Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

36 228 Wijziging van de Wet ter voorkoming van witwassen en financieren van terrorisme in verband met het verbod op contante betalingen voor goederen vanaf 3.000 euro en het uitbreiden van de mogelijkheden voor informatie-uitwisseling ten behoeve van de poortwachtersfunctie (Wet plan van aanpak witwassen)

Nr. 4

ADVIES AFDELING ADVISERING RAAD VAN STATE EN NADER RAPPORT[1]

Hieronder zijn opgenomen het advies van de Afdeling advisering van de Raad van State d.d. 13 januari 2021 en het nader rapport d.d. 18 oktober 2022, aangeboden aan de Koning door de Minister van Financiën, mede namens de Minister van Justitie en Veiligheid. Het advies van de Afdeling advisering van de Raad van State is cursief afgedrukt.

Blijkens de mededeling van de Directeur van Uw kabinet van 5 oktober 2020, nr. 2020002033, 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 13 januari 2021, nr. W06.20.0354/III, bied ik U hierbij aan.

De tekst van het advies treft u hieronder aan, voorzien van mijn reactie.

Bij Kabinetsmissive van 5 oktober 2020, no. 2020002033, heeft Uwe Majesteit, op voordracht van de Minister van Financiën, mede namens de Minister van Justitie en Veiligheid, bij de Afdeling advisering van de Raad van State ter overweging aanhangig gemaakt het voorstel van wet tot wijziging van de Wet ter voorkoming van witwassen en financieren van terrorisme en de Wet toezicht trustkantoren 2018 in verband met het verbod op contante betalingen voor goederen vanaf 3.000 euro, het uitbreiden van de mogelijkheden voor informatie-uitwisseling ten behoeve van de poortwachtersfunctie en de aanscherping van de regels voor trustkantoren (Wet plan van aanpak witwassen), met memorie van toelichting.

Het wetsvoorstel vloeit voort uit een plan van aanpak van de regering om witwassen en financiering van terrorisme tegen te gaan. De maatregelen strekken onder andere tot een inperking van contante betaling voor

[1] De oorspronkelijke tekst van het voorstel van wet en van de memorie van toelichting zoals voorgelegd aan de Afdeling advisering van de Raad van State is ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

kst-36228-4
ISSN 0921 - 7371
's-Gravenhage 2022

goederen, verruiming van gegevensdeling tussen instellingen die een poortwachtersfunctie vervullen ter voorkoming van witwassen en financieren van terrorisme en strengere regels voor trustkantoren.

De Afdeling advisering van de Raad van State onderschrijft het doel van het wetsvoorstel om witwassen en financiering van terrorisme te bestrijden. Daarbij spelen banken en andere poortwachters een belangrijke rol om misbruik van het financiële stelsel te voorkomen en ongebruikelijke transacties te melden aan de overheid. Twee van de voorgestelde maatregelen om dit doel beter te realiseren leiden evenwel tot vergaande inbreuken op grondrechten van burgers en bedrijven tot bescherming van vertrouwelijke gegevens en van de persoonlijke levenssfeer. Hoe belangrijk de bestrijding van witwassen en van financiering van terrorisme ook is, bij deze maatregelen is de vraag of het doel de middelen die worden voorgesteld, wel heiligt. Deze middelen gaan in de huidige opzet van het wetsvoorstel te ver. Het gaat daarbij om informatie-uitwisseling bij gezamenlijke monitoring van banktransacties en bij cliëntenonderzoek.

De massale schaal waarop banktransacties gezamenlijk zullen worden gemonitord, is ongekend en betekent een vergaande inbreuk op de vertrouwelijkheid van zakelijke en particuliere cliëntgegevens. Daarbij gaat het niet alleen om een vergaande inbreuk op het recht op privacy, deze monitoring kan ook leiden tot uitsluiting en discriminatie. De noodzaak en proportionaliteit van de gezamenlijke transactiemonitoring is niet aangetoond. Daarbij komt dat de rechtsbescherming in het geding is. Het wetsvoorstel voorziet niet in passende maatregelen ter bescherming van de rechten en vrijheden van burgers en bedrijven maar laat het regelen daarvan over aan de banken. De Afdeling adviseert daarom de grondslag voor de gezamenlijke transactiemonitoring te schrappen en van gezamenlijke transactiemonitoring af te zien.

Ook de voorgestelde gegevensdeling bij de onderzoeksplicht in het kader van het cliëntonderzoek vormt een inbreuk op de bescherming van vertrouwelijke bedrijfs- en persoonsgegevens. De noodzaak en proportionaliteit van deze onderzoeksplicht en gegevensdeling zijn onvoldoende gemotiveerd. De Afdeling adviseert alsnog in een dragende motivering te voorzien.

In verband met deze bezwaren dient het wetsvoorstel nader te worden overwogen.

1. Inleiding

Het wetsvoorstel wijzigt de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) en de Wet toezicht trustkantoren 2018 en bevat de volgende maatregelen:

- *gezamenlijk monitoren van transacties mogelijk maken voor banken (zie punt 3 en 4);*
- *gegevensdeling mogelijk maken tussen instellingen behorend tot dezelfde categorie in het kader van het cliëntenonderzoek bij een hoger risico op witwassen of terrorismefinanciering (zie punt 5);*
- *verduidelijking van het gebruik van bijzondere categorieën persoonsgegevens en persoonsgegevens van strafrechtelijke aard in het kader van verplichtingen op grond van de Wwft;*
- *een verbod voor beroeps- of bedrijfsmatige handelaren in goederen om transacties vanaf € 3.000 in contanten te verrichten, en*
- *een verbod op doorstroomvennootschappen en trustdienstverlening met betrokkenheid van hoog-risicolanden of van landen die op de lijst van non-coöperatieve landen op belastinggebied staan.*

De Afdeling gaat in dit advies in op de gezamenlijke transactiemonitoring en de gegevensdeling tussen instellingen in het kader van het cliëntenonderzoek. De Afdeling schetst hiertoe eerst in punt 2 een breder kader waartegen deze maatregelen vervolgens worden beoordeeld.

2. Uitgangspunten

De Afdeling stelt voorop dat het doel van het wetsvoorstel onomstreden is, namelijk de bestrijding van witwassen en van financiering van terrorisme te verbeteren. Dit doel is niet alleen van belang voor de integriteit van het financiële stelsel, maar ook om allerlei vormen van criminaliteit tegen te gaan. De vraag is echter of de voorgestelde middelen proportioneel zijn in het licht van de doelstellingen van het voorstel.

Meer algemeen beschouwd ziet de Afdeling een risico dat maatregelen ter bescherming van de maatschappelijke orde afbreuk doen aan diezelfde orde door te vergaande beperking van de fundamentele rechten en vrijheden die in het geding zijn. In het geval van de bestrijding van witwassen en de financiering van terrorisme is de vraag gerechtvaardigd of hierin de juiste balans is getroffen.
In het wetsvoorstel valt op dat veel aan marktpartijen wordt overgelaten. Niet alleen de bestrijding van witwassen en de financiering van terrorisme zelf, maar ook de noodzakelijke waarborgen ter bescherming van de grondrechten waarop de bestrijding inbreuk maakt. De overheidsinspanning lijkt zich te beperken tot het creëren van wettelijke grondslagen. Ter waarborging van de inbreuken die op grondrechten worden gemaakt en in het licht van een adequate rechtsbescherming heeft ook de overheid een eigen verantwoordelijkheid om de rechten van burgers en bedrijven te beschermen.

Financiële instellingen zoals banken vervullen een poortwachtersfunctie in het kader van de Wwft. Zij moeten voorkomen dat het betalingssysteem opzettelijk wordt gebruikt voor een ander doel dan waar het voor dient, namelijk witwassen of financiering van terrorisme. Deze instellingen moeten daartoe voortdurend onderzoek doen naar (potentiële en bestaande) cliënten en transacties monitoren. Zij zijn verplicht om ongebruikelijke transacties te melden. Deze verplichtingen vloeien voort uit Europese regelgeving die in Nederland is verwerkt in de Wwft.[2] Het huidige wetsvoorstel is nationaal en additioneel aan de Europese regulering.

De toelichting meldt dat het delen van gegevens wordt gezien als de meest effectieve manier om het gebruik van het financiële stelsel voor witwassen en het financieren van terrorisme te voorkomen. Volgens de toelichting wordt met het voorstel de kennis en capaciteit van instellingen effectiever gebundeld en hun informatiepositie verbeterd, zodat de instellingen hun poortwachtersfunctie adequater kunnen invullen.[3]

Bij de vormgeving van de regelgeving ter bestrijding van witwassen en van financiering van terrorisme dient de proportionaliteit van de voor te stellen middelen uitgangspunt te zijn. Het doel heiligt niet alle middelen, zeker niet als die middelen vergaande inbreuken op grondrechten impliceren. De uitwisseling en verwerking van vertrouwelijke gegevens van cliënten waarmee de voorgestelde uitbreiding van de onderzoeks-

---

[2] 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, PbEU 2015, L 141 (Vierde anti-witwasrichtlijn).
[3] Memorie van toelichting, paragraaf 2.2.

plicht en de gezamenlijke transactiemonitoring gepaard gaan, betekenen een inbreuk op het recht op respect voor het privéleven en op het recht op gegevensbescherming.[4] Een dergelijke inbreuk dient te worden gerechtvaardigd: de inbreuk moet voorzien zijn bij wet, noodzakelijk zijn in een democratische samenleving, en een legitiem doel dienen.[5] De gegevensverwerking dient verder te voldoen aan de Algemene Verordening Gegevensbescherming (AVG).[6]

In dit verband merkt de Afdeling op dat de gevolgen van cliëntenonderzoek en transactiemonitoring voor de cliënt zeer groot zijn als deze wordt uitgesloten van financiële dienstverlening.[7] Adequate rechtsbescherming is daarom van groot belang. Ook kan de meer principiële vraag gesteld worden of het wel aan private partijen overgelaten moet worden om op deze manier cliëntinformatie te gaan delen en onderzoeken.

Tegen het hiervoor geschetste kader roept het wetvoorstel een aantal vragen op vanuit het oogpunt van de gegevensbescherming en privacy van burgers en bedrijven. Over beide maatregelen uit het wetsvoorstel maakt de Afdeling in dat kader de volgende opmerkingen.

2. In de uitgangspunten formuleert de Afdeling reeds enkele principiële kritiekpunten op twee van de maatregelen uit het wetsvoorstel. Alvorens in te gaan op de specifieke adviezen van de Afdeling op onderdelen van de maatregelen, ga ik graag in op deze principiële punten. Naar aanleiding van het kritische advies van de Afdeling is het wetsvoorstel heroverwogen en is uitvoerig onderzocht op welke wijze het beste tegemoet kan worden gekomen aan de adviezen en opmerkingen van de Afdeling. De Afdeling constateert dat het doel van het wetsvoorstel – de bestrijding van witwassen en het financieren van terrorisme – onomstreden is, maar uit tegelijkertijd fundamentele kritiek. Witwassen is een hardnekkig en complex probleem. Het voorkomen en bestrijden van witwassen is van groot belang voor de effectieve preventie en repressie van allerlei vormen van (ondermijnende) criminaliteit. Het verhullen van de criminele herkomst van opbrengsten van misdrijven stelt daders van deze misdrijven in staat om buiten het bereik van onder meer overheidsinstanties te blijven en ongestoord van het vergaarde vermogen te genieten. Ook kunnen deze illegale inkomsten worden gebruikt voor de financiering van dezelfde of nieuwe criminele activiteiten. Het opgebouwde vermogen biedt hen tevens de mogelijkheid om posities te verwerven in bonafide ondernemingen en in sommige gevallen het gezag van de overheid te ondermijnen. Bovendien wordt de integriteit van het financieel-economisch stelsel aangetast door mensen die criminele verdiensten proberen te verhullen. Het is daarom cruciaal dat de legale financiële kanalen waarlangs het witwasproces zich kan voltrekken worden beschermd tegen gebruik voor criminele doeleinden. Tegelijkertijd hanteren criminelen steeds complexere methoden om buiten het zicht van de poortwachters en opsporingsinstanties te blijven, juist door gebruik te maken van de zwakheden van het systeem.

---

[4] Artikel 8 EVRM, artikel 7 en 8 Handvest EU.

[5] Artikel 8, tweede lid, EVRM; artikel 7, 8 en 52, eerste lid, Handvest EU en artikel 6, eerste lid onder c, en derde lid, AVG. Zie ook memorie van toelichting, paragraaf 3.1, A.

[6] De AVG is onverkort van toepassing op maatregelen ter bestrijding van witwassen en van financiering van terrorisme (zie overweging 42, artikel 41 en 43 Richtlijn 2015/849/EU) en bijvoorbeeld ook op betalingsdiensten (zie artikel 94 Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, PbEU 2015, L 337 (PSD 2).

[7] Ook de Autoriteit Persoonsgegevens (AP) wijst hierop in haar consultatiereactie.

Poortwachters dienen, ieder afzonderlijk, per cliënt een individuele risicobeoordeling te maken en zelfstandig de transacties van de cliënt doorlopend te monitoren. Zij kunnen hierbij slechts gebruik maken van de informatie die zij zelf verzameld hebben. Dit zorgt er voor dat de instellingen hun poortwachtersrol moeten uitvoeren op basis van beperkte informatie, waardoor het enerzijds moeilijker is om een goede risicogebaseerde beoordeling te maken en, anderzijds, arbeidsintensiever is. Criminelen maken hier gebruik van door doelbewust hun activiteiten te spreiden over veel verschillende instellingen of van instelling te wisselen, om zodoende de informatiepositie van elke individuele poortwachter zo beperkt mogelijk te maken.

Met de twee maatregelen waar de Afdeling in haar advies op ingaat, wordt beoogd specifieke informatiedeling tussen poortwachters mogelijk te maken om de aanpak van witwassen en terrorismefinanciering te versterken. Ik ben mij terdege bewust van de spanning die een doelstelling als deze oplevert ten opzichte van gegevensbescherming. Blijkens het advies van de Afdeling is de gegevensbescherming onvoldoende in het wetsvoorstel teruggekomen. De Afdeling merkt op dat het wetsvoorstel veel aan marktpartijen overlaat, maar dat de overheid ook een eigen verantwoordelijkheid heeft om passende waarborgen te treffen voor de inbreuken op rechten van burgers. De Afdeling wijst hierbij specifiek op het recht op respect voor het privéleven, het recht op gegevensbescherming en adequate rechtsbescherming.

Het uitgangspunt van het wetsvoorstel was dat in Nederland reeds een uitgebreid kader geldt dat waarborgen verplicht bij gegevensdeling, te weten de Algemene Verordening Gegevensbescherming (AVG) en de uitvoeringswet AVG (UAVG), die onverkort van toepassing zijn op alle vormen van verwerking van persoonsgegevens en daarbij al veel verplichtingen en waarborgen voorschrijven. Daarnaast is uitbesteding door banken reeds met waarborgen omkleed middels hoofdstuk 5 van het Besluit prudentiële regels, waarin waarborgen ten aanzien van de controle van de uitbestedende partij, gegevensuitwisseling en het toezicht worden gesteld. Gelet op het belang van een adequate bescherming van persoonsgegevens heb ik, naar aanleiding van het advies van de Afdeling, gezocht naar manieren om de grondslagen voor gegevensdeling preciezer te omschrijven en aanvullende waarborgen op te nemen. Dit heeft geleid tot een substantiële herziening van het wetsvoorstel. Hiertoe is de hoeveelheid gegevens die gedeeld mag worden maximaal ingeperkt, tot aan de grens dat de effectiviteit van het gezamenlijk monitoren van transacties fundamenteel ondergraven zou worden. Daartoe is de reikwijdte van de te verwerken gegevens ingeperkt en zijn de afzonderlijke categorieën gegevens die verwerkt mogen worden voorgeschreven. Daarnaast zijn er aanvullende waarborgen wat betreft de verwerking opgenomen in het gewijzigde wetsvoorstel, zoals de wijze van verwerking en beveiliging van de gegevens. Voor de uitwisseling van gegevens in het kader van cliëntenonderzoek zijn de voorwaarden voor uitwisseling en de uit te wisselen informatie nader aangescherpt. Hieronder zal ik, in reactie op de opmerkingen van de Afdeling, per maatregel nader ingaan op de aanpassing van de maatregelen.

3. Gezamenlijke transactiemonitoring banken: wettelijke grondslag

a. Gezamenlijke transactiemonitoring

Het wetsvoorstel creëert de mogelijkheid voor banken om transactiegegevens samen te brengen in een gezamenlijke database en deze gegevens vervolgens onderling te delen voor de bestrijding van witwassen en van

de financiering van terrorisme.[8] Volgens de toelichting wil een vijftal banken deze gezamenlijke voorziening opzetten. Daarbij worden bijna 10 miljard transacties per jaar bij 35 miljoen cliënten gemonitord.[9] Het voorstel neemt twee wettelijke belemmeringen weg door zowel het delen van transacties als de uitbesteding van de monitoring toe te staan.[10]

Gegevens die kunnen worden gedeeld, betreffen vertrouwelijke gegevens van particuliere en zakelijke cliënten. Hieronder vallen ook persoonsgegevens, waaronder het BSN.[11] De verwerking van persoonsgegevens wordt beëindigd indien deze niet langer noodzakelijk is voor het melden van ongebruikelijke transacties.[12] Daarbij geldt een bewaartermijn van vijf jaar.[13] Ook is geregeld dat instellingen die een gezamenlijke voorziening opzetten, jaarlijks een verslag uitbrengen over de naleving van de Wwft, de effectiviteit van de voorziening en over het filteren van onterecht als risico aangemerkte informatie.[14] Tot slot is bepaald dat een onafhankelijke audit moet worden verricht naar de vraag of voldaan wordt aan de eisen voor uitbesteding en gegevensbescherming.[15]

Een gezamenlijke voorziening waarvoor de wettelijke basis nu wordt voorgesteld, is al in 2019 aangekondigd en momenteel in voorbereiding.[16] Het gaat om Transactie Monitoring Nederland (TMNL), een samenwerkingsverband tussen ABN AMRO, ING, Rabobank, Triodos en de Volksbank. Door het grote gezamenlijke marktaandeel van de deelnemende banken zullen er vertrouwelijke gegevens worden opgeslagen, geanalyseerd en bewerkt van vrijwel alle Nederlandse burgers en bedrijven. Onder deze gegevens zullen ook bijzondere persoonsgegevens zijn, zoals (betaling van) medische facturen en strafrechtelijke boetes, lidmaatschap van politieke partijen en vakbonden en bezoek aan seksclubs, casino's en coffeeshops.[17]

De schaal waarop wordt voorgenomen om dit te organiseren is tot op heden ongekend in Nederland. De voorgenomen monitoring betekent een vergaande inbreuk op de vertrouwelijkheid van zakelijke en particuliere cliëntgegevens. In het bijzonder is het recht op bescherming van persoonsgegevens en van het recht op privacy in bredere zin op fundamentele wijze aan de orde.[18] Daarnaast zijn andere fundamentele belangen in het geding, zoals rechtsbescherming.[19] Ook de regering onderkent dat deze vorm van uitbesteding en gegevensdeling «bijzonder gevoelig» is.[20]

---

[8] Voorgesteld artikel 34b Wwft.

[9] Memorie van toelichting, paragraaf 2.2.2.

[10] Memorie van toelichting, paragraaf 2.2.2.

[11] Voorgesteld artikel 34b, derde lid.

[12] Voorgesteld artikel 34b, vierde lid.

[13] Artikel 33, derde lid, van de Wwft.

[14] Voorgesteld artikel 34b, vijfde lid.

[15] Voorgesteld artikel 34b, vijfde lid, sub b.

[16] *«Nederlandse banken bundelen krachten tegen witwassen», persbericht NVB, 13 september 2019.*

[17] Ook is het denkbaar dat uit de transactiemonitoring van transacties die op zichzelf geen bijzondere persoonsgegevens bevatten wel bijzondere persoonsgegevens kunnen worden afgeleid. Dit was anders in de zaak EHRM 22 december 2015, ECLI:CE:ECHR:2015:1222JUD002860111 (G.S.B./Zwitserland), ro. 93, waarin de gegevensuitwisseling enkel bankgegevens, oftewel uitsluitend financiële informatie, betrof die geen intieme details of gegevens gerelateerd aan de klagers identiteit onthulde die meer bescherming genieten.

[18] Artikel 8 EVRM, artikel 7 en 8 Handvest EU, artikel 10 Grondwet.

[19] Afdeling advisering van de Raad van State, Ongevraagd advies over de effecten van de digitalisering voor de rechtsstatelijke verhoudingen, 2018, Kamerstukken II 2017/18, 26 643, nr. 557. Zie ook bijv. S. Kulk & S. van Deursen, Juridische aspecten van algoritmen die besluiten nemen. Een verkennend onderzoek, Den Haag: WODC 2020.

[20] Memorie van toelichting, artikelsgewijze toelichting op artikel 34b.

3a. De Afdeling merkt op dat de schaal van de gezamenlijke transactiemonitoring tot op heden ongekend is en een verregaande inbreuk betekent op de privacy. In reactie hierop wil ik opmerken dat transactiegegevens op dit moment reeds verwerkt worden, zij het door de banken afzonderlijk. Ten eerste is de verwerking van de transactiegegevens inherent aan het faciliteren van het betalingsverkeer. Ten tweede zijn banken, en andere financiële instellingen, reeds verplicht om een voortdurende controle uit te voeren op cliënten en hun transacties teneinde te voorkomen dat het financiële stelsel wordt misbruikt om wit te wassen of terrorisme te financieren. Deze verplichting bestaat reeds geruime tijd en is een van de internationaal en Europees erkende[21] pijlers van het beleid ter voorkoming van het gebruik van het financiële stelsel voor witwassen en het financieren van terrorisme. Dit voorstel beoogt enkel mogelijk te maken om, onder voorwaarden, gezamenlijk transacties te monitoren.

b. Noodzaak en proportionaliteit

De publiekrechtelijke grondslag die het voorstel creëert voor een dergelijke massale en vergaande gegevensverwerking, met inbegrip van profilering, dient te worden getoetst aan het recht op respect voor het privéleven en het recht op gegevensbescherming.[22] Buiten kijf staat dat de gezamenlijke transactiemonitoring een vergaande inbreuk is op het privéleven. Transacties zijn immers persoonsgegevens die een gedetailleerd inzicht geven in het leven van de betrokkene, overigens ongeacht of dit bijzondere persoonsgegevens zijn.[23] De Afdeling wijst erop dat dit eveneens geldt voor zakelijke gegevens.[24] Voor de beoordeling is voorts van belang dat het gaat om een bundeling van persoonsgegevens van bijna alle Nederlanders.

3b. De Afdeling gaat in op de noodzaak en proportionaliteit van het voorstel voor een grondslag voor gezamenlijke transactiemonitoring. Zij maakt daarbij opmerkingen van uiteenlopende aard, die zien op verschillende elementen van het gehele stelsel ter voorkoming van het gebruik van het financiële stelsel voor witwassen en het financieren van terrorisme in Nederland.

Een dergelijk vergaande inbreuk dient te worden gerechtvaardigd aan de hand van de vraag of deze maatregel noodzakelijk en proportioneel is.[25] De memorie van toelichting laat de afweging of gezamenlijke monitoring noodzakelijk is over aan de banken «aangezien zij hun cliëntenbestand het beste kennen».[26] Over de proportionaliteit wordt slechts gemeld dat de monitoring beperkt is tot Nederlandse banken en in Nederland gevestigde bijkantoren van buitenlandse banken.[27]

---

[21] «International standards on combating money laundering and the financing of terrorism & proliferation», The FATF Recommendations, maart 2022 (update) en Richtlijn (EU) 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.

[22] Artikel 8, tweede lid, EVRM, artikel 7 en 8 Handvest EU, artikel 10 Grondwet.

[23] Zie EHRM 4 december 2008, ECLI:CE:ECHR:2008:1204JUD003056204 (S. en Marper/Verenigd Koninkrijk), ro. 66–67, en EHRM 7 juli 2015, ECLI:CE:ECHR:2015:0707JUD002800512 (M.N. e.a./San Marino), ro. 51; EHRM 16 februari 2000 (GK), ECLI:CE:ECHR:2000:0216JUD002779895 (Amann/Zwitserland), ro. 70.

[24] *Zie EHRM 16 december 1992 (GK), ECLI:CE:ECHR:1992:1216JUD001371088 (Niemietz/Duitsland), ro. 29–31, EHRM 7 juli 2015, ECLI:CE:ECHR:2015:0707JUD002800512 (M.N. e.a./San Marino), ro. 51, en EHRM 16 februari 2000 (GK), ECLI:CE:ECHR:2000:0216JUD002779895 (Amann/Zwitserland), ro. 65.*

[25] Artikel 8, tweede lid, EVRM, artikel 52, eerste lid, Handvest EU, en artikel 6, derde lid, AVG.

[26] Memorie van toelichting, paragraaf 3.2.

[27] Memorie van toelichting, paragraaf 3.2.

De Afdeling merkt op dat de regering geen eigen afweging maakt of er een noodzaak bestaat tot gezamenlijke transactiemonitoring maar dit oordeel overlaat aan de banken. Daarmee wordt ook de waarborging van de fundamentele rechten die hier in het geding zijn, uitbesteed aan diezelfde banken. De Afdeling wijst erop dat dit de overheid niet ontslaat van de verplichting zelfstandig af te wegen of het creëren van de mogelijkheid van een dergelijke voorziening niet alleen gewenst maar ook noodzakelijk is gelet op de fundamentele rechten die in het geding zijn. Dat banken zelf kunnen afwegen of zij van een voorziening gebruik maken, doet daar niet aan af.

In de toelichting op het wetsvoorstel is aangegeven dat de noodzaak van het gezamenlijke monitoren van transacties voortkomt uit het gegeven dat de huidige verplichting voor banken om individueel transacties te monitoren ertoe leidt dat banken slechts beperkte informatie hebben om vast te stellen dat een transactie ongebruikelijk is. Dit is met name beperkend als het gaat om transacties die via verschillende cliënten en banken lopen. Criminelen maken gebruik van deze beperking door complexe netwerken van transacties in te richten, waarbij crimineel geld via een scala van transacties en verschillende banken wordt geleid. Doordat banken zich bij het individueel monitoren van transacties beperken tot de transacties die via hun bank gelopen zijn, kan de ongebruikelijkheid van transacties die via een groot netwerk lopen, onder de radar blijven. Het creëren van een grondslag om, binnen bepaalde voorwaarden middels een gezamenlijke voorziening, gezamenlijk transacties te monitoren is daarvoor noodzakelijk. De toelichting is nader aangevuld op dit punt. Daarnaast is het wetsvoorstel aangepast zodat deze grondslag na vier jaar wordt geëvalueerd. In deze evaluatie zullen zowel de effectiviteit van het gezamenlijk monitoren van transacties, als de bescherming van persoonsgegevens worden betrokken. De evaluatie zal uitgevoerd worden door een onafhankelijke partij. Publieke partijen met een voor de evaluatie relevante taak, zoals De Nederlandsche Bank (DNB) en de FIU-Nederland, zullen nauw betrokken zijn bij deze evaluatie. Het klopt dat de grondslag de afweging om deel te nemen aan een gezamenlijke voorziening aan banken laat. De specifieke dienstverlening die een bank aanbiedt is essentieel voor de afweging of deelname aan een voorziening noodzakelijk is om te voldoen aan de wettelijke verplichting om doorlopend transacties te monitoren.

Daarnaast merkt de Afdeling op dat de gezamenlijke transactiemonitoring leidt tot het verwerken van de gegevens van alle cliënten, ook van cliënten zonder ongebruikelijke transacties. Deze ongedifferentieerde verzameling en verwerking gaat de grenzen van het strikt noodzakelijke te buiten,[28] de maatregel is daarmee niet proportioneel.[29]

Allereerst verwijs ik naar de toelichting hierboven. Het is niet mogelijk om op voorhand een schifting te maken van transacties die (mogelijk) nodig zijn om ongebruikelijke transactiepatronen te identificeren, aangezien die patronen worden gevormd door op het eerste gezicht gebruikelijke transacties. Het is dus op voorhand niet duidelijk welke transacties (mogelijk) onderdeel zijn van een ongebruikelijk transactiepatroon.

---

[28] Vergelijk in deze zin HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238 (Digital Rights Ireland), punt 52.

[29] Vergelijk in deze zin HvJ EU 6 oktober 2020,C-623/17, ECLI:EU:C:2020:790 (Privacy International), punt 80, HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238 (Digital Rights Ireland), punt 58.

Naar aanleiding van de opmerkingen van de Afdeling is onderzocht op welke wijze de verwerking van gegevens beperkt zou kunnen worden en is het wetsvoorstel aangepast. Het uitgangspunt hierbij was om zo min mogelijk persoonsgegevens door de gezamenlijke voorziening te laten verwerken, zonder fundamenteel afbreuk te doen aan de effectiviteit van de gezamenlijke transactiemonitoring. Bepaald is nu in het wetsvoorstel dat de transactiegegevens van particulieren – dus niet-zakelijke transacties – voor transacties onder de € 100 niet in de gezamenlijke voorziening verwerkt mogen worden. Daarnaast is voorzien dat bij zakelijke transacties met een particuliere tegenrekening voor bedragen onder de € 100 slechts de volgende gegevens van de particulier mogen worden verwerkt: het IBAN-nummer (het rekeningnummer), het BIC-nummer (de bank identificatie code) en de landencode. Deze beperkte set gegevens is vereist om mogelijk relevante transactiepatronen vanaf een zakelijke rekening te kunnen herkennen. De schatting van de Nederlandse Vereniging van Banken op basis van een inventarisatie bij de bij TMNL betrokken banken is dat hiermee 60–70% van de transactiegegevens van particuliere cliënten en ongeveer 5% van alle transacties niet in de gezamenlijke voorziening zal worden verwerkt. Daarmee is een aanzienlijke inperking gerealiseerd van de hoeveelheid verwerkte persoonsgegevens in de gezamenlijke voorziening.

Het is daarbij de vraag of banken als poortwachters de reeds bestaande (wettelijke) mogelijkheden wel ten volle hebben benut om te voldoen aan de wettelijke onderzoeks- en meldplicht. Banken hebben de laatste jaren een noodzakelijke inhaalslag gemaakt en geïnvesteerd in personeel en technologie. Tegelijk tonen de signalen uit het DNB-toezicht en de opsporing aan dat er ruimte is voor verbetering in de monitoring en melding van ongebruikelijke transacties. DNB constateerde begin 2020 onder andere verouderde ICT, databeheer dat niet op orde is en onvoldoende (gekwalificeerd) personeel.[30]

De Afdeling stelt dat het de vraag is of banken hun mogelijkheden wel ten volle hebben benut om te voldoen aan hun wettelijke verplichtingen. Zoals hierboven toegelicht, is de inherente beperking van de huidige wettelijke verplichting om individueel transacties te monitoren, dat de ongebruikelijkheid van transacties die via een groot netwerk lopen, onder de radar blijven en dat criminelen hier gebruik van maken door ingewikkelde constructies op te zetten. Het creëren van een grondslag om, binnen bepaalde voorwaarden middels een gezamenlijke voorziening, gezamenlijk transacties te monitoren is noodzakelijk om dit probleem aan te pakken.

De noodzaak tot gezamenlijke monitoring moet ook worden bekeken in het licht van de al zeer uitgebreide en fijnmazige Europese wetgeving. Nog maar recent zijn het UBO-register[31] en het bankenportaal[32] in werking getreden. De praktische implementatie van deze instrumenten is nog niet voltooid, en evenmin is bekend wat de effecten ervan zijn. Het is

---

[30] «DNB: databeheer van banken nog te vaak niet op orde», in: FD, 22 januari 2020. Zie uitgebreider: DNB, Veranderen voor vertrouwen. Lenen, sparen en betalen in het datatijdperk, 2020.

[31] Op 27 september 2020 trad het UBO-register in werking en zijn ondernemingen verplicht om hun eigenaren of de personen die zeggenschap hebben, via de Kamer van Koophandel, in het UBO-register in te schrijven. De inschrijving voor bestaande organisaties moet plaatsvinden voor 27 maart 2022.

[32] Op 10 september 2020 trad de Wet verwijzingsportaal bankgegevens in werking. Het verwijzingsportaal bankgegevens is een digitale voorziening voor de geautomatiseerde verstrekking van identificerende gegevens die opgevraagd worden door de daartoe bevoegde opsporingsdiensten en de Belastingdienst.

in dat licht bezien op zijn minst voorbarig om, bovenop de al bestaande Europese verplichtingen, een zodanig vergaande maatregel te introduceren.

Ik wil hierbij opmerken dat de genoemde maatregelen een ander doel hebben dan gezamenlijke transactiemonitoring. Het verwijzingsportaal bankgegevens heeft tot doel een geautomatiseerde verstrekking van identificerende gegevens die worden opgevraagd bij banken en andere betaaldienstverleners door de daartoe bevoegde opsporingsdiensten en de Belastingdienst. Het UBO-register heeft als doel om de uiteindelijke belanghebbenden van juridische entiteiten transparant en inzichtelijk te maken middels een openbaar toegankelijk register. Met gezamenlijke transactiemonitoring wordt, zoals hierboven aangegeven, beoogd om banken in staat te stellen ongebruikelijke transactiepatronen in beeld te krijgen, die ze individueel niet kunnen identificeren. Hoewel alle drie de maatregelen de aanpak van witwassen en terrorismefinanciering beogen te verbeteren, zien ze op verschillende aspecten van deze aanpak. Ze zijn zodoende niet onderling inwisselbaar.

Tot slot moet de noodzaak ook bezien worden in het licht van de te verwachten effectiviteit. Aan de kant van potentiële witwassers zal het betrekkelijk eenvoudig zijn de gezamenlijke voorziening te omzeilen door gebruik te maken van niet-deelnemende banken in Nederland of daarbuiten. Aan de kant van de banken wordt aanzienlijk geïnvesteerd. Dit stelt echter ook eisen aan de rest van de «anti-witwas-keten». Dan gaat het onder andere om FIU Nederland (de instantie waar alle meldingen samenkomen), de opsporingsdiensten en de inlichtingendiensten. FIU Nederland kampt nu reeds met een tekort aan capaciteit (zowel personeel en financieel als technologisch) om de stroom meldingen te verwerken.[33]

Ik wil drie kanttekeningen maken bij deze opmerking van de Afdeling. Ten eerste is het achterliggende doel van het monitoren van transacties tweeledig. Het heeft zowel een rol in het voorkomen als het bestrijden van witwassen en terrorismefinanciering. De FIU-Nederland analyseert meldingen van ongebruikelijke transacties. De door de FIU-Nederland verdacht verklaarde transacties kunnen vervolgens, naast andere informatiebronnen, worden gebruikt door opsporingsdiensten in het kader van het opsporen en vervolgen van de bestrijding van witwassers, potentiële daders van onderliggende delicten en diegenen die terrorisme mogelijk trachten te financieren. Banken monitoren transacties echter ook om hen in staat te stellen aan hun taak als poortwachters van het financiële stelsel te voldoen en het gebruik van het financiële stelsel voor witwassen of financiering van terrorisme te voorkomen. Indien het monitoren van transacties effectiever kan worden vormgegeven, geeft dat banken ook de mogelijkheid om hun poortwachtersfunctie beter in te vullen. Uiteraard zullen, zoals de Afdeling opmerkt, potentiële witwassers trachten deze maatregelen te omzeilen. Dit doet niet af aan de noodzaak om de poortwachtersfunctie te versterken en daarmee het Nederlandse financiële stelsel weerbaarder te maken. Ten tweede wil ik erop wijzen dat gezamenlijke transactiemonitoring niet tot doel heeft dat het aantal meldingen van ongebruikelijke transacties wordt verhoogd en hier ook niet per se toe hoeft te leiden. Doordat gezamenlijke transactiemonitoring banken in staat stelt om transacties gezamenlijk te analyseren, zouden er meer vals-positieven kunnen worden uitgesloten en de kwaliteit van de meldingen omhoog kunnen gaan. De FIU-Nederland en TMNL hebben in 2021 binnen de Fintell Alliance een pilot gedaan om ondergrondse banknetwerken te identificeren. De FIU-Nederland en de NVB geven

[33] Investico, Tachtig procent van Nederlandse witwasmeldingen verdwijnt in de la, 23 september 2020.

hierbij aan dat bijna 95% van deze circa 275 alerts onderzoekswaardig bleek te zijn. Ten slotte heeft de regering recent bekendgemaakt de capaciteit van de FIU-Nederland uit te breiden.[34]

Uit het voorgaande blijkt dat de noodzaak en proportionaliteit van de vergaande inbreuk op de gegevensbescherming van burgers en bedrijven en op de privacy die hiervan het gevolg zal zijn, niet aangetoond zijn. De Afdeling adviseert de voorgestelde grondslag voor gezamenlijke monitoring van banktransacties daarom te schrappen.

Zoals hierboven is uiteengezet is het mogelijk maken van gezamenlijke transactiemonitoring een noodzakelijke maatregel voor het verder versterken van het Nederlandse financiële systeem door de banken. De huidige verplichting voor banken om individueel transacties te monitoren leidt ertoe dat banken slechts beperkte informatie hebben om vast te stellen dat een transactie ongebruikelijk is. Bovendien blijkt uit de praktijk dat gezamenlijke transactiemonitoring tot veelbelovende resultaten leidt. Daarnaast is uiteengezet dat het niet mogelijk is om deze gezamenlijke monitoring zodanig in te richten dat alleen hoog risico transacties worden gedeeld, maar is het wetsvoorstel wel gewijzigd om de verwerking van gegevens in te perken en volgens de aanwijzingen van de Afdeling proportioneel in te richten. Op basis hiervan is de noodzaak en proportionaliteit van de voorstellen aangetoond en is tegelijkertijd gehoor gegeven aan de kritiek van de Afdeling.

Onverminderd het advies om de grondslag voor gezamenlijke transactiemonitoring te schrappen, adviseert de Afdeling, indien de regering toch vasthoudt aan dit onderdeel van het wetsvoorstel, in ieder geval met de volgende aspecten rekening te houden.

4. Gezamenlijke transactiemonitoring: overige aspecten

a. Automatische besluitvorming en rechtsbescherming

Volledig geautomatiseerde besluitvorming (inclusief profilering), zonder menselijke tussenkomst, is in beginsel niet toegestaan.[35] Deze is wel mogelijk als dit is toegestaan op grond van nationaal recht. Daarbij dient te worden voorzien in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkenen.[36] De toelichting gaat in op een aantal waarborgen, maar laat het regelen daarvan over aan de banken.[37]

De Afdeling wijst erop dat de hoeveelheid informatie die in de gezamenlijke transactiemonitoring wordt verwerkt, dusdanig groot is, dat de monitoring in de praktijk alleen geautomatiseerd mogelijk zal zijn. De hierop gebaseerde besluitvorming door banken kan voor individuele cliënten (zakelijk of particulier) verstrekkende gevolgen hebben. Als zij op basis van een «alert» uiteindelijk geen toegang tot het reguliere bankwezen hebben (of op een zwarte lijst komen), kunnen zij feitelijk niet

---

[34] Kamerstukken II 2021/22, 29 911, nr. 358.

[35] Artikel 22, eerste lid, AVG.

[36] Artikel 22, tweede lid, onder b, AVG.

[37] Zo zal een bank een gegevensbeschermingseffectbeoordeling moeten uitvoeren, en zo nodig de AP raadplegen. Ook moet de bank ingaan op de maatregelen die worden genomen om de rechten van betrokkenen te waarborgen. De alerts die voortkomen uit de gezamenlijke voorziening moeten daarnaast door menselijke tussenkomst worden onderzocht. Tot slot moet de bank zijn cliënten informeren over de verwerking van de persoonsgegevens. Daarnaast bevat het voorstel een grondslag om bij of krachtens amvb regels te stellen met betrekking tot de uitoefening van de rechten van betrokkenen.

deelnemen aan het maatschappelijk verkeer (werken, zaken doen, belasting betalen).

Deze gevolgen klemmen temeer, als op basis van ongebruikelijke transactiepatronen (profilering) bepaalde categorieën cliënten onterecht worden uitgesloten. Dit creëert, naast de inbreuk van de transactiemonitoring op het recht op privéleven en het recht op gegevensbescherming, ook risico's op stigmatisering of zelfs discriminatie.[38] Zorgvuldige en goed gemotiveerde besluitvorming door de banken is daarom cruciaal. Daarbij moet helder zijn op basis van welke data en beslisregels een besluit is genomen; of deze data juist en volledig zijn en gewijzigd kunnen worden; en hoe het uiteindelijke besluit precies wordt gemotiveerd.

De Afdeling wijst erop dat blijkens de toelichting wordt beoogd dat de alerts die voortkomen uit de gezamenlijke transactiemonitoring wel door menselijke tussenkomst moeten worden onderzocht. Deze menselijke tussenkomst dient betekenisvol te zijn.[39] Op voorhand is niet duidelijk hoe betekenisvolle tussenkomst wordt gegarandeerd, nu het juist de geautomatiseerde transactiemonitoring is die ongebruikelijke transacties in kaart zal brengen en het bovendien gaat om zeer grote hoeveelheden gegevens. Het is niet ondenkbaar dat aan de alerts of signalen die hieruit voortkomen veel gewicht wordt toegekend.

Het wetsvoorstel bevat weinig waarborgen voor betekenisvolle menselijke tussenkomst en ter voorkoming van uitsluiting en discriminatie. In het bijzonder bij geautomatiseerde besluitvorming is het noodzakelijk dat in het wetsvoorstel zelf waarborgen worden opgenomen ter bescherming van de rechten en vrijheden van cliënten. Dit is ook vereist als bijzondere en strafrechtelijke gegevens worden verwerkt.[40] Het volstaat dan ook niet in de toelichting slechts te wijzen op de afweging die de individuele banken zelf moeten maken.[41]

Bovendien zijn zinvolle mogelijkheden om in verzet te komen tegen een besluit van een bank, waaronder een besluit tot plaatsing op een «zwarte lijst», onmisbaar in het kader van een effectieve rechtsbescherming. De toelichting gaat echter niet in op de uitoefening van de rechten van betrokkenen in relatie tot de gezamenlijke voorziening (TMNL). Blijkens de toelichting zijn de banken verwerkingsverantwoordelijke jegens wie betrokkenen hun rechten kunnen uitoefenen.

De Afdeling acht dat onvoldoende. Zij benadrukt dat voorkomen moet worden dat verantwoordelijkheid voor de uiteindelijke beslissing in de praktijk verschuift tussen de verschillende instellingen en TMNL. Van belang is daarom dat de bank onder meer de betrokkene informeert, en deze ook kan informeren over de onderliggende logica als sprake is van geautomatiseerde besluitvorming.[42] Ook zal de betrokkene zijn overige rechten op een effectieve wijze jegens de bank moeten kunnen uitoefenen.

Gelet op het belang van de rechtspositie en de daarmee samenhangende rechtsbescherming van de betrokkene acht de Afdeling het daarom in elk geval gewenst in het voorstel subdelegatie uit te sluiten voor onderwerpen die hieraan raken, zoals de uitoefening van de rechten van

---

[38] Vergelijk hier Rechtbank Den Haag, 5 februari 2020, ECLI:NL:RBDHA:2020:865 (SyRI).
[39] Vergelijk WP29, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p. 21.
[40] Artikel 9, tweede lid, onder g, en artikel 10 AVG.
[41] Memorie van toelichting, paragraaf 3.2.
[42] Artikel 13, 14 en 15 AVG.

betrokkenen.[43] Op ten minste het niveau van een algemene maatregel van bestuur (amvb) dient de regering helder te maken hoe de burger op effectieve wijze in zijn rechten wordt beschermd.

Gelet op het voorgaande dient het wetsvoorstel te worden aangepast. De Afdeling adviseert in het wetsvoorstel de nodige waarborgen op te nemen met betrekking tot de gegevensverwerking, de geautomatiseerde besluitvorming en de rechtsbescherming, en subdelegatie ten aanzien van onderwerpen die de rechtsbescherming raken uit te sluiten.

4a. De Afdeling merkt op dat de grondslag voor gezamenlijke transactiemonitoring ook een grondslag biedt voor profilering en er sprake is van geautomatiseerde besluitvorming. Dit is niet het geval en ook nooit beoogd met dit wetsvoorstel. Dit is verduidelijkt in het wetsvoorstel en de toelichting door met een verwijzing naar artikel 22, eerste lid, van de AVG, besluitvorming uitsluitend op basis van geautomatiseerde verwerking, waaronder profilering, binnen de gezamenlijk voorziening expliciet te verbieden. Daarnaast is het wetsvoorstel aangepast en zijn de mogelijkheden voor banken om taken aan de gezamenlijke voorziening uit te besteden op basis van artikel 10 van de wet ingeperkt. De mogelijkheid om het melden van ongebruikelijke transacties[44] uit te besteden is komen te vervallen. Banken kunnen derhalve alleen de voortdurende controle van transacties aan de gezamenlijke voorziening uitbesteden. Indien binnen de gezamenlijke voorziening wordt vastgesteld dat een transactie kenmerken vertoont van een ongebruikelijke transactie, ontvangt de aangesloten bank een *alert* dat de transactie mogelijk ongebruikelijk is. De deelnemende bank dient zodoende telkens een zelfstandige afweging te maken op basis van de alert van de gezamenlijke voorziening en het uitsluitend bij de individuele bank aanwezige nadere informatie over de cliënt, of er een melding gedaan moet worden bij de FIU-Nederland van een ongebruikelijke transactie en of de bank mitigerende maatregelen dient te treffen ten aanzien van de cliënt.

Naar aanleiding van de opmerkingen van de Afdeling zijn daarnaast aanvullende voorwaarden voor de verwerking binnen de gezamenlijke voorziening in het wetsvoorstel opgenomen. Ten eerste dienen alle persoonsgegevens binnen de gezamenlijke voorziening gepseudonimiseerd en versleuteld te worden, zodat binnen de gezamenlijke voorziening de transacties niet gekoppeld kunnen worden aan (rechts)personen en deze alleen bij de individuele bank bekend zijn. Daarnaast worden in het wetsvoorstel waarborgen voorgeschreven ten aanzien van geautomatiseerde analyse van persoonsgegevens: deze mag alleen plaatsvinden middels algoritmes waarvan de uitkomsten navolgbaar en controleerbaar zijn en waarvan de verwerking wordt vastgelegd. Voorts merkt de Afdeling op dat een alert kan leiden tot plaatsing op een zwarte lijst met uitsluiting tot het gevolg. Hoewel dit inderdaad een mogelijkheid is, is dit tegelijkertijd een uiterste consequentie waarbij de hierboven beschreven tussenstappen plaats dienen te vinden. Op dit moment kan een financiële instelling naar aanleiding van geconstateerde fraude of onacceptabele risico's op witwassen of terrorismefinanciering besluiten de zakelijke relatie met de cliënt te beëindigen, dit volgt uit de wet, en kan een instelling besluiten dit te registeren in een centraal systeem. Voor gevallen van fraude bestaat op dit moment een zwarte lijst, daarnaast creëert dit wetsvoorstel de grondslag om een zwarte lijst in te richten bij aantoonbare risico's op witwassen of het financieren van terrorisme.

---

[43] Voorgesteld artikel 34a, vijfde lid. Zie ook het advies van de Afdeling advisering van de Raad van State van 26 maart 2020, W13.19.0425/III, Kamerstukken II 2019/20, 35 515, nr. 4, paragraaf 8.

[44] Artikel 16 Wwft.

Onder punt 5b ga ik daar nader op in, alsmede de daarbij verplichte waarborgen.

De Afdeling wijst voorts op het belang van regels ten behoeve van de rechtsbescherming van betrokkene. Het wetsvoorstel kende reeds een grondslag om bij of krachtens algemene maatregel van bestuur nadere regels te stellen op dit punt in het voorgestelde 34a, vijfde lid. De Afdeling merkt daarbij dat, gelet op het belang van de effectieve rechtsbescherming van burgers, subdelegatie ongewenst is. In het gewijzigde wetsvoorstel wordt subdelegatie daarom uitgesloten. Hieronder ga ik verder in op de verdeling van verantwoordelijkheden tussen de gezamenlijke voorziening en de deelnemende banken.

b. Verdeling verantwoordelijkheden

De gezamenlijke voorziening TMNL gaat voor de banken hun betalingstransacties in samenhang monitoren op signalen die kunnen duiden op witwassen of terrorismefinanciering.[45] Blijkens de website blijven de banken de eigen transacties monitoren, naast de gezamenlijke monitoring. De voorgestelde wetstekst sluit niet uit dat ook de eigen monitoring per bank wordt uitbesteed.

De Afdeling merkt op dat de voorgenomen vormgeving vragen oproept over de verdeling van verantwoordelijkheden. De deelnemende banken blijven verantwoordelijk om te voldoen aan hun wettelijke verplichtingen onder de Wwft.[46] De toelichting meldt dat zij daarnaast verwerkingsverantwoordelijke blijven zoals bedoeld in de AVG. De vraag is evenwel hoe dit in de praktijk zal uitwerken: hoe zijn verantwoordelijkheid en aansprakelijkheid geregeld tussen TMNL en de afzonderlijke banken? Dit dient duidelijk te zijn voor het geval er iets misgaat. Bijvoorbeeld als een cliënt vindt dat een bank ten onrechte consequenties verbindt aan een signaal, of als een transactie ten onrechte wel of niet wordt gesignaleerd, of in geval van een gegevenslek of een inbraak (hack) bij de gezamenlijke voorziening TMNL. Uit de toelichting begrijpt de Afdeling dat het de bedoeling is dat het toezicht indirect via de aangesloten banken loopt. In de toelichting wordt echter niet ingegaan op de effectiviteit van dit indirecte toezicht en de mogelijkheden corrigerend op te treden als er zaken misgaan.

De vraag is tot slot, meer fundamenteel, hoever de verantwoordelijkheid gaat van private instellingen (zoals banken, in welke samenwerkingsvorm dan ook) ten opzichte van de verantwoordelijkheid van de overheid. Deze vraag wordt pregnanter indien (vrijwel) alle banken in één gezamenlijke voorziening hun transacties laten monitoren.

Gelet op het voorgaande dient het wetsvoorstel te worden aangepast. De Afdeling adviseert de verantwoordelijkheden en de inrichting van het toezicht daarin te expliciteren.

4b. De Afdeling wijst op de onduidelijke verantwoordelijkheidsverdeling tussen de gezamenlijke voorziening en de deelnemende banken. De AVG legt de verantwoordelijkheid en aansprakelijkheid voor gegevensverwerking bij de verwerkingsverantwoordelijke en niet bij de verwerker. Dit uitgangspunt geldt ook voor gezamenlijke transactiemonitoring: niet de gezamenlijke voorziening, maar de banken zijn verantwoordelijk en aansprakelijk. Naar aanleiding van de opmerkingen van de Afdeling zijn

[45] Zie https://tmnl.nl. De deelnemende banken zijn aandeelhouder in de besloten vennootschap TMNL. De samenwerking staat in beginsel open voor andere in Nederland gevestigde banken.
[46] Artikel 10 eerste en (voorgesteld) tweede lid Wwft.

aanvullende waarborgen opgenomen ten aanzien van de verantwoordelijkheid van de aangesloten banken. Ten eerste is in het wetsvoorstel geëxpliciteerd dat de banken, als verwerkingsverantwoordelijken, ieder zelfstandig verantwoordelijk zijn voor de voorgeschreven waarborgen die de gezamenlijke voorziening dient te treffen. Deze waarborgen zien op de wijze van de verwerking van persoonsgegevens binnen de gezamenlijke voorziening: bijvoorbeeld het pseudonimiseren en versleutelen van persoonsgegevens, organisatorische waarborgen ten aanzien van de verwerking en het beveiligingsniveau en waarborgen ten aanzien van de automatische gegevensanalyse. Voorts dienen de banken ten minste één functionaris voor gegevensbescherming aan te wijzen binnen de gezamenlijke voorziening. Daarnaast zijn de banken verantwoordelijk voor de vastlegging en bekendmaking van de verantwoordelijkheid en aansprakelijkheid van de banken binnen de gezamenlijke voorziening ten opzichte van de betrokkene wiens gegevens binnen de voorziening worden gedeeld.

c. Cybersecurity

De Afdeling wijst er verder op dat het samenbrengen van zoveel (bijzondere) persoonsgegevens en andere vertrouwelijke zakelijke en particuliere gegevens in één systeem ten behoeve van de transactiemonitoring op een veilige en verantwoorde manier moet zijn geregeld.

De informatiebeveiliging in de financiële sector kent de nodige kwetsbaarheden.[47] DNB waarschuwt dat financiële instellingen mogelijk kwetsbaar zijn via dienstverleners waaraan werkzaamheden zijn uitbesteed en die toegang hebben tot hun data-infrastructuur.[48] Van belang is verder het zogenoemde concentratierisico doordat met één hack toegang kan worden verkregen tot de data van meerdere financiële instellingen tegelijk. De beoogde concentratie van gegevens in TMNL vormt een mogelijk aantrekkelijk doelwit voor cyberaanvallen. Daarmee zijn de beveiligingsrisico's (kans én impact) aanzienlijk. Ook indien de beveiliging bij de individuele banken en TMNL op termijn wel goed is geregeld, is het een gegeven dat deze nooit 100% te garanderen valt. Dit vormt niet alleen een risico vanuit de AVG bezien maar ook voor de integriteit van het financiële systeem en het vertrouwen van burgers in het bankwezen.

De Afdeling adviseert in de toelichting diepgaand in te gaan op de waarborgen ten aanzien van de cybersecurity en op de wijze waarop het toezicht hierop wordt georganiseerd.

4c. Naar aanleiding van deze opmerking is in de toelichting opgenomen dat het kader van de AVG en UAVG regels biedt voor de beveiliging van persoonsgegevens. Op grond van dit bestaande kader zijn gegevensverwerkers verplicht om passende technische en organisatorische maatregelen te treffen teneinde een op het risico afgestemd beveiligingsniveau te waarborgen daarbij rekening houdend met de laatste stand van de techniek. Daarnaast wil ik er op wijzen dat er op dit moment reeds sprake is van een hoge mate van dataconcentratie bij banken en andere financiële instellingen, die verder reikt dan alleen transactiegegevens. Deze concentratie is vereist voor het ordentelijk verloop van het betalingsverkeer en is maatschappelijk geaccepteerd. Het besluit prudentiële regels Wft schrijft op dit vlak reeds voor dat instellingen de nodige maatregelen

---

[47] DNB, Jaarlijkse informatiebeveiligingsmonitor, april 2020. DNB wijst onder meer op het niet tijdig doorvoeren van «patches» om kwetsbaarheden te minimaliseren, werkprocessen die draaien op verouderde software, onvoldoende inzicht in de life cycle van systemen en onvoldoende scheiding in het netwerk van banken (netwerksegmentatie).

[48] DNB, Jaarlijkse informatiebeveiligingsmonitor, april 2020.

dienen te nemen en beschikken over procedures en maatregelen om de integriteit, voortdurende beschikbaarheid en beveiliging van geautomatiseerde gegevensverwerking te waarborgen. De beveiliging van gegevens is derhalve reeds een integraal onderdeel van de bedrijfsvoering van financiële instellingen, waar toezicht op wordt gehouden door DNB. Ik acht het daarom niet aangewezen voor deze specifieke maatregel aanvullende vereisten op te nemen.

5. Onderzoeksplicht en gegevensdeling tussen instellingen bij cliëntenonderzoek

Om «shopgedrag» van cliënten te voorkomen, introduceert het voorstel de regeling dat als een zakelijke relatie of transactie naar haar aard indicaties van een hoger risico op witwassen of financiering van terrorisme met zich brengt, de instelling redelijke maatregelen neemt om te onderzoeken of een andere instelling van dezelfde categorie aan de cliënt diensten verleent, heeft verleend of heeft geweigerd.[49] De instelling moet vervolgens navraag doen bij die andere instelling naar gebleken risico's op witwassen of financieren van terrorisme.[50] Het is niet redelijk te verlangen van instellingen om «op goed geluk» bij alle andere instellingen navraag te doen naar gebleken risico's, aldus de toelichting.[51] Redelijke maatregelen zijn onder meer het raadplegen van openbare bronnen of andere bronnen die instellingen tot hun beschikking hebben,[52] en eveneens het raadplegen van een zwarte lijst met personen bij wie «risico's op witwassen of het financieren van terrorisme zijn vastgesteld».[53]

Het wetsvoorstel maakt verder mogelijk dat bij amvb bepaald kan worden dat het onderzoek zich kan uitstrekken tot instellingen van een andere categorie.[54] Ook regelt het voorstel dat advocaten en notarissen ten behoeve van de naleving van de in dit artikel opgenomen verplichtingen niet gehouden zijn aan hun wettelijke geheimhoudingsplicht.[55]

a. Noodzaak en proportionaliteit van gegevensdeling

Bij de onderzoeksplicht is sprake van verwerking van gegevens van cliënten waarbij het recht op respect voor het privéleven en het recht op gegevensbescherming in het geding zijn. Inbreuken hierop dienen te worden gerechtvaardigd aan de hand van de vereisten van noodzakelijkheid en proportionaliteit, zoals hiervoor ook al aan de orde is gekomen met betrekking tot de gezamenlijke monitoring.

Volgens de toelichting is de maatregel noodzakelijk omdat instellingen nog niet altijd goed in staat zijn om een juist risicoprofiel van de cliënt op te stellen. Het delen van gegevens zou de effectiviteit ten goede komen omdat zo een juist risicoprofiel van de cliënt kan worden opgesteld en «shopgedrag» wordt voorkomen, aldus de toelichting.[56] Het voorstel zou volgens de toelichting ook proportioneel zijn, omdat gegevensuitwisseling wordt beperkt tot die cliënten die een hoger risico met zich brengen, en er

---

[49] Voorgesteld artikel 3b, eerste lid. Memorie van toelichting, paragraaf 2.2.1.
[50] Voorgesteld artikel 3b, tweede lid.
[51] Memorie van toelichting, paragraaf 2.2.1.2.
[52] Memorie van toelichting, paragraaf 2.2.1.2.
[53] Dat mogelijk fungeert naast het al bestaande externe verwijzingsregister. Memorie van toelichting, paragraaf 2.2.1.2.
[54] Voorgesteld artikel 3b, vijfde lid.
[55] Voorgesteld artikel 3b, zesde lid.
[56] Memorie van toelichting, paragraaf 3.1, B.

bovendien alleen gegevens worden uitgewisseld tussen instellingen van dezelfde categorie.[57]

De Afdeling wijst er op dat in het kader van het noodzakelijkheidsvereiste de omvang van het probleem – in welke mate problematisch «shopgedrag» voorkomt – niet is toegelicht. Ook is niet duidelijk of dit niet op andere manieren kan worden opgelost.[58] *In samenhang met de vraag naar de noodzaak van deze maatregel, merkt de Afdeling op dat als informatie wordt gedeeld tussen instellingen over (de uitkomsten van) cliëntenonderzoek en gebleken risico's, vervolgens de vraag rijst wat de ontvangende instelling met die informatie kan. De toelichting stelt immers dat het delen van informatie de vragende instelling niet van de plicht ontslaat om zelf onderzoek te doen.*

De vraag is of dit in de praktijk goed kan worden geborgd, omdat het voor een instelling uit het oogpunt van doelmatigheid (wat de reden voor deze wijziging is) voor de hand ligt het eigen onderzoek te beperken als er signalen zijn van een andere instelling. Tegelijkertijd zal een instelling haar beslissing niet (uitsluitend) kunnen motiveren op basis van de informatie ontvangen van een andere instelling. De instelling is immers verplicht een eigen afweging te maken, zoals de toelichting aangeeft. De verstrekte gegevens kunnen slechts als hulpmiddel dienen bij deze afweging en kunnen daarvoor niet in de plaats komen.[59]

Een instelling dient redelijke maatregelen te nemen als een cliënt «naar haar aard indicaties van een hoger risico op witwassen of financieren van terrorisme met zich brengt».[60] *Deze open norm (wanneer een cliënt een hoger risico is) wordt in de toelichting niet geconcretiseerd. Dit kan ertoe leiden dat de drempel voor het delen van gegevens erg laag wordt. Ook is niet gespecificeerd welke gegevens een andere instelling moet delen. Voor de cliënt kan dit ingrijpende gevolgen hebben. Zo is het bijvoorbeeld goed denkbaar dat het aangaan van een bankrelatie in de praktijk moeilijk of onmogelijk wordt. Dat is ook het geval wanneer gebruik gemaakt wordt van zwarte lijsten, waarop in de volgende subparagraaf nader wordt ingegaan.*

Gelet op de ingrijpende gevolgen is het wetsvoorstel niet proportioneel als niet nader wordt gespecificeerd wanneer en welke gegevens kunnen worden uitgewisseld. De Afdeling adviseert daarom de noodzaak en proportionaliteit dragend te motiveren, en zo nodig het wetsvoorstel aan te passen.

5a. De Afdeling merkt op dat de noodzaak en proportionaliteit van de voorgestelde maatregel onvoldoende gemotiveerd is en adviseert om de verplichtingen en de uit te wisselen gegevens van de maatregel duidelijker te specificeren teneinde de drempel voor het delen van gegevens niet te laag wordt. Naar aanleiding van de opmerkingen zijn het wetsvoorstel en de toelichting aangepast. Met deze aanpassingen wordt de drempel voor het delen van gegevens zowel voor de verzoekende, als de ontvangende instelling verhoogd en gekoppeld aan concrete risico's. Ten eerste is gespecificeerd wanneer een instelling dient te onderzoeken of een andere instelling uit dezelfde categorie diensten verleent, heeft verleend of heeft geweigerd aan een cliënt. De verplichting geldt a) indien

---

[57] Idem, paragraaf 2.2.1.1.

[58] De AP wijst in haar advies hieromtrent bijvoorbeeld op uitbreiding van de capaciteit voor cliëntenonderzoek of een goed gebruik van het bestaande stelsel van zwarte lijsten, als mogelijke alternatieven.

[59] Memorie van toelichting, paragraaf 2.2.1.4.

[60] Voorgesteld artikel 3b, eerste lid.

de zakelijke relatie of transactie naar haar aard indicaties van een hoger risico op witwassen of financieren van terrorisme met zich brengt, b) indien de risicofactoren, bedoeld in bijlage III bij de vierde anti-witwasrichtlijn, van toepassing zijn; of c) de instelling het cliëntenonderzoek als bedoeld in artikel 8 verricht. Voor de eerste twee gevallen in onderdelen a en b is gekozen om een onderscheid te maken tussen subjectieve indicatoren en objectieve indicatoren, die zijn gestoeld op de systematiek van de indicatoren voor de verplichting tot het melden van ongebruikelijke transacties. In het derde geval, onder c, is de verplichting onderdeel van het verscherpt cliëntenonderzoek uit artikel 8. Deze indicaties sluiten aan bij de risicogebaseerde benadering die instellingen reeds dienen te hanteren bij de uitvoering van het cliëntenonderzoek. Voorts zijn naar aanleiding van het advies van de Afdeling ook de risico's die bij een verzoek om uitwisseling gedeeld mogen worden ingekaderd en gekoppeld aan objectieve factoren. De ontvangende instelling mag alleen risico's uitwisselen waarop de ontvangende instelling maatregelen heeft genomen om de risico's te beheersen. Hieronder wordt in ieder geval verstaan het weigeren of beëindigen van de dienstverlening. Derhalve zijn de uitgewisselde risico's niet willekeurig, maar moeten zij van een dusdanige aard zijn geweest dat de ontvangende instelling maatregelen heeft getroffen ter beheersing van deze risico's.

Daarnaast merkt de Afdeling op dat niet voldoende gespecificeerd is welke gegevens worden uitgewisseld. Naar aanleiding van deze opmerking is in het wetsvoorstel verduidelijkt welke gegevens dit betreft. Hiervoor is aansluiting gezocht bij de reeds verplicht te verzamelen gegevens voor het cliëntenonderzoek, vastgesteld in artikel 33 van de wet. Aangezien de verplichting om deze gegevens vast te leggen alvorens een zakelijke relatie aan te gaan voor alle instellingen geldt, zullen deze gegevens bij alle instellingen beschikbaar zijn.

b. Strafrechtelijke gegevens en zwarte lijsten

Het ligt in de rede dat instellingen van de hier gecreëerde mogelijkheid gebruik zullen maken om een gezamenlijk register te maken van verricht cliëntenonderzoek om dubbel werk te voorkomen. Het wetsvoorstel maakt zo een stelsel van zwarte lijsten mogelijk. De Afdeling merkt op dat er reeds zwarte lijsten bestaan, zoals het Incidentenwaarschuwingssysteem Financiële Instellingen, In het licht daarvan is de noodzaak, proportionaliteit en toegevoegde waarde van nog meer zwarte lijsten onduidelijk.[61] Ook merkt de Afdeling op dat een stelsel van zwarte lijsten een stigmatiserend karakter kan hebben.

Met een dergelijk stelsel van (extern werkende) zwarte lijsten is niet uitgesloten dat ook strafrechtelijke gegevens worden verwerkt.[62] Strafrechtelijke gegevens omvatten niet alleen strafrechtelijke veroordelingen en strafbare feiten,[63] maar ook «min of meer gegronde verdenkingen».[64] Strafrechtelijke gegevens kunnen alleen onder strikte

---

[61] https://www.nvb.nl/publicaties/protocollen-regelingen-richtlijnen/protocol-incidenten-waarschuwingssysteem-financi%C3%ABle-instellingen/. Overigens zou ook bij het externe verwijzingsregister, dat nu reeds als een zwarte lijst fungeert, navraag gedaan moeten worden bij de betreffende instelling die het incident heeft geregistreerd – en zou het dus op dezelfde manier functioneren als hier wordt beoogd.

[62] Vergelijk E. de Vries en L. Mourcous, «Privacyrechtelijke voorwaarden voor het gebruik van een zwarte lijst», Privacy & Informatie 2019–246.

[63] *Artikel 10 AVG, artikel 32 en 33 UAVG.*

[64] E. de Vries en L. Mourcous, «Privacyrechtelijke voorwaarden voor het gebruik van een zwarte lijst», Privacy & Informatie 2019–246, paragraaf 3. Zie ook het advies van de Afdeling advisering van de Raad van State van 26 maart 2020, W13.19.0425/III, Kamerstukken II 2019/20, 35 515, nr. 4, paragraaf 3b.

voorwaarden worden verwerkt. Ze mogen slechts worden verwerkt onder toezicht van de overheid, of als de verwerking is toegestaan bij een lidstaatrechtelijke bepaling die passende waarborgen biedt voor de rechten en vrijheden van de betrokkenen.[65] Met andere woorden, een zwarte lijst is mogelijk, maar bij de uitvoering moet worden voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.[66]

De toelichting ziet in de beoogde gegevensdeling meer mogelijkheden dan in het enkele gebruik van zwarte lijsten.[67] Tegelijkertijd sluit de toelichting niet uit dat gezamenlijke gegevensdeling juist leidt tot een verhoging van het gebruik van zwarte lijsten.[68] De Afdeling wijst er op dat het voorstel een grondslag creëert voor het verwerken van persoonsgegevens van strafrechtelijke aard,[69] onder meer voor het nemen van «redelijke maatregelen»,[70] waaronder een mogelijk stelsel van zwarte lijsten.

De Afdeling constateert dat buiten de primaire vraag naar de noodzaak en proportionaliteit (zie hiervoor) ook de vraag rijst naar passende waarborgen. De grondslag voor het verwerken van persoonsgegevens van strafrechtelijke aard is geformuleerd in algemene bewoordingen,[71] en waarborgen als de beveiliging van persoonsgegevens en de uitoefening van de rechten van betrokkenen worden niet verder geconcretiseerd.[72] De Afdeling merkt op dat nu een grondslag voor het verwerken van strafrechtelijke gegevens wordt gecreëerd, in het voorstel concrete passende waarborgen moeten worden geboden, zoals de AVG vereist.[73] Dit klemt temeer vanwege het stigmatiserende karakter van een mogelijk stelsel van zwarte lijsten.

De Afdeling adviseert de passende waarborgen te concretiseren en op te nemen in het wetsvoorstel.

5b. De Afdeling wijst er op dat de grondslag voor het uitwisselen van risico's tussen instellingen in het kader van het cliëntenonderzoek tevens een grondslag vormt voor het instellen van zwarte lijsten. Dat klopt, een centraal register (zwarte lijst) waarmee instellingen binnen dezelfde categorie risico's kunnen uitwisselen binnen de grenzen van de verplichting en de AVG kan een effectieve manier zijn om aan de verplichting te voldoen. De Afdeling wijst daarbij ook op Incidentenwaarschuwingssysteem Financiële Instellingen, dat reeds bestaat en onlangs opnieuw vergund is door de Autoriteit Persoonsgegevens.[74] Naar aanleiding van de opmerking van de Afdeling wordt in de toelichting nader ingegaan op de kaders waar een dergelijk centraal register aan dient te voldoen. Daarnaast is middels de beperking op de uit te wisselen risico's, zoals hierboven beschreven, reeds een aanzienlijke inperking van de verwerking gerealiseerd. Voorts wijst de Afdeling op de noodzaak voor passende waarborgen bij de verwerking van persoonsgegevens van strafrechtelijke aard, die verwerkt kunnen worden in het kader van de

---

[65] Artikel 10 AVG.
[66] Artikel 33, vijfde lid, UAVG.
[67] Memorie van toelichting, paragraaf 3.1, B.
[68] Memorie van toelichting, paragraaf 3.1, C.
[69] Voorgesteld artikel 34a, eerste lid.
[70] Voorgesteld artikel 3b, eerste lid.
[71] Voorgesteld artikel 34a, eerste lid.
[72] Voorgesteld artikel 34a, vijfde lid.
[73] Artikel 10 AVG. Zie ook het advies van de Afdeling advisering van de Raad van State van 26 maart 2020, W13.19.0425/III, Kamerstukken II 2019/20, 35 515, nr. 4, paragraaf 3b.
[74] Te raadplegen via: https://autoriteitpersoonsgegevens.nl/nl/nieuws/vergunning-voor-financiele-instellingen-om-info-over-fraude-te-delen.

uitvoering van deze verplichting. Ik onderschrijf die noodzaak volledig. Daarom zijn er nadere waarborgen op het gebied van gegevensbescherming toegevoegd aan het wetsvoorstel (zie hieronder onder het kopje *Overige wijzigingen*). Daarnaast bevat het wetsvoorstel een grondslag om bij algemene maatregel van bestuur nadere regels te stellen omtrent de rechten van betrokkenen en de beveiliging van gegevens bij de verwerking van bijzondere categorieën persoonsgegevens en persoonsgegevens van strafrechtelijke aard.

c. Geheimhoudingsplicht

Het voorstel creëert een grondslag om bij amvb uitwisseling tussen verschillende categorieën van instellingen mogelijk te maken.[75] Naast de vraag hoe omgegaan moet worden met de vertrouwelijkheidsregimes van banken,[76] roept dit de vraag op hoe omgegaan moet worden met de vertrouwelijkheidsregimes van bijvoorbeeld advocaten en notarissen. Het wetsvoorstel regelt dat advocaten en notarissen niet gehouden zijn aan hun geheimhoudingsplicht. Zolang zij met elkaar uitwisselen is dat geen probleem. Dat ligt echter anders op het moment dat moet worden uitgewisseld met een instelling die onder een lichter of zelfs geen vertrouwelijkheidsregime valt.

De Afdeling merkt op dat de geheimhoudingsplicht van advocaten en notarissen een publiek belang dient. Eenieder moet zich vrijelijk en zonder vrees voor openbaarmaking tot een advocaat of notaris kunnen wenden voor bijstand en advies.[77] De geheimhoudingsplicht is van groot belang voor het functioneren van de rechtsstaat en gaat om die reden vergezeld van een verschoningsrecht. De Afdeling wijst er daarom op dat een beperking van de geheimhoudingsplicht nader gemotiveerd dient te worden en duidelijk dient te worden afgebakend. Bij voorkeur wordt dit op geregeld bij wet, zodat het parlement daar ook expliciet mee kan instemmen.

De Afdeling adviseert in het licht van voorgaande de geheimhoudingsplicht in relatie tot het wetsvoorstel nader toe te lichten, en in het voorstel op te nemen dat de geheimhoudingsplicht tussen verschillende categorieën instellingen niet kan worden doorbroken.

5c. Naar aanleiding van het advies van de Afdeling is het wetsvoorstel aangepast. In de maatregel was reeds opgenomen dat alleen instellingen behorend tot dezelfde categorie, zoals bijvoorbeeld notarissen en advocaten, onderling risico's mogen uitwisselen. Daarnaast is een grondslag opgenomen dat bij algemene maatregel van bestuur de categorieën instellingen die met elkaar risico's uitwisselen, kunnen worden uitgebreid tot meerdere categorieën, dan wel nader ingeperkt kunnen worden binnen de categorie. Dit liet de mogelijkheid open dat bij algemene maatregel van bestuur bepaald kon worden dat advocaten of notarissen met andere categorieën instellingen risico's kunnen uitwisselen, dat is onwenselijk. In het wetsvoorstel is naar aanleiding van het advies van de Afdeling opgenomen dat de mogelijkheid tot uitbreiding niet geldt voor advocaten en notarissen, teneinde het beroepsgeheim van deze instellingen te respecteren.

---

[75] Voorgesteld artikel 3b, vijfde lid.

[76] Organisatorisch en technisch dienen banken voldoende maatregelen («Chinese walls») te nemen om te voorkomen dat informatie van andere banken voor andere afdelingen toegankelijk wordt.

[77] HR 22 juni 1984, ECLI:NL:PHR:1984:AG4835; HR 1 maart 1985, ECLI:NL:PHR:1985:AC9066 (Maas II, Notaris Maas-beschikking).

6. De Afdeling verwijst naar de bij dit advies behorende redactionele bijlage.

6. In de redactionele opmerkingen heeft de Afdeling verzocht om in de toelichting op artikel 10 expliciteren dat het gaat om omzetting van artikel 25 van Richtlijn (EU) 2015/849 en toelichten hoe wordt voldaan aan de uitbestedingseisen in artikel 25 tot en met 28 van deze richtlijn. Artikel 25 van de richtlijn is echter niet geïmplementeerd middels artikel 10 van de Wwft, maar middels artikel 5 van de Wwft. Artikelen 25 tot en met 28 van de richtlijn zien op nakoming door derden, dat wil zeggen dat een instelling in bepaalde gevallen mag vertrouwen op cliëntenonderzoek uitgevoerd door een andere instelling. Artikel 29 van de richtlijn stelt dat de bepalingen voor nakoming door derden niet van toepassing zijn op uitbestedings- of agentuurverhoudingen. In die gevallen geldt de partij die uitbestede taken uitvoert namens de instelling formeel als de instelling zelf, deze vorm van uitbesteding wordt in de wet geregeld middels artikel 10.

De Afdeling advisering van de Raad van State heeft een aantal bezwaren bij het voorstel en adviseert het voorstel niet bij de Tweede Kamer der Staten-Generaal in te dienen, tenzij het is aangepast.

De vice-president van de Raad van State,
Th.C. de Graaf

7. Overige wijzigingen

Van de gelegenheid is gebruik gemaakt om enkele andere wijzigingen in het wetsvoorstel en de memorie van toelichting aan te brengen.

Verbod op contante betalingen voor beroeps- of bedrijfsmatige handelaren

Naar aanleiding van inzichten opgedaan aan de hand van een tweede uitvoeringstoets van de Belastingdienst en recente ervaringen uit de praktijk zijn enkele wijzigingen aangebracht in het voorstel voor een verbod op contante transacties van € 3.000 of meer voor handelaren in goederen, het voorgestelde artikel 1f. Ten eerste is de reikwijdte van de verplichting uitgebreid tot handelaren in kunstvoorwerpen en pandhuizen, de instellingen genoemd in artikel 1a, eerste lid, onderdelen k en p, van de wet. De activiteiten van deze instellingen kunnen immers ook handel in goederen betreffen, het verbod geldt dan ook alleen voor deze activiteiten. Aangezien deze instellingen ook voor andere handelingen dan contante transacties onder de wet vallen worden zij niet geheel uitgezonderd van de verplichtingen volgend uit de Wwft. Ten tweede is verduidelijkt dat het verbod geldt voor transacties in of vanuit Nederland. In de toelichting is nader uiteengezet wat dit betekent en zijn ter verduidelijking enkele voorbeelden gegeven. Tot slot is in het voorgestelde artikel 1f een tweede lid opgenomen dat een grondslag biedt om bij algemene maatregel van bestuur indicatoren vast te stellen die een aanwijzing zijn dat een transactie plaatsvindt door middel van meer handelingen waartussen een verband bestaat. Inzichten uit de praktijk van het huidige toezicht op handelaren wijst uit dat criminelen bewust transacties opdelen om onder de huidige grens van € 10.000 te blijven. De huidige definitie van samengestelde transacties, «twee of meerdere transacties waartussen een verband bestaat», levert rechtsonzekerheid op en sluit niet goed aan op veranderende casuïstiek in de praktijk.

Extra waarborgen gebruik bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard

Het voorstel bevat een verduidelijking van het gebruik van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard. Deze bepaling schrijft voor dat Wwft-instellingen alleen persoonsgegevens, waaronder bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard, mogen verwerken voor zover dat noodzakelijk is om te voldoen aan de verplichtingen van de wet. Daarnaast zullen bij algemene maatregel van bestuur nadere regels worden gesteld over deze verwerking, in ieder geval betreft de beveiliging en uitoefening van rechten van betrokkene. De Afdeling heeft geen opmerkingen gemaakt in haar advies ten aanzien van deze maatregel. Desalniettemin, is – in het licht van de opmerkingen bij de andere onderdelen van het wetsvoorstel – ervoor gekozen om deze grondslag aan te vullen met waarborgen. Wwft-instellingen dienen ook vast te leggen welke persoonsgegevens worden verwerkt, de wijze van verwerking en op grond van welke verplichting. Daarnaast moet de Wwft-instelling de betrokkene informeren over de verwerking. Voorts is de toelichting op het wetsvoorstel aangevuld met een nadere uitleg over de voortdurende controle van transacties en welke gegevens hierbij verwerkt worden en waarom de verwerking van (bijzondere) persoonsgegevens noodzakelijk is om effectief te voldoen aan de verplichtingen van het cliëntenonderzoek, waaronder het monitoren van transacties.

Schrappen maatregelen trustkantoren

Het voorstel bevatte oorspronkelijk maatregelen ten aanzien van trustkantoren. Deze maatregelen zagen op een verbod om als doorstroomvennootschap op te treden en zaken te doen met cliënten uit derde hoog risicolanden aangewezen als niet coöperatief op belastinggebied. Deze maatregelen zijn uit het voorstel gehaald en middels een separaat wetsvoorstel ingediend.[78]

Ik verzoek U, mede namens de Minister van Justitie en Veiligheid, 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,
S.A.M. Kaag

[78] Kamerstukken II 2021/22, 36 102, nr. 2.

Redactionele bijlage bij het advies van de Afdeling advisering van de Raad van State betreffende no. W06.20.0354/III

In de toelichting op artikel 10 expliciteren dat het gaat om omzetting van artikel 25 van Richtlijn (EU) 2015/849 en toelichten hoe wordt voldaan aan de uitbestedingseisen in artikel 25 tot en met 28 van deze richtlijn.