienen zij zich te houden aan de Wabb.

4.8 Overige maatregelen

Het verwijzingsportaal bankgegevens is zo ingericht dat het naast de genoemde waarborgen nog verschillende andere waarborgen bevat om de verwerking van persoonsgegevens te beperken, de kwaliteit van de gegevens te waarborgen en de verwerkingen te beveiligen. Deze maatregelen worden vastgelegd bij of krachtens algemene maatregel van bestuur, in een vorderingsprotocol en een verwerkersovereenkomst en zijn periodiek onderwerp van een audit.

Om ongeoorloofde toegang tot het systeem te voorkomen, is het systeem niet toegankelijk via het internet. Het verwijzingsportaal bankgegevens heeft een eigen fysieke infrastructuur, die met een firewall is afgeschermd van het netwerk van het ministerie van Justitie en Veiligheid. Ook is er een autorisatie- en inlogvoorziening voor medewerkers die bevoegd zijn gegevens op te vragen en worden de beheerders van het systeem door de AIVD gescreend. De identificatie, authenticatie en autorisatie verloopt voor onderdelen van de Rijksoverheid via de gebruikelijke systemen die de Rijksoverheid hiervoor gebruikt. De opsporingsdiensten zijn verantwoordelijk voor het gebruikersbeheer van de eigen organisatie. De autorisatie binnen het verwijzingsportaal bankgegevens wordt bepaald op basis van de rol die gebruiker heeft binnen zijn eigen organisatie. Dit betekent dat een geautoriseerde medewerker van de Belastingdienst die inlogt op het portaal daarin alleen die gegevens kan vorderen die hij op grond van de voor hem geldende vorderingsgrondslag ook mag vorderen.

Voordat het verwijzingsportaal bankgegevens in gebruik zal worden genomen, wordt een penetratietest uitgevoerd.

In het systeem worden verder verschillende maatregelen genomen om de inbreuk op de persoonlijke levenssfeer te beperken, bijvoorbeeld het versleuteld versturen van (persoons)gegevens. Hiermee is gekozen voor een oplossing die zo min mogelijk risico's met zich brengt.

4.9 Rechten van betrokkenen

De betrokkene kan bij de bank of betaaldienstverlener terecht voor een antwoord op de vraag over welke gegevens de bank van de betrokkene beschikt. De bank of betaaldienstverlener moet deze informatie in beginsel verstrekken op grond van artikel 12 AVG (transparantiebeginsel). Welke informatie verstrekt moet worden is veelal opgenomen in een privacyverklaring. De meeste banken hebben een privacyverklaring. Daarin is vaak ook opgenomen dat een bank op basis van wettelijke verplichtingen gegevens moet verwerken; verstrekken is een vorm van verwerken. Op grond van artikel 23 AVG kunnen aan de reikwijdte van de verplichtingen en rechten van betrokkenen (onder voorwaarden en in bepaalde situaties) beperkingen gelden. In de gevallen waar het in dit wetsvoorstel om gaat zal dat veelal de in artikel 23, eerste lid, onderdeel d, genoemde situatie zijn: 'de voorkoming, de opsporing en de vervolging van strafbare feiten...'. Indien de betrokkene vraagt of de bank of betaaldienstverlener deze informatie aan derden heeft verstrekt, mag de bank of betaaldienstverlener hier geen antwoord op geven voor zover hiervoor in de (specifieke) wet geheimhouding is voorgescreven. Zie bijvoorbeeld artikel 126bb Sv voor een dergelijke wettelijke geheimhoudingsplicht.

De betrokkene kan eveneens aan de aangesloten overheidsinstanties vragen over welke informatie zij beschikken. Zij zullen dit verzoek eveneens toetsen aan de hand van de wettelijke kaders die van toepassing zijn.

5. Uitvoeringsgevolgen

Het verwijzingsportaal bankgegevens is nodig voor de volledig geautomatiseerde doorgeleiding van identificerende gegevens. De kosten voor de ontwikkeling en ingebruikname worden begroot op totaal circa 9,1 mln. euro. De jaarlijkse exploitatie- en onderhoudskosten worden thans geschat op 1,2 mln. euro. Deze kosten worden deels betaald uit een Europese subsidie. De overige kosten komen voor rekening van het Ministerie van Justitie en Veiligheid en het Ministerie van Financiën.

Met de introductie van het verwijzingsportaal bankgegevens wijzigt het proces van het versturen van een vordering of verzoek aan een bank of andere betaaldienstverlener en het ontvangen van de identificerende gegevens. Dit heeft zowel organisatorische als technische gevolgen voor de overheidsinstanties die bij het verwijzingsportaal bankgegevens zijn aangesloten. De voorzieningen bij de overheidsinstanties komen voor rekening van deze organisaties. Hier staat tegenover dat de verwach-

ting is dat het automatiseren van het proces voor de opsporingsdiensten tijdswinst per opsporingszaak zal opleveren, omdat er per vordering of verzoek minder handelingen verricht hoeven te worden. Hierdoor kunnen in dezelfde periode meer vorderingen of verzoeken worden gedaan in vergelijking met de huidige situatie. Hiermee kan sneller worden gereageerd in specifieke zaken en is meer actuele informatie voorhanden. Verwacht mag worden dat opsporingsdiensten adequater en sneller kunnen acteren en daarmee het succes van opsporingsonderzoeken kunnen vergroten.

Het wetsvoorstel is voor een uitvoeringstoets voorgelegd aan de Justitiële Informatiedienst, de politie, het OM, FIU-Nederland, de FIOD en de Belastingdienst. Op grond van de uitvoeringstoetsen is geconcludeerd dat het wetsvoorstel voor deze organisaties uitvoerbaar is. De uitvoeringstoetsen hebben dan ook niet geleid tot aanpassing van het wetsvoorstel.

5.1 Gevolgen voor ICT

Het verwijzingsportaal is bedoeld om het proces voor het vorderen, opvragen en verstrekken van identificerende gegevens bij banken en betaaldienstverleners geautomatiseerd te laten plaatsvinden. Opsporingsdiensten kunnen via het verwijzingsportaal gegevens opvragen, indien nodig bij meerdere banken tegelijkertijd. Het portaal wordt hiertoe gekoppeld aan de systemen van banken. Banken worden wettelijk verplicht om bevragingen via het portaal geautomatiseerd te beantwoorden.

5.2 BIT advies

Op 10 december 2018 heeft het BIT advies uitgebracht over het VB. Het BIT onderschrijft het nut en de noodzaak van het VB. Het VB zoals het nu is ontworpen, vindt zij echter nog geen robuuste oplossing om het huidige proces goed te vervangen. Ter onderbouwing hiervan heeft het BIT op vier onderdelen bevindingen gedaan: (i) het ontbreken van inzicht voor opsporingsambtenaren of de door banken aangeleverde gegevens compleet zijn; (ii) het ontbreken van enkele noodzakelijke beveiligingsmaatregelen; (iii) de gewenste beschikbaarheid van het VB kan nog niet worden gegarandeerd; en (iv) het VB is nog niet direct te gebruiken voor bevragingen bij alle banken, omdat banken waarschijnlijk niet allemaal tijdig zijn aangesloten. Om het VB tot een succes te maken adviseert het BIT om vóór grootschalige inzet een aantal verbeteringen door te voeren ten aanzien van het ontwerp, de beveiliging, de beschikbaarheid en de bruikbaarheid van het VB. Voor de nadere uitwerking van de adviezen wordt verwezen naar het BIT-advies d.d. 10 december 2018 (bijlage bij Kamerstuk 26 643, nr. 592).

Reactie op BIT advies:

Mede gelet op de adviezen van het BIT is de planning van de implementatie van het VB een half jaar vooruitgeschoven, van 1 juli 2019 naar 1 januari 2020. Het ontwerp is inmiddels op belangrijke punten aangepast en aanvullende maatregelen zijn gepland om de robuustheid van het VB te verbeteren. Binnen het project VB zijn gedurende het afgelopen jaar al concrete maatregelen genomen om het VB als systeem en de processen daaromheen te verbeteren en de aansluiting van banken goed voor te bereiden. De uitwerking daarvan heeft deels parallel gelopen met het onderzoek en de presentatie van de uitkomsten van het BIT. Om die reden is een belangrijk deel van de door het BIT geadviseerde maatregelen al geadresseerd of zelfs gerealiseerd. De doorgevoerde aanpassingen zijn voor elk van de vier delen van het BIT advies toegelicht door de minister van Justitie en Veiligheid in zijn brief aan de Tweede Kamer van 5 februari 2019 (Kamerstuk 26 643, nr. 592).¹⁰

6. Regeldruk

Banken en andere betaaldienstverleners verstrekken ook op dit moment, naar aanleiding van een vordering of een verzoek, gegevens aan de politie, de bijzondere opsporingsdiensten, het Openbaar Ministerie, de FIU-Nederland en de Belastingdienst. Het aantal vorderingen en verzoeken dat banken en andere betaaldienstverleners nu ontvangen, verschilt sterk per partij. Afhankelijk van de hoeveelheid ontvangen vorderingen en verzoeken, alsmede van de wijze waarop de interne organisatie van de bank of betaaldienstverlener is ingericht, levert het gebruik van het verwijzingsportaal bankgegevens een besparing op, omdat medewerkers van banken of betaaldienstverleners de gevraagde of gevorderde gegevens niet meer handmatig hoeven te verstrekken. Daarvoor wordt op dit moment een onkostenvergoeding uitgekeerd, die zal komen te vervallen, zodat deze kostenbesparing geen regeldrukeffect heeft.

De aansluiting op het verwijzingsportaal bankgegevens vergt een eenmalige ICT-aanpassing, die vervolgens moet worden onderhouden en beheerd. De kosten voor deze ICT-aanpassing en het beheer verschillen per bank en betaaldienstverlener en komen voor rekening van de betreffende bank en betaaldienstverlener. De omvang van de kosten is onder andere afhankelijk van het aantal (klant)syste-

¹⁰ Kamerstukken II 2018/19, 26 643, nr. 592 (bijlage).

men dat op het verwijzingsportaal bankgegevens moet worden aangesloten en het huidige ontwerp van deze systemen. De omvang van een ICT systeem kan worden uitgedrukt in functiepunten. ICTU heeft in 2017 in een onderzoek ingeschat dat de koppeling die banken moeten ontwikkelen 34 functiepunten telt. ICTU gebruikt standaard productiviteitscijfers van NESMA (17 uur per functiepunt) en vermenigvuldigt het aantal uren met een factor 1,5 vanwege de complexiteit. Hieruit volgt een geraamde impact van 867 ontwikkeluren per bank. Met een intern uurtarief voor hoogopgeleide medewerkers van € 54 zijn de kosten voor ontwikkeling geraamd op € 46.818. Op basis van een pilot met ABN AMRO bestaat de aansluiting voor de helft uit ontwikkelkosten, de andere helft bestaat uit kosten voor vooronderzoek, informatiebeveiliging en coördinatie. Wanneer deze uren (867) geraamd worden tegen het tarief voor managers en leidinggevendenden (€ 77) leidt dit tot € 66.759 aan overige kosten. Verder dient de bank een penetratietest uit te voeren om de beveiliging te toetsen. De kosten hiervan worden ingeschat op € 20.000. Hiermee komen de incidentele kosten per bank op € 133.597. Naar verwachting vallen 87 banken binnen de verplichting om aan te sluiten, waarmee de totale incidentele kosten voor de bankensector: € 11.622.939 bedragen.

Opgemerkt moet worden dat uit het onderzoek van ICTU uit 2017 een andere kostenindicatie volgde: de totale ontwikkelkosten voor een grote bank zijn toen door ICTU voorlopig geschat op (afgerond) € 729.000, de kosten per middelgrote bank werden ingeschat op gemiddeld € 110.000 en per kleine bank op gemiddeld € 55.000. ABN AMRO heeft daarentegen aangegeven voor aansluiting op het systeem voorsnag op € 1,2 miljoen in te schatten. Dat is wel inclusief een extra inspanning die geleverd is bij deelname aan een pilot.

De daadwerkelijke financiële consequenties kunnen per bank sterk uiteenlopen en zijn afhankelijk van de omvang van de klantadministratie en de complexiteit van de technische infrastructuur bij banken.

De structurele lasten voor banken voor het beheer en onderhoud van de verbinding met het verwijzingsportaal bankgegevens worden geschat ten opzichte van de ontwikkelkosten. Op basis van de 'handreiking voor kosten-baten analyses voor ICT projecten' van Ecorys uit 2007 worden de structurele lasten ingeschat op 20% van de ontwikkelkosten. De structurele lasten worden derhalve per bank op € 9.364 per jaar geschat en voor de totale bankensector op € 814.633.

Door de aansluiting op het verwijzingsportaal bankgegevens worden de administratieve lasten verlicht die nu gepaard gaan met het beoordelen en beantwoorden van vorderingen.

Het wetsvoorstel heeft geen financiële gevolgen voor burgers.

7. Consultatie en advies

Het wetsvoorstel is binnen het project verwijzingsportaal bankgegevens afgestemd met de betrokken overheidsinstanties en een vertegenwoordiging van de banken en de Nederlandse Vereniging van Banken (NVB). Over de gevolgen van het verwijzingsportaal voor de ICT heeft het BIT op 10 december 2018 een advies uitgebracht. Voor een korte beschrijving van dit advies en de wijze waarop met het advies is omgegaan wordt verwezen naar paragraaf 5.2.

7.1 Internetconsultatie

Voor dit wetsvoorstel heeft van 14 juni tot 14 juli 2018 internetconsultatie plaatsgevonden. Daarbij zijn dertien openbare reactie binnengekomen en drie niet openbare reacties. Van de openbare reacties zijn er negen afkomstig van particulieren. De overige vier reacties zijn van de Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders (KBG), de Stichting Privacy First, de NVB en de Piratenpartij.

7.2 Consultatiereacties

Uit de meeste reacties komen zorgen naar voren over de bescherming van de persoonsgegevens bij het gebruik van het verwijzingsportaal bankgegevens. Dit onderwerp heeft bij de ontwikkeling van het verwijzingsportaal bankgegevens veel aandacht gehad. Naar aanleiding van de reacties wordt hier in de toelichting uitgebreider op ingegaan. Ook is het verslag van de uitgevoerde gegevensbeschermingseffectbeoordeling (PIA) als bijlage bij deze memorie van toelichting gevoegd. Daarin staat in detail beschreven hoe aan de regels op het gebied van gegevensbescherming wordt voldaan.

Op een aantal specifieke vragen en opmerking uit de reacties wordt hieronder nog ingegaan.

Twee reacties stellen aan de orde dat de gegevens die via het portaal bij een bank worden opgevraagd beter bij de rekeninghouder zelf opgevraagd kunnen worden.

In het geval van de Belastingdienst gebeurt dit op grond van het Voorschrift informatie fiscus/banken in principe ook eerst bij de belastingplichtige zelf. Indien de informatie niet via de belastingplichtige

zelf kan worden verkregen, krijgt hij de gelegenheid om dit zelf bij de bank op te vragen. Pas als dat niet tot het gewenste resultaat leidt vraagt de Belastingdienst de identificerende gegevens op bij de bank via het verwijzingsportaal bankgegevens. Bij gebruik van het portaal door de Belastingdienst op grond van artikel 62bis Invorderingswet (één bankrekeningnummer) controleert de Belastingdienst gegevens die van de rekeninghouder zelf zijn verkregen. Ook bij het vorderen van gegevens door opsporingsdiensten zal eerst worden afgewogen of er geen andere manier is om aan de benodigde gegevens te komen; een wijze die minder inbreuk maakt op het recht op bescherming van persoonsgegevens. Daarbij is het wel belangrijk om te beseffen dat opsporingsdiensten de informatie opvragen ten behoeve van het voorkomen en opsporen van fraude en andere vormen van criminaliteit en het opsporen van (criminele) vermogens. Het is in het algemeen niet mogelijk dit onderzoek uit te voeren als de betrokkenen daarvan op de hoogte zijn.

In een van de reacties wordt gevraagd of in de wet kan worden benoemd welke gegevens via het verwijzingsportaal bankgegevens opgevraagd kunnen worden en met welk doel. Voorgesteld wordt om dit bij of krachtens een algemene maatregel van bestuur voor te schrijven. In het wetsvoorstel is nadrukkelijk benoemd dat aangesloten overheidsinstanties via het verwijzingsportaal bankgegevens alleen *identificerende gegevens* kunnen opvragen van cliënten van banken en betaaldienstverleners en van personen die als gemachtigden namens hen zeggenschap kunnen uitoefenen over financiële producten die zij afnemen. Verder is beschreven *welke vorderingen of verzoeken* de aangesloten overheidsinstanties via het portaal kunnen doen; de grondslagen van de vorderingen die via het portaal gedaan kunnen worden, staan immers opgesomd. Hiermee is voldoende omlijnd welke gegevens via het portaal kunnen worden verstrekt en met welk doel. Bij of krachtens algemene maatregel van bestuur wordt nog een opsomming gegeven van alle mogelijke categorieën gegevens die via het portaal uitgevraagd kunnen worden. Deze gegevens worden ook in paragraaf 2.5 van deze toelichting benoemd. Welke categorieën identificerende gegevens in een specifiek geval precies kunnen worden opgevraagd en met welk doel, hangt af van de gebruikte grondslag. De grondslag van het verzoek of de vordering bepaalt dit immers. De opsomming is een technische uitwerking van het begrip identificerende gegevens, zodat een algemene maatregel van bestuur een geschikte plaats is om dit te regelen. Dit levert ook de nodige flexibiliteit op als de bevoegdheden wijzigen of als besloten wordt dat op dezelfde grondslagen nog andere identificerende gegevens via het verwijzingsportaal bankgegevens opgevraagd moeten kunnen worden. Vanwege de kaders van de wet kunnen alleen identificerende gegevens, die gevorderd kunnen worden op grond van de wettelijke grondslagen die zijn opgesomd in de wet, worden toegevoegd. Andere wijzigingen of uitbreidingen in de op te vragen gegevens vergen een wetswijziging.

De NVB vraagt wat de gevolgen zijn van de introductie van het verwijzingsportaal bankgegevens voor de aansprakelijkheid van aangesloten banken en betaaldienstverleners als blijkt dat zij ten onrechte gegevens hebben verstrekt. Een andere partij vraagt of de Minister van Justitie en Veiligheid daarvoor aansprakelijk is.

Het wetsvoorstel laat bestaande regels en systemen voor het vaststellen van aansprakelijkheid onverlet. Alle betrokken partijen zijn en blijven er zelf voor verantwoordelijk dat zij bij het verwerken van gegevens de regels in acht nemen die daarbij gelden. Voor de partijen die persoonsgegevens via het portaal verstrekken, geldt dat zij dit doen op grond van een wettelijke verplichting, zodat daarvoor een rechtsgrond bestaat (artikel 6, eerste lid, onderdeel c, algemene verordening gegevensbescherming). Banken en betaaldienstverleners mogen er daarbij vanuit gaan dat de vorderingen en verzoeken die hen via het systeem bereiken rechtmatig zijn gedaan en dat zij dus verplicht zijn daaraan te voldoen. De werking van het systeem bevat verschillende waarborgen om dat te verzekeren.

De NVB benadrukt dat banken graag toegang zouden krijgen tot de Basisregistratie Persoonsgegevens (BRP) om op basis van hit/no hit gegevens van hun cliënten te verifiëren voordat zij die via het verwijzingsportaal verstrekken.

Voor de werking van het verwijzingsportaal bankgegevens zou de controle die de NVB voorstelt van toegevoegde waarde zijn. Die controle zorgt ervoor dat de gegevens die via het portaal worden verstrekt beter betrouwbaar zijn. Ook voorkomt het dat geen gegevens worden gevonden omdat bij de bank bijvoorbeeld niet de juiste adresgegevens geregistreerd staan. Of banken voor een dergelijke controle toegang zouden moeten krijgen tot het BPR vraagt echter om een bredere afweging van de noodzakelijkheid en de proportionaliteit van die verwerking. Daarbij moet worden afgewogen of de positieve effecten voor de werking van het verwijzingsportaal opwegen tegen de inbreuk op de rechten van betrokkenen. Bij een dergelijke afweging zal ook moeten worden bekeken of er nog andere positieve of negatieve effecten van een dergelijke controle zijn. Een en ander gaat het bestek van dit wetsvoorstel te buiten.

In een van de reacties wordt de vraag opgeworpen hoe het huidige wetsvoorstel zich verhoudt tot eerdere voornemens om het opvragen van informatie van banken efficiënter in te richten. De behoefte om het proces van het vorderen of opvragen van identificerende gegevens van banken

efficiënter in te richten bestaat al lange tijd. Om verschillende redenen is dit eerder niet doorgegaan. Door de ontwikkelingen in het betalingsverkeer nam intussen wel de noodzaak toe om snel actuele gegevens te kunnen opvragen. Ook namen de mogelijkheden toe om een technische faciliteit als het verwijzingsportaal te beveiligen, alsmede om waarborgen te scheppen voor de bescherming van de privacy. Deze gewijzigde omstandigheden maken dat het verwijzingsportaal bankgegevens nu wordt ingericht.

Verschillende partijen vragen hoe wordt beoordeeld of het verwijzingsportaal bankgegevens effectief is en wordt gebruikt zoals het is bedoeld. Zij vragen of en hoe de Minister van Justitie en Veiligheid het systeem laat toetsen en daarover rapporteert.

Deze technische aspecten zullen worden geregeld bij of krachtens algemene maatregel van bestuur. Een concept voor een algemene maatregel van bestuur is in het kader van de internetconsultatie gepubliceerd. Daaruit volgt dat de Minister van Justitie en Veiligheid jaarlijks een verslag opstelt waaruit het aantal opvragen volgt en op welke grondslag die zijn gedaan. Verder laat hij elke twee jaar een audit uitvoeren waarbij wordt beoordeeld of het verwijzingsportaal bankgegevens voldoet aan de regels uit de wet en gesteld bij of krachtens algemene maatregel van bestuur.

De NVB wijst erop dat veel opsporingsdiensten de bevoegdheid hebben om identificerende gegevens op te vragen op grond van artikel 19 van de Wed. Zij verzoekt artikel 19 van de Wed aan te passen, zodat het voor degene die een vordering op grond van de Wed ontvangt duidelijker is waarop die vordering is gebaseerd en hij kan controleren of die vordering bevoegd is gedaan.

In paragraaf 3 over de bescherming van persoonsgegevens is al beschreven dat de procedures voor het goedkeuren van een vordering en het vastleggen daarvan buiten het verwijzingsportaal om plaatsvinden. Deze wijzigen ook niet door dit wetsvoorstel. Dat geldt ook voor de procedures voor vorderingen op grond van de Wed. Verder is van belang dat niet alle partijen die op grond van artikel 19 van de Wed de bevoegdheid hebben om identificerende gegevens op te vragen, ook zijn aangesloten op het verwijzingsportaal. Alleen de opsporingsambtenaren van de Fiscale Inlichtingen- en Opsporingsdienst, de Inlichtingen- en Opsporingsdienst van de Nederlandse Voedsel- en Warenautoriteit, de directie Opsporing van de Inspectie Sociale Zaken en Werkgelegenheid en de Inlichtingen- en Opsporingsdienst van de Inspectie Leefomgeving en Transport zullen de mogelijkheid krijgen om via het portaal identificerende gegevens op te vragen op grond van artikel 19 van de Wed. Voor ambtenaren van deze diensten gelden dezelfde waarborgen voor autorisatie en gebruik van het verwijzingsportaal bankgegevens als voor de politie.

De NVB merkt op dat het op grond van het wetsvoorstel onvoldoende duidelijk is voor welke taken de FIU-Nederland identificerende gegevens in het verwijzingsportaal bankgegevens kan opvragen.

De FIU-Nederland kan in het portaal identificerende gegevens opvragen op grond van artikel 17 van de Wwft. Uit dat artikel volgt dat de FIU-Nederland die gegevens kan opvragen in het kader van haar taak om gegevens te verzamelen om te bezien of meldingen van ongebruikelijke transacties van belang kunnen zijn voor het voorkomen en opsporen van misdrijven en om anderen van relevante gegevens te voorzien. Door de verwijzing naar artikel 17 van de Wwft blijkt dit voldoende duidelijk uit de wet. Net als in de huidige situatie, waarbij de FIU-Nederland handmatig vordert, is het primair de verantwoordelijkheid van de FIU-Nederland om ervoor te zorgen dat zij alleen gegevens vordert via het portaal als zij daartoe bevoegd is. In het kader van de audits naar de werking van het systeem zal dit worden beoordeeld.

De NVB stelt aan de orde dat de kosten voor het aansluiten op het verwijzingsportaal bankgegevens disproportioneel zijn voor banken die in Nederland maar weinig cliënten hebben. De NVB vraagt of nog nader onderzocht kan worden wat de mogelijkheden zijn om die kosten te beperken. Ook met betrekking tot specifieke klantgroepen, waarvoor het complex kan zijn om gegevens via het portaal aan te leveren, vraagt de NVB om andere oplossingen te onderzoeken.

Zoals de NVB zelf ook aangeeft, wordt momenteel gezamenlijk met de bij het project betrokken partijen onderzocht hoe de kosten van het aansluiten voor kleine partijen beperkt kunnen worden. Ook met betrekking tot specifieke klantgroepen kan gezamenlijk worden bekeken of er mogelijkheden zijn voor een aangepaste werkwijze. Op grond van de richtlijn tot wijziging van de vierde anti-witwasrichtlijn bestaat wel de verplichting dat identificerende gegevens via een centraal elektronisch systeem geautomatiseerd opvraagbaar zijn. Aan deze minimumeis zal dus voldaan moeten worden.

De NVB wijst erop dat op dit moment geen Europese standaard bestaat voor de inrichting van het portaal en verzoekt om dit wel te bevorderen, zodat banken die in verschillende lidstaten opereren geen kosten hoeven maken voor de implementatie van verschillende systemen.

Op dit moment bestaat nog geen duidelijk beeld van de manier waarop de verschillende lidstaten het centrale elektronische systeem, dat de richtlijn tot wijziging van de vierde anti-witwasrichtlijn voorschrijft, in willen richten. Wel is duidelijk dat hier verschillende ideeën over bestaan. Dit kan worden verklaard doordat de richtlijn als doel heeft om nationale procedures voor het opvragen van identificerende gegevens te centraliseren en te automatiseren, zonder direct in te grijpen op vormge-

ving van die procedures zelf. Omdat die procedures per lidstaat verschillen, zal dat naar verwachting ook zo zijn als zij geautomatiseerd plaatsvinden. Daar komt nog bij dat veel lidstaten al beschikken over een geautomatiseerd systeem (dat aansluit op hun nationale procedures). Deze landen zullen bij de implementatie waarschijnlijk zoveel mogelijk bij dit bestaande systeem willen aansluiten. Om te bevorderen dat andere lidstaten aansluiten bij de vorm die in Nederland is gekozen, heeft Nederland wel een presentatie voor de andere lidstaten gegeven in Brussel.

De NVB vraagt tot slot om een kostendekkende vergoeding voor ontwikkeling van systemen om aan te sluiten op het portaal en een jaarlijkse bijdrage in de kosten.

De kosten die banken maken voor de aansluiting op het portaal vloeien voort uit de richtlijn tot wijziging van de vierde anti-witwasrichtlijn, aangezien die voorschrijft dat identificerende gegevens van – kort gezegd – cliënten van banken opgevraagd kunnen worden via een centraal elektronisch informatiesysteem. Uitgangspunt is dat marktpartijen dergelijke kosten, die direct voortkomen uit Europese voorschriften, zelf dragen. Er is geen reden daar in dit geval een uitzondering op te maken.

In twee reacties wordt gevraagd om toe te lichten wat de verhouding is van het wetsvoorstel tot de Wet op de inlichtingen en veiligheidsdiensten 2018 (Wiv 2018) en tot het wetsvoorstel gegevensverwerking in samenwerkingsverbanden (Wgs).

Het onderhavige wetsvoorstel heeft geen betrekking op bevoegdheden van inlichtingen- en veiligheidsdiensten en staat daarmee los van de Wiv. De inlichtingen- en veiligheidsdiensten kunnen het verwijzingsportaal bankgegevens niet raadplegen. Voor de Wgs geldt dat de wet erop is gericht om samenwerking tussen verschillende partijen te bevorderen indien dit een doel van zwaarwegend algemeen belang dient. Hierbij wordt primair gedacht aan samenwerking tussen publieke partijen, al kunnen ook private partijen betrokken worden. Om het doel van het samenwerkingsverband te bereiken, kunnen partijen die aangesloten zijn bij een samenwerkingsverband in de zin van de Wgs gegevens uitwisselen en combineren. Dit is anders in het onderhavige wetsvoorstel, dat betrekking heeft op een middel voor het verstrekken van informatie door banken en betaaldienstverleners aan aangesloten overheidsinstanties. De overheidsinstanties gebruiken deze gegevens vervolgens voor de uitvoering van hun individuele taak, zodat geen sprake is van samenwerking. Beide wetsvoorstellen dienen dan ook een verschillend doel.

De KBG vraagt in haar reactie of ook gerechtsdeurwaarders de mogelijkheid kunnen krijgen om het verwijzingsportaal bankgegevens te raadplegen vanwege hun rol als informatie-instantie op grond van de Uitvoeringswet verordening Europees beval tot conservatoir beslag op bankrekeningen (Uitvoeringswet EAPO).

Zoals beschreven komt het onderhavige wetsvoorstel in eerste instantie voort uit de wens om effectiever op te kunnen treden tegen criminaliteit. Het project is gestart als onderdeel van de Rijksbrede aanpak criminaliteit. Met deze achtergrond zijn dan ook de overheidsinstanties geselecteerd die gegevens kunnen opvragen via het verwijzingsportaal bankgegevens. Eventuele toegang van gerechtsdeurwaarders tot het verwijzingsportaal bankgegevens kent een heel andere achtergrond en strekking. Dit vraagt dan ook om een nieuwe beoordeling van de noodzaak en proportionaliteit van toegang door gerechtsdeurwaarders tot het verwijzingsportaal. Dit valt buiten het bestek van dit wetsvoorstel.

7.3 Advies Adviescollege toetsing regeldruk

Op 19 juni 2018 is advies over het wetsvoorstel gevraagd aan het Adviescollege toetsing regeldruk. Het Adviescollege heeft op 5 juli advies uitgebracht. Het college adviseert om een berekening te maken van de structurele en eenmalige gevolgen voor regeldruk conform de daarvoor geldende landelijke systematiek en die toe te voegen. Naar aanleiding van dit advies is de paragraaf regeldruk aangevuld.

7.4 Advies Autoriteit Persoonsgegevens

Bij brief van 29 november 2018 heeft de Autoriteit Persoonsgegevens (AP) advies uitgebracht over het wetsvoorstel, op grond van artikel 36, vierde lid, van de Algemene verordening gegevensbescherming (AVG). De AP adviseert om in de memorie van toelichting de beoogde invulling van de verwerkingsverantwoordelijkheid en de vormgeving van de relatie met de beheerder/verwerker uiteen te zetten. Het advies is bij het wetsvoorstel betrokken en heeft tot een aanpassing in de toelichting geleid in de zin dat in paragraaf 4 een onderdeel is ingevoegd over de verwerkingsverantwoordelijkheid.

§ 8 Overgangsrecht en inwerkingtreding

Beoogd is om de wet op 1 januari 2020 in werking te laten treden. Er is niet voorzien in overgangsrecht, aangezien het systeem van het verwijzingsportaal bankgegevens alleen werkt als alle banken en andere betaaldienstverleners daarop zijn aangesloten. Als dat niet het geval is, moeten immers

meerdere processen worden gevolgd om bij verschillende instellingen dezelfde informatie te halen, terwijl het wetsvoorstel juist tot doel heeft om het proces van opvragen/vorderen en verstrekken van identificerende gegevens efficiënter te maken. Daarnaast is de verwachting dat in geval van overgangrecht banken en andere betaaldienstverleners zo laat mogelijk zullen aansluiten.

§ 9 Transponeringstabel

Artikel 32bis van richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU (PbEU 2018, L 156)

Bepaling EU-regeling	Bepaling in implementatieregeling of bestaande regeling: Toelichting indien niet geïmplementeerd of naar zijn aard geen implementatie behoeft	Omschrijving beleidsruimte	Toelichting
32bis, lid 1	Artikel 3:267i Wft	–	
32bis, lid 2	Artikel 3:267i Wft		Het verwijzingsportaal bankgegevens is direct toegankelijk voor de FIU en bevoegde autoriteiten.
32bis, lid 3	Besluit verwijzingsportaal bankgegevens, met uitzondering van de informatie betreffende de uiteindelijk belanghebbende van de houder van de rekening en de datum van opening en sluiting van de rekening of looptijd van de huur van de kluis		Betreft de informatie die via het verwijzingsportaal bankgegevens toegankelijk moet zijn. De verplichting informatie over de uiteindelijk belanghebbende, de datum van opening en sluiting van de rekening of de looptijd van de huur van de kluis te verstrekken zullen in een ander wetgevingstraject worden geïmplementeerd.
32bis, lid 4	Besluit verwijzingsportaal bankgegevens	Lidstaatoptie om meer informatie toegankelijk te maken, hiervan is beperkt gebruik gemaakt.	In het verwijzingsportaal zijn ook enkele administratieve kenmerken van producten en cliënten beschikbaar. Daarnaast is informatie te vorderen en opvraagbaar over cliënten die andere producten afnemen dan betaalrekeningen en kluizen.
32bis, lid 5	–		Behoeft geen implementatie, betreft een verplichting van de Europese Commissie

Artikelsgewijs

Artikel I (Wet op het financieel toezicht)

A

In het voorgestelde artikel 3:267i wordt verwezen naar de SEPA-verordening. Dit onderdeel voegt een definitie van deze verordening toe in artikel 1:1 van de Wft.

B

In het voorgestelde artikel 1:49a is een bepaling opgenomen die DNB en de Minister van Justitie en Veiligheid, als verantwoordelijke voor Justid, verplicht om samen te werken ten behoeve van de goede uitoefening van het toezicht en de handhaving door DNB. Dit houdt onder meer in dat de Minister van Justitie en Veiligheid verplicht is om DNB tijdig te voorzien van de juiste informatie. Dit is nodig, omdat DNB haar taak als toezichthouder op de naleving van de in artikel 3:267i opgenomen verplichtingen voor banken en andere betaaldienstverleners alleen kan uitoefenen als zij beschikt over informatie van de Minister van Justitie en Veiligheid (Justid). Zie ook paragraaf 3.3 van deze toelichting.

C

Met het eerste lid van het voorgestelde artikel 1:93h wordt mogelijk gemaakt dat DNB ten behoeve van het toezicht op de naleving en de handhaving van de in artikel 3:267i opgenomen aansluitverplichting voor banken en andere betaaldienstverleners toezichtvertrouwelijke gegevens kan delen met Justid, als beheerder van het verwijzingsportaal bankgegevens. Dit is noodzakelijk, omdat DNB in het kader van een (lopend) onderzoek of een handavingsmaatregel Justid bijvoorbeeld moet kunnen informe-

ren over eventuele afspraken met een instelling over de termijn waarbinnen een instelling (wederom) aangesloten dient te zijn. Dit kan bijvoorbeeld aan de orde zijn als een last onder dwangsom is opgelegd aan een instelling. Als DNB deze informatie niet met Justid kan delen zou Justid DNB ook niet de informatie kunnen geven die nodig is om te controleren of vervolgens aan de last is voldaan. Het gaat hierbij alleen om het delen van vertrouwelijke gegevens of inlichtingen die geen persoonsgegevens bevatten en die door DNB zijn verkregen in het kader van het toezicht en de handhaving van de verplichtingen uit artikel 3:267i.

D

Artikel 3:267i

Eerste lid, aangesloten private partijen

Banken en andere betaaldienstverleners die rekeningen aanbieden met een IBAN-identificatienummer dat de landcode 'NL' bevat, alsmede banken die kluizen aanbieden, zijn verplicht om aan te sluiten op het verwijzingsportaal bankgegevens. Voor deze partijen is gekozen, omdat artikel 32bis van de richtlijn tot wijziging van de vierde anti-witwasrichtlijn voorschrijft dat in het verwijzingsportaal bankgegevens identificerende gegevens opvraagbaar moeten zijn van houders van rekeningnummers met een IBAN-identificatienummer dat op Nederlands grondgebied is uitgegeven en van houders van kluizen die worden aangehouden bij banken op Nederlands grondgebied. Voor het uitgeven van een rekening met een IBAN-identificatienummer is een zogenaamde Bank Identifier Code (BIC) nodig. Deze BIC wordt gedeeltelijk in het IBAN identificatienummer opgenomen. Als een financiële instelling in Nederland een rekening wil aanbieden met een IBAN-identificatienummer heeft zij daarvoor een Nederlandse BIC nodig. Deze is herkenbaar aan de letters NL in de code.

In het onderhavige wetsvoorstel wordt het begrip IBAN-identificatienummer gebruikt overeenkomstig de definitie in artikel 2, onder 15, van de zogenoemde SEPA-verordening¹¹: een identificatienummer van een internationale betaalrekening, dat een individuele betaalrekening ondubbelzinnig identificeert in een lidstaat, en waarvan de elementen zijn omschreven door de Internationale Organisatie voor Normalisatie (International Standard Organisation – ISO). Op grond van de SEPA-verordening moeten bepaalde in die verordening beschreven rekeningen beschikken over een IBAN-identificatienummer.

Het eerste lid bepaalt dat het verwijzingsportaal bankgegevens wordt beheerd door de Minister van Justitie en Veiligheid.

Tweede lid, cliënten

In het verwijzingsportaal bankgegevens kunnen gegevens opgevraagd worden van houders van rekeningen of andere financiële producten en van personen die als gemachtigde namens die houders over deze producten kunnen beschikken. Hiermee wordt bereikt dat de aangesloten overheidsinstanties via het portaal ruimer inzicht kunnen krijgen in welke natuurlijke personen daadwerkelijk over een bepaalde rekening of een bepaald product kunnen beschikken.

Gegevens over gemachtigden voor een bepaald financieel product zijn niet altijd in de bankadministratie opgenomen. Net als voor andere identificerende gegevens zal dan ook bij de uitwerking van identificerende gegevens bij of krachtens algemene maatregel van bestuur worden bepaald dat de aangesloten banken en betaaldienstverleners de gegevens over eventuele gemachtigden alleen hoeven te verstrekken als die bekend zijn in hun administratie.

Derde lid, vorderingsgrondslagen

Aangesloten banken en betaaldienstverleners moeten identificerende gegevens via het verwijzingsportaal bankgegevens verstrekken als zij een vordering of verzoek krijgen op grond van een van de in het derde lid genoemde grondslagen. De omvang van de bevoegdheid om via het portaal te vorderen of te verzoeken en de omvang van de verplichting om aan die vordering of dat verzoek te voldoen, worden bepaald door die wetgeving en de daarop gebaseerde bepalingen. Bank en betaaldienstverlener verstrekken met andere woorden alleen via het verwijzingsportaal bankgegevens die identificerende gegevens die zij op grond van de (reeds bestaande) wetgeving moeten verstrekken. Hieronder volgt een beknopte toelichting op de verschillende grondslagen voor vorderingen of verzoeken via het verwijzingsportaal bankgegevens.

¹¹ Verordening (EU) nr. 260/2012 van het Europees Parlement en de Raad van 14 maart 2012 tot vaststelling van technische en bedrijfsmatige vereisten voor overmakingen en automatische afschrijvingen in euro en tot wijziging van Verordening (EG) nr. 924/2009 (PbEU 2012, L94).

- Artikel 126a van het Wetboek van Strafvordering
Artikel 126a kent opsporingsambtenaren in het kader van het strafrechtelijk financieel onderzoek een aantal bijzondere bevoegdheden toe. Deze bevoegdheden berusten op de rechterlijke machtiging ex artikel 126, derde lid, Wetboek van Strafvordering. De opsporingsambtenaren dienen bij de uitoefening van deze bevoegdheden een afschrift van die machtiging te tonen. De bevoegdheidsuitoefening is doelgebonden: zij moet ertoe (kunnen) strekken inzicht te verkrijgen in de vermogenspositie van de onderzochte persoon. Met dat doel voor ogen kunnen de bevoegde opsporingsambtenaren aan eenieder bevelen hun op de eerste vordering mondeling of schriftelijk bepaalde informatie te verstrekken. Schriftelijke bescheiden kunnen worden ingezien en kunnen zo nodig in beslag worden genomen. Het bevel kan ook inhouden dat degene tot wie het is gericht, de opsporingsambtenaar een kopie van de gevorderde informatie verstrekt. Voor zover de gevorderde informatie identificerende gegevens betreft, geschiedt de verstrekking via het verwijzingsportaal bankgegevens.
- Artikelen 126nc, 126uc, 126zk van het Wetboek van Strafvordering
De kern van deze artikelen bestaat uit de bevoegdheid van de opsporingsambtenaar om van degene, die daarvoor redelijkerwijs in aanmerking komt en die anders dan ten behoeve van persoonlijk gebruik gegevens verwerkt, te vorderen bepaalde opgeslagen of vastgestelde identificerende gegevens te verstrekken betreffende naam, adres, woonplaats, postadres, geboortedatum, geslacht, rekeningnummers en administratieve kenmerken behorende bij een persoon. In geval van een rechtspersoon kunnen daarnaast gegevens over rechtsvorm en vestigingsplaats worden gevorderd. De bevoegdheid tot het vorderen van identificerende gegevens bestaat in geval van verdenking van misdrijf en de bevoegdheid kan slechts worden uitgeoefend ‘in het belang van het onderzoek’. Dit accentueert dat de bevoegdheid alleen mag worden gehanteerd indien deze bijdraagt aan de opsporing van het delict. De Aanwijzing opsporingsbevoegdheden bevat nadere regels over de inzet van deze bevoegdheid. Deze regels zijn ook van toepassing op vorderingen via het verwijzingsportaal bankgegevens.
- Artikel 126ii van het Wetboek van Strafvordering
Artikel 126ii geeft de officier van justitie de bevoegdheid om in het kader van een verkennend onderzoek naar terroristische misdrijven identificerende gegevens te vorderen. Met behulp van identificerende gegevens kan worden vastgesteld wie de personen zijn waarop het onderzoek zich richt en welke verbanden er zijn tussen personen en tussen situaties en personen.
- Artikel 577bb van het Wetboek van Strafvordering
In artikel 577bb, eerste lid, zijn de bevoegdheden opgesomd die zich lenen voor toepassing in het onderzoek naar het vermogen van de veroordeelde, waaronder het vorderen van bepaalde opgeslagen of vastgelegde identificerende gegevens in de zin van artikel 126nc, tweede lid. Hiertoe kan bijvoorbeeld ook een bankrekeningnummer gerekend worden (eerste lid, onderdeel b). De opsporingsambtenaar is de bevoegde autoriteit, bij bevel daartoe van de officier van justitie.
- Artikel 19 van de Wet op de economische delicten
Artikel 19 verleent opsporingsambtenaren de bevoegdheid inzage te vorderen van gegevens en bescheiden en daarvan kopieën te maken. Zij mogen op grond van deze bepaling ook korte tijd de gegevens en bescheiden meenemen. De bevoegdheid tot het vorderen van inzage van gegevens en bescheiden kan door opsporingsambtenaren ‘in het belang van de opsporing’ en ‘voor zover dat redelijkerwijs voor de vervulling van hun taak nodig is’ worden uitgeoefend.
- Artikel 17 van de Wet ter voorkoming van witwassen en financieren van terrorisme
Artikel 17 van de Wwft geeft de Financiële inlichtingen eenheid (FIU-Nederland) de bevoegdheid om bij een Wwft-instelling die een melding heeft gedaan, alsmede bij een Wwft-instelling die bij een transactie was betrokken en waarover de FIU-Nederland gegevens heeft verzameld, nadere inlichtingen vragen. FIU-Nederland kan die gegevens opvragen in het kader van haar taak om gegevens te verzamelen om te bezien of meldingen van ongebruikelijke transacties van belang kunnen zijn voor het voorkomen en opsporen van misdrijven en om anderen van relevante gegevens te voorzien. Voor zover de gevorderde informatie identificerende gegevens betreft, geschiedt de verstrekking via het Verwijzingsportaal.
- Artikel 53 van de Algemene wet inzake rijksbelastingen
In artikel 53, eerste lid, aanhef en onderdeel a, AWR is geregeld welke verplichtingen voor administratieplichtigen als bedoeld in artikel 52 AWR gelden ten behoeve van de belastingheffing van derden. Op grond van die bepaling zijn banken gehouden om op verzoek informatie te verstrekken ten behoeve van de belastingheffing van derden, om kort gezegd, het mogelijk te maken voor de Belastingdienst (de inspecteur) om derden effectiever te kunnen controleren. Bankens kwalificeren in beginsel als administratieplichtigen. Een derde is ieder ander dan de administratieplichtige wiens administratie wordt geraadpleegd. In deze gevallen gaat het om een individuele derde of groepen van derden. Het zogenoemde voorschrift informatie fiscus/banken¹² bevat beleidsregels met betrekking tot de toepassing van onder meer artikel 53, eerste lid, aanhef en onderdeel a, AWR en artikel 62 IW 1990 (zie ook hieronder). Hierin is aangegeven op welke

¹² Besluit van de Staatssecretaris van Financiën van 13 december 2012, nr. BLKB 2012/1937M (Stcrt. 2012, 26782).

wijze de Belastingdienst om informatie over derden verzoekt met betrekking tot bancaire activiteiten en op welke wijze de banken daaraan moeten voldoen. In verband met het gebruik van het verwijzingsportaal bankgegevens voor de genoemde artikelen zal het voorschrift waar nodig worden aangepast.

- Artikel 62 van de Invorderingswet 1990
Artikel 62 IW 1990 legt aan administratieplichtigen de verplichting op om ten behoeve van de invordering ten aanzien van derden op verzoek van de ontvanger gegevens en inlichtingen te verstrekken, dan wel boeken, bescheiden en andere gegevensdragers of de inhoud daarvan ter beschikking te stellen. Verder maakt het artikel het mogelijk om bij ministeriële regeling werkzaamheden aan te wijzen waarbij het gebruik van het burgerservicenummer verplicht is en tevens aan te wijzen wie in relatie tot die werkzaamheden tot gebruik van het burgerservicenummer verplicht is.
- Artikel 62bis van de Invorderingswet 1990
Artikel 62bis IW 1990 bevordert de controle door de Belastingdienst (de ontvanger) of een door de burger opgegeven bankrekening voor de uitbetaling van een teruggaaf inkomstenbelasting juist is. De banken dienen identificatiegegevens te verstrekken zodat de Belastingdienst kan controleren of een door een belastingschuldige opgegeven bankrekening op zijn naam staat. De banken hebben daarnaast de wettelijke bevoegdheid om burgerservicenummers te gebruiken om de juistheid van de geregistreerde gegevens, met name de combinatie van naam/adres/woonplaats (NAW)-gegevens en burgerservicenummer, te controleren. Dat moet (identiteits)fraude en onnodige fouten voorkomen.
- Artikel 38 van de Algemene wet inkomensafhankelijke regelingen
Artikel 38 Awir regelt de kosteloze verstrekking aan de Belastingdienst/Toeslagen van gegevens en inlichtingen waarvan de kennisneming van belang kan zijn voor de uitvoering van de Awir. Omdat de aanspraak op of de hoogte van een tegemoetkoming mede afhankelijk kan zijn van informatie die niet binnen de Belastingdienst of de Belastingdienst/Toeslagen voorhanden is, is in het eerste lid van genoemd artikel 38 voor decentrale overheden, bepaalde semi-overheidslichamen en voor bij of krachtens algemene maatregel van bestuur aangewezen natuurlijke personen, rechtspersonen en instellingen een verplichting tot informatieverstrekking opgenomen. Het zesde lid van genoemd artikel 38 voorziet ook in de mogelijkheid dat banken de burgerservicenummers van hun rekeninghouders gebruiken in hun eigen administratie ten behoeve van het voldoen aan de informatieverplichting.

Vierde lid, delegatiebepaling

In het vierde lid van artikel 3:267i is bepaald dat bij of krachtens algemene maatregel van bestuur regels worden gesteld aan het verwijzingsportaal bankgegevens. Het schrijft voor dat in elk geval regels worden gesteld over het beheer van het verwijzingsportaal bankgegevens, over welke identificerende gegevens via het portaal verstrekt kunnen worden, over welke overheidsinstanties zijn aangesloten en de technische eisen waaraan aansluiting moet voldoen. Verder kunnen regels worden gesteld over de vorm waarop vorderingen of verzoeken worden gedaan en de manier waarop de banken en betaaldienstverleners de gegevens via het portaal aanbieden.

Vijfde lid, gebruik burgerservicenummer

Het vijfde lid van het voorgestelde artikel 3:267i voorziet in een wettelijke grondslag voor het gebruik van het burgerservicenummer ten behoeve van het koppelen van een vordering of een verzoek aan de betrokkene in het klantsysteem van de bank of andere betaaldienstverlener. Het burgerservicenummer wordt via het verwijzingsportaal bankgegevens niet aan de vragende instantie verstrekt.

Artikel 87 AVG laat op het punt van de verwerking van een nationaal identificatienummer ruimte om bij lidstatelijk recht specifieke voorwaarden te stellen. In dat kader regelt artikel 46 Uitvoeringwet AVG dat een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, bij de verwerking van persoonsgegevens slechts gebruikt wordt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald. Dit is een kapstokbepaling, waaraan in andere wetten invulling kan worden gegeven. Het burgerservicenummer is geen algemeen persoonsnummer buiten het publieke domein.¹³ Voor de overheid is het gebruik van een uniek persoonsnummer, het burgerservicenummer, geregeld in artikel 10 Wet algemene bepalingen burgerservicenummer (Wabb). Op die grond kunnen de aangesloten overheidsinstanties het burgerservicenummer gebruiken bij het vorderen of opvragen van gegevens uit het verwijzingsportaal bankgegevens.

Echter, voor aangesloten private partijen, die geen beroep kunnen doen op artikel 10 Wabb dient het gebruik te zijn voorgeschreven in sectorale wetgeving, zoals het geval is in artikel 3:267i, derde lid,

¹³ Kamerstukken II 2005/06, 30 312, nr. 3, p. 3.



Wft. Verdere verwerking van het burgerservicenummer voor andere doelen dan omschreven in dit artikellid is op grond daarvan niet toegestaan.

E

In dit onderdeel wordt geregeld dat bij niet-naleving van de verplichting voor banken of andere betaaldienstverleners om aan te sluiten op het verwijzingsportaal bankgegevens, zoals neergelegd in het eerste lid van artikel 3:267i, de toezichthouder – De Nederlandsche Bank – een last onder dwangsom (artikel 1:79 Wft) dan wel een bestuurlijke boete (artikel 1:80 Wft) kan opleggen. Dit gebeurt door artikel 3:267i te plaatsen op de lijsten van de bijlagen bij de Wft.

Deze toelichting wordt ondertekend mede namens de Minister van Justitie en Veiligheid.

De Minister van Financiën,