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. 3 **MEMORIE VAN TOELICHTING**

ALGEMEEN

§ 1. Inleiding

Het voorkomen en bestrijden van witwassen en financieren van terrorisme 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 opbrengsten 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. Het misbruik van het financiële stelsel door criminelen tast de integriteit van dit stelsel aan. Het is daarom cruciaal dat het gebruik van legale financiële kanalen voor criminele doeleinden wordt tegengegaan.

Het kabinet heeft een plan opgesteld waarin maatregelen zijn aangekondigd om de aanpak van witwassen effectiever te maken.[1] Deze maatregelen verhogen de barrières voor witwassen, vergroten de effectiviteit van de poortwachtersfunctie en het toezicht op de naleving en versterken de opsporing en vervolging. De maatregelen uit het plan van aanpak witwassen komen voort uit de bredere inzet van het kabinet om de integriteit van de financiële sector te vergroten, ook op het terrein van het voorkomen en bestrijden van financieren van terrorisme. In het onderhavige wetsvoorstel zijn enkele maatregelen opgenomen uit het plan die een wijziging vereisen van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) en de Wet op economische delicten.

[1] Kamerstukken II 2018/19, 31 477, nr. 41.

kst-36228-3
ISSN 0921 - 7371
's-Gravenhage 2022

Dit wetsvoorstel is onder te verdelen in vier onderdelen:
1. Een verbod voor beroeps- of bedrijfsmatige handelaren in goederen om transacties vanaf € 3.000 in contanten te verrichten;
2. Gegevensdeling mogelijk maken tussen instellingen behorend tot dezelfde categorie in het kader van het cliëntenonderzoek bij een hoger risico op witwassen of financieren van terrorisme;
3. Gezamenlijk monitoren van transacties mogelijk maken voor banken;
4. Verduidelijking van het gebruik van bijzondere categorieën persoonsgegevens en persoonsgegevens van strafrechtelijke aard in het kader van verplichtingen op grond van de Wwft, ter voorkoming van witwassen en financieren van terrorisme.

Deze wijzigingen worden ieder afzonderlijk toegelicht in de tweede paragraaf van deze toelichting. In de derde paragraaf wordt nader ingegaan op de gegevensbescherming. Paragraaf vier ziet op de handhaafbaarheid en uitvoerbaarheid van deze wijzigingen, waarbij met name aandacht wordt besteed aan de handhaving van het verbod op contante betalingen bij beroeps- of bedrijfsmatige handelaren in goederen. De financiële gevolgen en administratieve lasten van dit wetsvoorstel worden beschreven in paragraaf vijf en in paragraaf zes wordt ingegaan op de consultatiereacties op dit wetsvoorstel. In het tweede deel van deze toelichting worden de artikelen afzonderlijk toegelicht.

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

§ 2. Inhoud wetsvoorstel

§ 2.1. Verbod op contante betalingen vanaf € 3.000

Een van de maatregelen om de barrières voor witwassen te verhogen, is het beperken van het gebruik van grote sommen contant geld. Uit verschillende studies blijkt dat contant geld bij het witwassen van geld een belangrijke rol speelt.[2] Ook de supranationale risicobeoordeling, uitgevoerd door de Europese Commissie, bevestigt dat contant geld nog steeds het meest gebruikte instrument is om geld wit te wassen.[3] De voornaamste reden hiervoor is dat contant geld moeilijk traceerbaar is en daarom aantrekkelijk om de herkomst van crimineel vermogen te verhullen. Met de introductie van een verbod op contante betalingen vanaf € 3.000 wordt beoogd een balans te treffen tussen de noodzaak om deze risico's beter te adresseren en het belang van het in stand houden van een toegankelijk betalingsverkeer. Deze maatregel moet ertoe leiden dat het witwassen van grote sommen illegale middelen via contant geld moeilijker wordt.

Het huidige systeem ten aanzien van contante betalingen ziet er als volgt uit. Beroeps- of bedrijfsmatige handelaren, kopers en verkopers van goederen, vallen onder de reikwijdte van de Wwft, indien de betaling van de goederen in contanten plaatsvindt voor een bedrag van € 10.000 of meer, ongeacht of de transactie plaatsvindt in een handeling of door

[2] Voorbeelden van studies zijn: Europol (2015). Why is cash still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering; Ecorys (in opdracht van de Europese Commissie), Study on an EU initiative for a restriction on payments in cash.

[3] Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, COM(2019)370.

middel van meer handelingen waartussen een verband bestaat.[4] Dit betekent dat voor handelaren van goederen bij contante betalingen vanaf een bedrag van € 10.000 de verplichtingen van de Wwft gelden, zoals volgt uit artikel 2, derde lid, onder e van de (gewijzigde) vierde anti-witwasrichtlijn. In die gevallen moeten de handelaren onderzoek doen naar hun cliënten en ongebruikelijke transacties melden bij de FIU-Nederland. Een transactie is ongebruikelijk indien de transactie handelaren aanleiding geeft om te veronderstellen dat deze verband kan houden met witwassen of financieren van terrorisme (subjectieve indicator)[5]. Indien een transactie plaatsvindt waarbij één of meerdere voertuigen, schepen, kunstvoorwerpen, antiquiteiten, edelstenen, edele metalen, sieraden of juwelen gekocht of verkocht worden tegen geheel of gedeeltelijke contante betaling, waarbij het contant te betalen bedrag € 20.000 of meer bedraagt, moeten voornoemde handelaren hiervan altijd een melding doen bij de FIU-Nederland (objectieve indicator).[6]

Het systeem in Nederland zorgt ervoor dat contante betalingen onder € 10.000 bij beroeps- en bedrijfsmatige handelaren in goederen volledig buiten beeld blijven, terwijl er ook aan lagere bedragen risico's op witwassen en financieren van terrorisme verbonden zijn. Bovendien heeft het merendeel van de Europese lidstaten maatregelen getroffen om risico's bij lagere contante betalingen aan te pakken. Momenteel zijn er in totaal negentien lidstaten die een grens hanteren op contante betalingen, waaronder België en Frankrijk. Doordat de regels voor contante betalingen in Nederland soepeler zijn dan in deze landen, is Nederland aantrekkelijker voor criminelen om contant geld wit te wassen. Dit kan grofweg op twee manieren tegengegaan worden. Allereerst door het verlagen van de grens voor het verrichten van cliëntenonderzoek en het melden van ongebruikelijke transacties, ten tweede door het introduceren van een verbod op contante betalingen. In het kader van het plan van aanpak witwassen is de wenselijkheid en effectiviteit van beide maatregelen onderzocht. Uit overleg met diverse belanghebbenden, waaronder toezichthouders, opsporingsinstanties en private partijen, komt een verbod op contante betalingen naar voren als de meest effectieve maatregel. Daarbij is van belang dat een verbod op betalingen in contanten vanaf een bepaald bedrag duidelijk en goed uitvoerbaar is, terwijl het verlagen van de grens waarbij cliëntenonderzoek moet worden verricht, leidt tot meer lasten voor een grotere groep handelaren en cliënten.

Een belangrijke factor om rekening mee te houden bij het tegengaan van witwasrisico's in verband met contante betalingen is een mogelijk waterbedeffect. Om de kans hierop effectief te verminderen, is het noodzakelijk dat de Nederlandse inrichting van het verbod aansluit op de manier waarop de ons omringende landen een dergelijk verbod hebben ingericht. Om die reden is in onderhavig wetsvoorstel een verbod op contante betalingen vanaf een bedrag van € 3.000 voor beroeps- en bedrijfsmatige handelaren in goederen opgenomen. Deze inrichting van het verbod sluit aan bij de wijze waarop België het verbod op contante betalingen heeft vormgegeven, waar het verbod ook op € 3.000 is gesteld. De overweging daarbij is dat bij de introductie van een verbod op contante betalingen het belang van een toegankelijk betalingsverkeer in

---

[4] De leidraad van Bureau Toezicht Wwft geeft meer informatie over wanneer er sprake is van een samenhangende transactie. Factoren die relevant kunnen zijn bij het vaststellen van samenhang zijn bijvoorbeeld: hetzelfde factuuradres, identieke handtekening op de ontvangstbewijzen of de bedragen zijn afkomstig uit hetzelfde vermogen (bijvoorbeeld echtelieden).

[5] Zie Bijlage Indicatorenlijst bij het Uitvoeringsbesluit Wwft 2018. De subjectieve indicator geldt voor alle handelaren indien de betaling van de goederen in contanten plaatsvindt vanaf een bedrag van € 10.000 of meer.

[6] Zie Bijlage Indicatorenlijst bij het Uitvoeringsbesluit Wwft 2018.

ogenschouw moet worden genomen. In dat licht is het onwenselijk om contante betalingen onnodig te beperken. Om die reden is de hoogte van het verbod vastgesteld op € 3.000 en niet, zoals bijvoorbeeld in Frankrijk, op een bedrag van € 1.000. Duitsland is hierbij buiten beschouwing gelaten, aangezien daar geen extra maatregelen gehanteerd worden ten opzichte van contant geld. Het is vooraf lastig te kwantificeren wat de effecten zullen zijn van het verbod op omringende landen. De kans bestaat dat door de invoering van het verbod er een verschuiving zal plaatsvinden naar landen waar geen extra restricties gelden ten opzichte van contant geld. Het mogelijk optreden van een waterbedeffect naar andere landen zal meegenomen worden in de evaluatie van het verbod.

Het verbod geldt voor betalingen in contanten die in of vanuit Nederland worden verricht en geldt hoofdzakelijk voor beroeps- of bedrijfsmatige kopers en verkopers van goederen (handelaren). Deze partijen hebben nu al te maken met de Wwft bij contante betalingen van meer dan € 10.000. Met de inwerkingtreding van deze wet, vervalt de huidige verplichting voor handelaren tot het verrichten van cliëntenonderzoek, transactiemonitoring en het melden van ongebruikelijke transacties. Het verbod heeft geen invloed op de objectieve meldgrenzen en subjectieve meldplicht die gelden voor andere instellingen dan handelaren. Daarnaast geldt het ook voor handelaren in kunstvoorwerpen en pandhuizen voor zover zij goederen aan- of verkopen in contanten. Handelaren zijn professionele partijen die bedrijfs- of beroepsmatig met financiële stromen te maken hebben bij het verkopen of kopen van goederen. Het verbod geldt dus niet voor particulieren en heeft geen betrekking op diensten. De leidraad van Bureau Toezicht Wwft (BTWwft),[7] die toezicht houdt op deze groep, geeft meer informatie over welke partijen onder het begrip «handelaar» vallen.

Vijf jaar na inwerkingtreding van het verbod, zal de effectiviteit van het verbod geëvalueerd worden. Hierbij zal in ieder geval aandacht besteed worden aan de reikwijdte van het verbod, zowel ten aanzien van de maximale hoogte van toegestane contante betalingen als de doelgroep. Ook zal een eventueel waterbedeffect naar andere sectoren en landen worden bezien, alsmede de uitvoering en de handhaving van het verbod.

§ 2.2. Vergroten samenwerking en informatie-uitwisseling instellingen

Instellingen[8] vervullen een poortwachtersfunctie ten behoeve van de bescherming van de integriteit van het financiële stelsel. Deze poortwachtersfunctie wordt internationaal en Europees gezien als de meest effectieve manier om het gebruik van het financiële stelsel voor witwassen en financieren van terrorisme te voorkomen. Deze instellingen hebben immers direct contact met de cliënt bij het aangaan van een zakelijke relatie en hebben veelal doorlopend zicht op de cliënt na het aangaan van die zakelijke relatie. Zij zijn daarmee bij uitstek in staat om te beoordelen wanneer een transactie niet past binnen het profiel van een cliënt en om die reden als ongebruikelijk moet worden aangemerkt. De vervulling van de poortwachtersfunctie is zodoende een belangrijke maatschappelijke taak, die kennis en investeringen vereist. Met de introductie van de onderstaande twee maatregelen, krijgen instellingen de mogelijkheid om hun kennis en capaciteit effectiever te bundelen. Dit zal

[7] Leidraad Wet ter voorkoming van witwassen en financieren van terrorisme: richtlijnen voor kopers en verkopers van goederen, maart 2022.

[8] Met «instellingen» wordt in dit wetsvoorstel gedoeld op instellingen in de zin van artikel 1a van de Wwft. In dit artikel is bepaald voor welke instellingen de Wwft van toepassing is. In artikel 1a van de Wwft worden drie hoofdcategorieën onderscheiden: banken; andere financiële ondernemingen; en aangewezen natuurlijke personen, rechtspersonen of vennootschappen handelend in het kader van hun beroepsactiviteiten.

leiden tot een verbetering van hun informatiepositie, die cruciaal is voor effectief cliëntenonderzoek en het monitoren van transacties en zodoende zal leiden tot een meer adequate invulling van hun poortwachtersfunctie.

Hieronder wordt ten eerste de maatregel toegelicht die ziet op het instellen van een onderzoeksplicht voor instellingen behorend tot dezelfde categorie om bij vorige dienstverleners na te gaan of deze een hoger risico op witwassen of financieren van terrorisme heeft vastgesteld ten aanzien van een bepaalde cliënt en, indien van toepassing, relevante gegevens te delen. Daarna wordt de maatregel toegelicht waarmee gezamenlijk monitoren van transacties mogelijk wordt gemaakt voor banken.

§ 2.2.1. Gegevensdeling tussen instellingen bij cliëntenonderzoek

Vanuit meerdere partijen, waaronder instellingen, toezichthouders en opsporingsinstanties, is gewezen op de risico's van het probleem dat cliënten die bij een instelling geweigerd zijn of waaraan de dienstverlening is gestaakt vanwege risico's op witwassen of financieren van terrorisme, vervolgens opnieuw dienstverlening kunnen aanvragen bij andere instellingen («shopgedrag»). In dergelijke gevallen zullen opeenvolgende instellingen cliëntenonderzoek moeten doen zonder de wetenschap dat andere instellingen bij deze cliënt reeds risico's op witwassen of financieren van terrorisme hebben geconstateerd. Ook als er aanwijzingen zijn dat de cliënt eerder is afgewezen door een andere instelling, kan er geen gegevensdeling plaatsvinden en zal een instelling van vooraf aan onderzoek moeten doen naar de cliënt. Dit vormt niet alleen een onnodige werklast voor instellingen, maar het is ook een risico voor de integriteit van het financiële stelsel en ondergraaft de effectiviteit van de Wwft. Hierdoor wordt de kans vergroot dat kwaadwillende cliënten door middel van shopgedrag uiteindelijk toch toegang krijgen tot het financiële stelsel.

De wetgeving inzake gegevensbescherming en de Wwft staan reeds toe dat instellingen op basis van toestemming van de cliënt informatie over cliënten kunnen uitwisselen met andere instellingen. Bij het ontbreken van deze toestemming kan deze informatie-uitwisseling op dit moment niet plaatsvinden. Om de kans te verkleinen dat een kwaadwillende cliënt door middel van shopgedrag toegang krijgt tot het financiële stelsel en om te voorkomen dat elke instelling van vooraf aan hoeft te beginnen met het verzamelen van relevante gegevens, is het noodzakelijk dat instellingen informatie uitwisselen bij een cliënt met indicaties van een hoger risico op witwassen of financieren van terrorisme. Hiertoe wordt in dit wetsvoorstel de verplichting opgenomen voor instellingen om, indien een zakelijke relatie of transactie naar haar aard een hoger risico op witwassen of financieren van terrorisme met zich meebrengt, er sprake is van factoren die duiden op een hoger risico genoemd in bijlage III van de vierde anti-witwasrichtlijn en in het kader van het verscherpt cliëntenonderzoek, te onderzoeken of de cliënt een andere instelling uit dezelfde categorie om dienstverlening heeft verzocht, bij deze instelling dienstverlening heeft afgenomen of op dit moment afneemt.[9] Indien hier sprake van is, dient de instelling navraag te doen bij de andere instelling naar gebleken risico's op witwassen of financieren van terrorisme. Indien de andere dienstverlener dergelijke risico's heeft geconstateerd, is deze gehouden de relevante gegevens onverwijld te verstrekken. Het gaat hier met nadruk om één op één uitwisseling tussen instellingen. Instellingen dienen,

[9] Hiermee wordt tevens de motie van de leden Van der Linde en Ronnes (Kamerstukken II 2019/20, 35 245, nr. 12) afgedaan, waarin de regering wordt verzocht om zich in te spannen om dubbelingen in het cliëntenonderzoek zoveel als mogelijk te voorkomen.

voorafgaand aan de dienstverlening, hun cliënten te informeren over deze verplichting.

§ 2.2.1.1 Dezelfde categorie van instellingen

De verplichting tot het verrichten van onderzoek naar eerdere (geweigerde) dienstverlening of huidige dienstverleners geldt alleen met betrekking tot dezelfde categorie van de verschillende instellingen, zoals opgenomen in artikel 1a, tweede, derde en vierde lid, van de Wwft. Een bank hoeft dus alleen onderzoek te doen naar eerdere dienstverlening door andere banken en niet naar bijvoorbeeld dienstverlening door een advocaat en vice versa. In de artikelsgewijze toelichting wordt verder uiteengezet wanneer instellingen onder dezelfde categorie vallen. Hier is voor gekozen omdat instellingen uit dezelfde categorie over het algemeen soortgelijke producten of diensten aanbieden en daardoor ook te maken hebben met soortgelijke risico-inschattingen. Gegevensuitwisseling tussen deze instellingen zal zodoende het grootste effect sorteren. Daarnaast is een verplichting om onderzoek te verrichten en gegevens uit te wisselen tussen alle categorieën instellingen niet proportioneel, noch vanuit het oogpunt van lasten voor de instelling en cliënt, noch vanuit het oogpunt van gegevensbescherming. Wel is het denkbaar dat gegevensuitwisseling tussen specifieke verschillende categorieën van instellingen wenselijk zou kunnen zijn, bijvoorbeeld omdat er vergelijkbare of sterk verweven diensten worden aangeboden of omdat in de praktijk blijkt dat er veel shopgedrag plaatsvindt tussen deze verschillende categorieën van instellingen. In het wetsvoorstel is daarom een grondslag opgenomen om bij algemene maatregel van bestuur uitwisseling tussen verschillende categorieën van instellingen mogelijk kunnen te maken. Daarnaast bestaat er de mogelijkheid dat instellingen weliswaar formeel binnen dezelfde categorie vallen, maar in de praktijk weinig overeenkomsten kennen in hun dienstverlening. In dergelijke gevallen zou informatie-uitwisseling niet effectief en niet proportioneel zijn. De voornoemde grondslag voorziet derhalve ook in de mogelijkheid om de onderzoeksplicht alleen te laten gelden voor specifieke instellingen binnen dezelfde categorie.

§ 2.2.1.2 Inspanningsverplichting

De onderzoeksplicht van instellingen naar eerdere dienstverlening is een inspanningsverplichting. Dit betekent dat een instelling redelijke maatregelen moet hebben getroffen om na te gaan of een cliënt eerder bij een andere instelling uit dezelfde categorie diensten heeft afgenomen. Wat redelijk is, hangt af van de context van het specifieke geval. In zijn algemeenheid kan gesteld worden dat het niet redelijk is om te verlangen dat een instelling op goed geluk alle andere instellingen uit haar categorie benadert om navraag te doen. Binnen het redelijke valt bijvoorbeeld wel het nagaan bij de cliënt bij welke andere instellingen deze momenteel of in het verleden soortgelijke diensten heeft afgenomen, alsook het raadplegen van openbare bronnen en bronnen van informatie die instellingen tot hun beschikking hebben, zoals databases met verschillende nieuwsbronnen. Op basis hiervan kan worden bepaald bij welke andere instellingen uit dezelfde categorie de gebleken risico's op witwassen of het financieren van terrorisme moet worden nagegaan.

Daarnaast kunnen groepen instellingen of sectoren behorend tot dezelfde categorie ter uitvoering van deze verplichting een centraal registratiesysteem opzetten waarbij geconstateerde risico's op witwassen en financiering van terrorisme worden geregistreerd en uitgewisseld wanneer de verplichting van toepassing is. Indien een dergelijk registratiesysteem persoonsgegevens van strafrechtelijke aard bevat, dient hiervoor een vergunning aangevraagd te worden bij de Autoriteit Persoonsge-

gevens.[10] Een dergelijk registratiesysteem kan een effectief middel zijn om shopgedrag tussen instellingen te voorkomen.

De inspanningsverplichting om onderzoek te doen naar eerdere dienstverlening gaat terug tot dienstverlening die uiterlijk vijf jaar geleden is beëindigd. Hiermee wordt aangesloten bij de reeds geldende bewaartermijn voor bewijsstukken uit artikel 33, derde lid, van de Wwft. Aangezien een instelling vijf jaar na het beëindigen van de zakelijke relatie de gegevens dient te vernietigen, heeft het geen zin om navraag te doen naar oudere gegevens. Bij de inwerkingtreding van het wetsvoorstel zal er geen sprake zijn van terugwerkende kracht. Dit betekent dat de onderzoeksplicht zal gelden voor nieuwe cliënten en voor bestaande cliënten in het kader van het voortdurende cliëntenonderzoek (zie voor de toelichting onder paragraaf 2.2.1.3) en dat bij navraag enkel de gegevens mogen worden verstrekt waar de instelling na inwerkingtreding van dit wetsvoorstel de beschikking over heeft verkregen.

§ 2.2.1.3 Navraagplicht

De gegevensuitwisseling is uit overwegingen van proportionaliteit beperkt tot gevallen waarbij een zakelijke relatie of transactie naar haar aard indicaties van een hoger risico op witwassen of financieren van terrorisme met zich meebrengt, er sprake is van de risicofactoren genoemd in bijlage III van vierde anti-witwasrichtlijn en in het kader van het verscherpt cliëntenonderzoek. In de artikelsgewijze toelichting bij dit artikel wordt nader ingegaan op het verschil tussen deze drie categorieën.

De aanwezigheid van (indicaties van) een hoger risico rechtvaardigt dat informatie over de cliënt wordt gedeeld en de lasten die bij de instellingen worden neergelegd met deze maatregel. Het zou zowel vanuit het oogpunt van gegevensbescherming als vanuit het oogpunt van lasten voor instellingen en cliënten, niet proportioneel zijn als instellingen bij alle cliënten onderzoek zouden moeten doen. Door de beperking van deze maatregel tot de gevallen waarin sprake is van (indicaties van) een hoger risico, is de kans groter dat de navraag leidt tot deling van gegevens over risico's op witwassen of financieren van terrorisme. Deze gegevensdeling zal in de praktijk ook kunnen leiden tot een lastenverlichting voor de vragende instelling, aangezien deze gebruik kan maken van de informatie die de andere dienstverlener reeds heeft verzameld.

De verplichting om onderzoek te doen en de mogelijkheid om gegevens te delen geldt overigens niet uitsluitend in het geval dat er cliëntenonderzoek wordt gedaan voordat de zakelijke relatie wordt aangegaan of een transactie wordt uitgevoerd, maar ook bij reeds bestaande cliënten. De gegevens verzameld in het kader van het cliëntenonderzoek dienen immers, met inachtneming van het risicoprofiel van de cliënt, actueel gehouden worden door instellingen op grond artikel 3, elfde lid van de Wwft. Niet alleen bij aanvang van de zakelijke relatie, maar ook gedurende die zakelijke relatie kan er aanleiding bestaan om onderzoek te verrichten, bijvoorbeeld als er gedurende de zakelijke relatie indicaties ontstaan dat de cliënt betrokken is bij witwassen of financieren van terrorisme. Ook in de gevallen dat een instelling gedurende de zakelijke relatie cliëntenonderzoek verricht en er (indicaties van) een hoger risico op witwassen of financieren van terrorisme naar voren komt, moet deze instelling onderzoek doen naar dienstverlening door andere instellingen uit dezelfde categorie en kunnen er gegevens gedeeld worden indien er sprake is van gebleken risico's op witwassen of financieren van terrorisme. De instelling

[10] Artikel 33, vierde lid, onder c, van de UAVG.

dient, op grond van het vierde lid van artikel 3b, de cliënt te informeren over het bestaan van deze verplichting.

§ 2.2.1.4 Gegevensdeling

Bij het doen van navraag bij een andere instelling verstrekt de verzoekende instelling slechts de bij wet genoemde gegevens. De instelling bij wie navraag wordt gedaan over een bepaalde cliënt, deelt uitsluitend informatie over de cliënt in het geval dat deze risico's op witwassen of financieren van terrorisme heeft geconstateerd ten aanzien van de cliënt en geleid hebben tot het nemen van aanvullende maatregel, waaronder in ieder geval weigering of beëindiging van de relatie verstaan wordt. Hierbij worden uitsluitend de gegevens gedeeld die destijds relevant waren voor het nemen van deze maatregelen. Het desgevraagd delen van deze gegevens is een verplichting voor de instelling bij wie een verzoek wordt gedaan. Deze verplichting ontslaat de instelling echter niet van het tipping-off verbod neergelegd in artikel 23 van de Wwft. Dit betekent dat die instelling bij het verstrekken van de gegevens de vragende instelling niet mag informeren over meldingen en inlichtingen verstrekt aan de FIU-Nederland. Alleen de uitzondering van artikel 23, zesde lid, van de Wwft – waarin bepaalde instellingen, onder voorwaarden en binnen dezelfde categorie, gegevens kunnen uitwisselen – kan hier in individuele gevallen van toepassing zijn.

De gegevens dienen onverwijld na ontvangst van het verzoek verstrekt te worden. Dit betekent dat de instelling zo snel mogelijk de gegevens verstrekt. Om shopgedrag te voorkomen is het van belang dat de vragende instelling zo snel mogelijk de beschikking krijgt over de gegevens, zodat deze zo snel mogelijk betrokken kunnen worden bij het cliëntenonderzoek en facilitering van witwassen of financiering van terrorisme voorkomen kan worden. Als deze gegevens langer op zich laten wachten, wordt de doelstelling van de maatregel ondergraven.

De instelling die de geconstateerde risico's ontvangt, kan deze gebruiken ten behoeve van haar eigen afweging ten aanzien van de risico's op witwassen of financieren van terrorisme bij de cliënt. De verstrekte gegevens ontslaan de verzoekende instelling niet van de verplichting om een eigen afweging te maken ten aanzien van de risico's van de cliënt. De verstrekte gegevens kunnen zodoende als hulpmiddel dienen bij de eigen afweging, maar mogen nooit in de plaats komen van de eigen afweging van de verzoekende instelling. De verzoekende instelling dient op grond van haar eigen risicobeoordeling vast te stellen of haar dienstverlening zodanig is ingericht dat de risico's afdoende te mitigeren zijn. Dat kan bijvoorbeeld betekenen dat de bevraagde instelling op grond van de geconstateerde risico's in het verleden heeft besloten af te zien van dienstverlening of dienstverlening te staken, terwijl de verzoekende instelling de risico's kan mitigeren met aanvullende maatregelen en wel tot dienstverlening overgaat.

§ 2.2.1.5 Gezamenlijke register

Instellingen behorend tot dezelfde categorie kunnen ten behoeve van de uitvoering van deze verplichting een eigen register instellen waarbinnen instellingen risico's kunnen uitwisselen. Belangrijk daarbij is dat een dergelijk register voldoet voorwaarden voor uitwisseling die volgen uit de verplichting en de algemene voorwaarden die uit de Algemene Verordening Gegevensbescherming (AVG) en de uitvoeringswet AVG volgen. Naast de algemeen geldende verplichtingen betreffende zoals het gebruik van technologische hulpmiddelen, beveiliging en toegang tot het systeem en de rechten van betrokkenen, is het uitgangspunt van dataminimalisatie

in dit verband bijzonder relevant. Zoals hierboven beschreven geldt de verplichting slechts in beperkte gevallen, namelijk indien er indicaties zijn voor een hoger risico. Voorts dienen instellingen bij het doen en beantwoorden van een verzoek slechts beperkt gegevens uitwisselen, namelijk de geconstateerde risico's en de bij wet voorgeschreven gegevens van de cliënt. Bovendien mogen alleen instellingen die een verzoek doen en een verzoek ontvangen gegevens uitwisselen. Een gezamenlijk register dient aan deze voorwaarden van de verplichting te voldoen en moet met inachtneming van deze grenzen ingericht worden. De verplichting vormt geen grondslag voor een algemene database met informatie over cliënten waar elke instelling met toegang vrijelijk gegevens uit kan opvragen.

§ 2.2.2. Gezamenlijke transactiemonitoring door banken

Op grond van de Wwft hebben banken de plicht om de transacties van hun cliënten te monitoren. Het doel hiervan is tweeledig. Ten eerste faciliteert het monitoren van transacties banken in hun taak als poortwachters van het financiële stelsel. Zij dienen het gebruik van het financiële stelsel voor witwassen of financieren van terrorisme te voorkomen door de risico's van hun cliënten te mitigeren. Het monitoren van de transacties en identificeren van ongebruikelijke transacties stelt banken in staat te beoordelen of de getroffen maatregelen in afdoende mate de risico's van hun cliënten mitigeren. Ten tweede faciliteert het monitoren van transacties en het melden van ongebruikelijke transacties onderzoeken door diverse (bijzondere) opsporingsinstanties en inlichtingen- en veiligheidsdiensten. De FIU-Nederland analyseert de gemelde ongebruikelijke transacties in samenhang met andere informatie om te bezien of deze gegevens van belang kunnen zijn voor het voorkomen en opsporen van misdrijven. Hierbij bepaalt de FIU-Nederland of transacties als verdacht moeten worden aangemerkt. De verdachte transacties worden vervolgens verstrekt aan de hiervoor genoemde autoriteiten.

Banken monitoren op basis van de huidige wet- en regelgeving de transacties van hun cliënten teneinde zich ervan te verzekeren dat de transacties voldoen aan het risicoprofiel van de cliënt dat door de bank is opgesteld of dat er geen indicatoren aanwezig zijn die kunnen duiden op vermoedens van witwassen of financieren van terrorisme. Op dit moment verrichten banken deze monitoring individueel en baseren zich hierbij voornamelijk op hun eigen en openbare informatie. Deze vorm van transactiemonitoring biedt criminelen de kans om onder de radar te blijven door transacties via verschillende partijen en verschillende banken te laten lopen. Door een groot netwerk te creëren, waarbij het criminele geld doelbewust middels een veelvoud van verschillende transacties via verschillende instellingen wordt geleid, verkleinen criminelen de kans dat een individuele bank in staat zal zijn om de ongebruikelijkheid van de transactie vast te stellen. Een bank heeft immers slechts het deel van het netwerk in beeld dat via de eigen bank is gelopen.

Om te onderzoeken of deze beperking aan het individueel monitoren van transacties opgelost zou kunnen worden, heeft een vijftal banken in 2018 een pilot uitgevoerd, waarbij de transacties van een geselecteerde groep van midden- en kleinbedrijven gezamenlijk is gemonitord.[11] De Nederlandse Vereniging van Banken (NVB) geeft aan dat uit deze pilot naar voren kwam dat gezamenlijke transactiemonitoring leidt tot meer en

[11] Persbericht NVB, *Nederlandse banken bundelen krachten tegen witwassen*, 13 september 2019.

nauwkeuriger detectie dan individuele transactiemonitoring.[12] Doordat bij gezamenlijke transactiemonitoring vaker informatie beschikbaar is over beide partijen in transacties, is meer detectie te bereiken dan bij monitoring van individuele transactiemonitoring. Daarnaast werden in de pilot cases zichtbaar die individuele banken niet hadden kunnen identificeren, omdat niet de volledige context zichtbaar is voor de individuele bank. Bovendien liet een steekproef zien dat de onderzoekswaardigheid van alerts bij gezamenlijke transactiemonitoring hoger bleek dan bij individuele transactiemonitoring. Zodoende was een van de conclusies van de banken dat gezamenlijke transactiemonitoring leidt tot meer, nieuwe en unieke detectie van cases. Bovendien leidt het tot scherpere detectie, omdat het leidt tot minder vals-positieve resultaten. De NVB geeft aan dat dit beeld wordt bevestigd door de eerste uitkomsten van de testfase van Transactie Monitoring Nederland (TMNL)[13]. Ook hieruit blijkt dat TMNL met diverse netwerken kan detecteren die mogelijk als ongebruikelijke transactie(s) kunnen worden aangemerkt en die voor individuele banken niet of niet in het geheel zichtbaar zijn.

Daarnaast hebben de FIU-Nederland en TMNL binnen de Fintell Alliance[14] in 2021 een pilot gedaan om ondergrondse banknetwerken te identificeren. De FIU-Nederland en de NVB geven aan dat hierbij binnen TMNL een model is ontworpen op basis van risico-indicatoren die zijn opgesteld aan de hand van informatie van de FIU-Nederland. Met dit model konden bedrijven worden geïdentificeerd die mogelijk betrokken waren bij ondergronds bankieren. De transacties zijn als alerts aangeleverd bij individuele banken, die de alerts nader hebben onderzocht en, zo nodig, als ongebruikelijke transactie gemeld aan de FIU-Nederland. De FIU-Nederland en NVB geven aan dat bijna 95% van deze circa 275 alerts onderzoekswaardig bleek te zijn.

Het blijkt zodoende dat als banken transacties gezamenlijk monitoren in plaats van individueel dit een positief effect heeft op de effectiviteit van de monitoring. Ongebruikelijke transacties worden vaker en eerder ontdekt, doordat het samenvoegen van de informatie van de verschillende banken leidt tot een breder en beter beeld van criminele netwerken. Dit maakt het moeilijker voor criminelen om de monitoring van banken te omzeilen door transacties via verschillende banken laten lopen. Bovendien kan de publiek-private samenwerking tussen de FIU-Nederland en de banken effectiever worden ingericht, doordat er een feedbackloop ontstaat.

De Financial Action Task Force (FATF)[15] onderkent deze notie. In een verkenning naar het combineren van data[16] komt de FATF tot de conclusie dat het combineren en gezamenlijk analyseren van gegevens het potentieel heeft om financiële instellingen beter in staat te stellen om risico's te begrijpen, beoordelen en te mitigeren. Dit wordt ondersteund

---

[12] De NVB maakt hierbij de kanttekening dat de onderzoeksresultaten niet één op één vergelijkbaar zijn met statistieken van individuele transactiemonitoring, aangezien de pilot specifiek gericht is op gezamenlijke transactiemonitoring, waarmee inzichten worden opgedaan die voor individuele banken niet zichtbaar kunnen zijn.

[13] https://tmnl.nl/.

[14] Een publiek-privaat samenwerkingsverband tussen de FIU-Nederland en de vier grootbanken, gericht op het uitwisselen van kennis en het versterken van de effectiviteit van het melden van ongebruikelijke transacties.

[15] De Financial Action Task Force is een onafhankelijk intergouvernementeel orgaan dat beleid ontwikkelt en bevordert ter bescherming van het mondiale financiële systeem tegen het witwassen van geld, de financiering van terrorisme en de financiering van massavernietigingswapens. De FATF heeft zogenaamde aanbevelingen (recommendations) ontwikkeld, die worden erkend als internationale norm voor de bestrijding van witwassen en de financiering van terrorisme en proliferatie. De landen die lid zijn van FATF worden op basis van deze aanbevelingen geëvalueerd.

[16] FATF/OECD, Stocktake on data pooling, collaborative analytics and data protection, 2021.

door de voortschrijdende technologie waarmee dit proces kan plaatsvinden met adequate waarborgen voor gegevensbescherming. In een recent rapport onderschrijft de FATF bovendien dat criminelen gebruik maken van de beperkingen van individuele financiële instellingen om de gehele puzzel te zien en het belang van gezamenlijke analyse en het bijeen brengen van data om dit tegen te gaan.[17]

Het gezamenlijk monitoren van transacties door banken biedt zodoende een oplossing voor een beperking die inherent is aan het individueel monitoren van transacties en biedt banken de mogelijkheid om meer ongebruikelijke transactiepatronen in beeld te krijgen. Daarom wordt met dit wetsvoorstel een grondslag opgenomen in de Wwft voor banken om een gezamenlijke voorziening in te richten ten behoeve van de verplichting om transacties te monitoren. In deze voorziening kunnen de transactiegegevens van cliënten van de individuele banken worden gecombineerd en in samenhang worden gemonitord. Hierbij worden de transactiegegevens in samenhang geanalyseerd en kunnen er alerts[18] worden vastgesteld. Indien binnen de gezamenlijke voorziening wordt vastgesteld dat er sprake is van een alert bij een specifieke (serie van) transactie(s), worden de banken die betrokken zijn bij deze specifieke (serie van) transactie(s) hierover geïnformeerd. Deze banken kunnen vervolgens de alert verder onderzoeken, mede op basis van andere informatie over de cliënt, om vast te stellen of er daadwerkelijk sprake is van een ongebruikelijke transactie. Dit laatste gebeurt buiten de gezamenlijke voorziening om, omdat anders niet alleen de transactiegegevens van cliënten, maar ook alle informatie die individuele banken over hun cliënten bijhouden in de gezamenlijke transactievoorziening opgenomen zou moeten worden. Dit laatste is niet proportioneel. Bovendien is het ook niet noodzakelijk, omdat de bij de transactie(s) betrokken banken – als er eenmaal een alert is gegenereerd – deze gezamenlijk kunnen onderzoeken buiten de gezamenlijke voorziening om. Dit onderzoek kan leiden tot de conclusie dat de banken nadere maatregelen dienen te treffen om de risico's van de desbetreffende client te mitigeren en indien er sprake is van een ongebruikelijke transactie deze te melden bij de FIU-Nederland. Dit laatste dienen de betrokken banken zelfstandig te doen.

Ten slotte is van belang om te vermelden dat hoewel het gezamenlijk monitoren van transacties tegemoet komt aan een beperking die inherent is aan het individueel monitoren van transacties en die tot een meer effectieve aanpak van witwassen en financieren van terrorisme zal leiden, het ook een meer verdergaande verwerking van gegevens door banken dan bij individuele transactiemonitoring met zich meebrengt. Bij de vormgeving van de grondslag is daarom uitdrukkelijk aandacht besteed aan afwegingen van proportionaliteit en evenredigheid die hebben geleid tot beperking van de grondslag en de introductie van extra privacy waarborgen. Hier zal in paragraaf 3.2 nader op worden ingegaan. Hiermee is een goede balans getroffen tussen een effectieve aanpak van witwassen en financieren van terrorisme en de privacy van burgers.

§ 2.2.2.1 Uitbesteding

Naast het introduceren van een wettelijke grondslag voor gezamenlijke transactiemonitoring door banken, wordt met dit wetsvoorstel ook een wettelijke belemmering weggenomen. De gezamenlijke voorziening waarin de banken de gegevens delen dient weliswaar door de banken opgezet te zijn, maar heeft ook een aparte rechtspersoonlijkheid. Om

[17] FATF, Data protection, technology and private sector information sharing, 2022.
[18] Alerts zijn indicaties dat er mogelijk sprake is van een ongebruikelijke transactie die op grond van artikel 16, eerste lid, van de Wwft gemeld moet worden aan de FIU-Nederland.

mogelijk te maken dat het monitoren van transacties binnen de gezamenlijke voorziening plaats vindt, dient mogelijk gemaakt te worden dat banken het monitoren van transacties kunnen uitbesteden aan de gezamenlijke voorziening. Ook hierin voorziet het wetsvoorstel. Van belang is hierbij te benadrukken dat het hierbij uitsluitend gaat om de uitbesteding van het genereren van alerts. De opvolging van deze alerts kan niet worden uitbesteed aan de gezamenlijke voorziening. Dat betekent dat de banken zelf dienen te onderzoeken of de transactie ongebruikelijk is. Als dit het geval blijkt te zijn, ligt de verantwoordelijkheid bij de individuele bank die bij de transactie betrokken is om het opleggen van nadere mitigerende maatregelen te overwegen en een melding van een ongebruikelijke transactie te doen bij de FIU-Nederland.

Het feit dat de huidige Wwft het uitbesteden van het monitoren van transacties niet toestaat, volgt niet uit de (gewijzigde) vierde anti-witwasrichtlijn. De richtlijn laat ruimte voor deze vorm van uitbesteding en stelt alleen regels over het kunnen afgaan op cliëntenonderzoeken die zijn verricht door een derde. De richtlijn geeft daarbij expliciet aan dat die regels geen verband houden met uitbesteding.[19] Bij uitbesteding blijft de verantwoordelijkheid immers bij de uitbestedende instelling liggen. Alles wat de derde partij doet, doet deze namens de instelling. Hierbij is het van belang om te onderstrepen dat bij uitbesteding de banken altijd zelf verantwoordelijk blijven voor de naleving van de op hen rustende wettelijke verplichtingen. Een bank kan zodoende te allen tijde aangesproken worden, door bijvoorbeeld de toezichthouder, als de derde aan wie de uitvoering is uitbesteed, niet voldoet aan de verplichtingen van de wet.

§ 2.2.2.2 Gebruik burgerservicenummer

Om transacties in een gezamenlijke voorziening te kunnen monitoren is het noodzakelijk dat zekerheid bestaat over de persoon die de transactie verricht. De Nederlandse banken hebben gezamenlijk 35 miljoen cliënten, waarvan 31 miljoen retailcliënten, die over één of meer (al dan niet aan elkaar gekoppelde) rekeningen beschikken. De NVB geeft aan dat er 12 miljard transacties plaats hebben gevonden in 2021 bij Nederlandse banken. Elke bank kent een eigen administratiesysteem van cliënten. Er zijn geen unieke nummers die uniform door de banken gebruikt worden waaruit de identiteit van een cliënt overkoepelend kan worden afgeleid.

Voor een effectieve werking van de monitoring in een gezamenlijke voorziening is het noodzakelijk dat unieke nummers aan een cliënt gekoppeld kunnen worden. Het ontbreken van een overkoepelend uniek nummer leidt ertoe dat aan elke transactie een groot aantal persoonsgegevens zou moeten worden verbonden om vast te stellen dat verschillende transacties van verschillende banken bij dezelfde cliënt horen. Hoewel het op voorhand onmogelijk is om aan te tonen in hoeveel van de gevallen het niet mogelijk zal zijn om een cliënt te identificeren, zonder gebruik van een uniek nummer, zijn er meerdere redenen om aan te nemen dat dit om een substantieel aantal zal gaan. Ten eerste zijn initialen en achternaam onvoldoende onderscheidend. Ook in combinatie met woonadres en/of geboortedatum is nog steeds niet in alle gevallen te bepalen of het dezelfde persoon betreft. Ten tweede is er een verscheidenheid aan registraties bij deze gegevens. Zo is de schrijfwijze van namen niet altijd uniform, zeker als het buitenlandse namen betreft. Ook wisselen namen van dezelfde personen, bijvoorbeeld doordat zij in het huwelijk treden. Bij de ene bank kan daardoor dezelfde persoon onder een andere naam zijn geregistreerd als bij een andere bank. Verder zijn

[19] Zie artikel 29 van de vierde anti-witwasrichtlijn.

woonadressen niet altijd gelijk bij dezelfde personen. Ten derde bestaat er in algemene zin bij de invoer van gegevens altijd een bepaalde foutmarge. Bij het combineren van gegevens neemt deze marge aanzienlijk toe naarmate meer gegevens nodig zijn om vast te stellen of sprake is van dezelfde persoon.

Het ontbreken van een uniek nummer en het als gevolg daarvan niet met zekerheid kunnen vaststellen of sprake is van dezelfde cliënt, leidt op meerdere vlakken tot problemen.
Allereest zorgt dit voor een minder effectieve monitoring van transacties. Transacties zullen onterecht als ongebruikelijk worden aangemerkt doordat verschillende personen als dezelfde persoon worden aangezien *(false positives)*. Andersom zullen transacties onterecht als gebruikelijk worden aangemerkt omdat het niet duidelijk is dat het om dezelfde persoon gaat *(false negatives)*. De verwachting is dat zonder toepassing van een uniek nummer er een aanzienlijke uitval zal zijn in vergelijking met gecombineerde transactiemonitoring waarbij wel een uniek nummer wordt gebruikt.

Ten tweede kan het vaststellen of sprake is van dezelfde cliënt, zonder gebruik van een uniek nummer, ertoe leiden dat er onevenredig veel persoonsgegevens verwerkt moeten worden. Bovendien wordt hierdoor de foutmarge vergroot, aangezien de hiervoor genoemde problematiek van een verscheidenheid aan registraties hierdoor wordt versterkt. Een uniek nummer verkleint deze foutmarge en maakt het mogelijk om minder persoonsgegevens te verwerken. Een uniek nummer is noodzakelijk voor de effectiviteit van het voorkomen en bestrijden van witwassen en financieren van terrorisme (doelbinding) en is in lijn met de principes van dataminimalisatie en juistheid van gegevensverwerking.

De hiervoor genoemde problemen kunnen op twee manieren worden ondervangen, namelijk door: i) banken gezamenlijk een uniek nummer te laten ontwikkelen of ii) wettelijk toe te staan dat banken het burgerservicenummer (BSN) mogen verwerken ten behoeve van het gezamenlijk monitoren van transacties. Beide mogelijkheden zijn tegen elkaar afgewogen. De conclusie is dat het gebruik van het BSN in dit geval de voorkeur verdient. Daar liggen diverse redenen aan ten grondslag. Zo is onderzocht of banken zelf tot een uniek nummer zouden kunnen komen. De set van gegevens die hiervoor nodig is en de beheerfaciliteit daarachter zou echter voor een onevenredige verwerking van persoonsgegevens zorgen. Daarnaast zou hier een grote kosteninvestering mee gemoeid zijn. Tegelijkertijd beschikken banken meestal al over het unieke BSN van cliënten. Dit nummer zijn zij ook verplicht te gebruiken voor het verrichten van specifieke wettelijke taken, indien ze over het BSN beschikken. Het gaat dan om taken in het kader van de uitvoering van fiscale wetten (renseignering), het Deposito Garantiestelsel en het Verwijzingsportaal bankgegevens. Bovendien speelt mee dat banken ervaring hebben met het gebruik van het BSN en over vereiste waarborgen beschikken om de bescherming van de gegevens te verzekeren. Ook is van belang dat banken een vergunning hebben op grond van de Wet financieel toezicht (Wft), aan strenge eisen ten aanzien van de bedrijfsvoering (waaronder beveiligingseisen) moeten voldoen en onder doorlopend toezicht van De Nederlandsche Bank (DNB) staan.

Gezien het bovenstaande wordt geregeld dat banken die in het kader van transactiemonitoring binnen een gezamenlijke voorziening transacties delen, voor dat doel het BSN mogen gebruiken, indien zij daar reeds over beschikken. Op grond van artikel 34b, zesde lid, onder a, dient het BSN gepseudonimiseerd en versleuteld te worden.

§ 2.3 Verduidelijking gebruik bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard

Bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard zijn in bepaalde gevallen onlosmakelijk verbonden met een cliënt of transactie. Instellingen hebben op grond van de Wwft de wettelijke verplichting tot het uitvoeren van taken waarvoor die gegevens in bepaalde gevallen zeer relevant zijn omdat deze een indicatie op witwassen of het financieren van terrorisme vormen. In deze paragraaf wordt dit nader uiteengezet middels enkele concrete voorbeelden. De Wwft laat zich op dit moment niet expliciet uit over de mogelijkheid van gebruik van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard in het kader van de wettelijke taken van de Wwft. Mede naar aanleiding van het advies van de Autoriteit Persoonsgegevens (AP) inzake een concept van dit wetsvoorstel (zie paragraaf 3.4.1 van deze toelichting), is gebleken dat er onduidelijkheid bestaat over het gebruik van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard in het kader van de verplichtingen die voortvloeien uit de Wwft. Op grond van de artikelen 9 en 10 van de AVG is verwerking van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard verboden, tenzij sprake is van een in dat artikel genoemde uitzondering. Bij bijzondere categorieën van persoonsgegevens is dat onder meer het geval als sprake is van een zwaarwegend algemeen belang (artikel 9, tweede lid, onderdeel g, van de AVG). Dit is aan de orde bij het voorkomen van witwassen en financieren van terrorisme. Op grond van artikel 10 van de AVG mogen persoonsgegevens van strafrechtelijke aard alleen worden verwerkt als aan in dat artikel genoemde voorwaarden wordt voldaan. Om de onduidelijkheid over het verwerken van deze persoonsgegevens zowel voor de betrokkenen als voor de verwerkers weg te nemen, is in onderhavig wetsvoorstel een specifieke grondslag opgenomen voor de verwerking van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard voor zover dat noodzakelijk is voor de uitvoering van de wettelijke taken die voortvloeien uit de Wwft. Voor alle gegevens verzameld in het kader van de wettelijke taken in de Wwft geldt dat deze niet voor een ander doel gebruikt mogen worden.

§ 2.3.1 Verplichtingen voor instellingen op grond van de Wwft

De Wwft bevat twee hoofdverplichtingen: het uitvoeren van cliëntenonderzoek en melden van ongebruikelijke transacties. Met deze wijziging wordt beoogd om onduidelijkheid over de mogelijkheid van verwerking van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard ten aanzien van deze hoofdverplichtingen weg te nemen. Om witwassen en financieren van terrorisme te voorkomen, dienen instellingen op grond van artikel 3, eerste lid, van de Wwft, cliëntenonderzoek te verrichten. Dit onderzoek dient de instelling bijvoorbeeld in staat te stellen om de cliënt te identificeren en de identiteit te verifiëren (artikel 3, tweede lid, onder a, van de Wwft) en de aard en het beoogde doel van de zakelijke relatie vast te stellen (artikel 3, tweede lid, onder c, van de Wwft). Daarnaast dient een instelling een voortdurende controle uit te oefenen op de zakelijke relatie en de tijdens de duur van deze relatie verrichte transacties, om te verzekeren dat deze overeenkomen met de kennis die de instelling heeft van de cliënt en diens risicoprofiel (artikel 3, tweede lid, onder d, van de Wwft). Vervolgens bepaalt de instelling op basis van ten minste de risicofactoren die zijn vastgelegd in de anti-witwasrichtlijn of de zakelijke relatie of transactie naar haar aard een laag (artikel 6 van de Wwft) dan wel een hoog (artikel 8 en artikel 9 van de Wwft) risico op witwassen of financieren van terrorisme met zich meebrengt. In het eerste geval kan volstaan worden met

een vereenvoudigd cliëntenonderzoek, terwijl in het tweede geval een instelling een verscherpt cliëntenonderzoek dient uit te voeren. Bij een vereenvoudigd cliëntenonderzoek dient de instelling aantoonbaar voldoende gegevens te verzamelen om vast te kunnen stellen of er inderdaad sprake is van een laag risico (artikel 6, tweede lid, van de Wwft), dient de instelling redelijke maatregelen te nemen om ervoor te zorgen dat de gegevens actueel worden gehouden (artikel 6, derde lid, van de Wwft) en dient de instelling zorg te dragen voor een toereikende controle van de transacties of de zakelijke relatie om te verzekeren dat kan worden voldaan aan de verplichting om ongebruikelijke transacties te melden aan de FIU-Nederland (artikel 6, vierde lid, van de Wwft). Bij een verscherpt cliëntenonderzoek dient de instelling diepgaander onderzoek te doen naar de zakelijke relatie of transactie door een scala aan aanvullende cliëntenonderzoeksmaatregelen te nemen (artikel 8 en 9 van de Wwft). Een verrichte of voorgenomen ongebruikelijke transactie dient de instelling op grond van artikel 16, eerste lid, van de Wwft, te melden aan de FIU-Nederland. Het cliëntenonderzoek is zodoende essentieel voor de beoordeling van de instelling of de diensten van de instelling niet worden gebruikt voor witwassen of financieren van terrorisme en om te oordelen over voortzetting van de zakelijke relatie of het melden van een ongebruikelijke transactie en vormt zodoende een cruciaal onderdeel van het voorkomen van het gebruik van het financieel stelsel voor witwassen en financieren van terrorisme.

§ 2.3.2 Samenhang verplichtingen met de verwerking van persoonsgegevens

Afhankelijk van de omstandigheden van de cliënt, de diensten die de cliënt afneemt en de transacties die de cliënt verricht, kunnen bij het cliëntenonderzoek bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard betrokken zijn. Daar waar dit noodzakelijk is voor het uitvoeren van hun wettelijke taak tot het verrichten van cliëntenonderzoek en het melden van ongebruikelijke transacties, dienen instellingen bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard te kunnen verwerken om aan hun verplichtingen te kunnen voldoen. Het verwerken van deze persoonsgegevens kan zowel aan de orde zijn bij het bijhouden van de verrichte transactie(s), alsook bij het betrekken van deze gegevens bij de risicobeoordeling en de beoordeling van de ongebruikelijkheid van een transactie. Instellingen dienen het doel van de zakelijke relatie of de uiteindelijke belanghebbende (UBO) vast te stellen. Bij het voldoen aan deze verplichtingen kunnen bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard verwerkt worden. Het voldoen aan de verplichting om transacties te monitoren houdt eveneens reeds meerdere vormen van verwerking in. Een instelling moet daarvoor onder meer de transacties verzamelen, opslaan, ordenen en, indien daar aanleiding voor is, raadplegen. Voor de vaststelling dat een transactie ongebruikelijk is, is het raadplegen van (eventuele) eerder verrichte transacties door een cliënt kortom essentieel. Bovendien is, zoals hierboven beschreven, het uitoefenen van een voortdurende controle op de zakelijke relatie en de tijdens de duur van deze relatie verrichte transacties een onderdeel van het cliëntenonderzoek. Om te kunnen beoordelen of een transactie voor een bepaalde cliënt past in diens risicoprofiel en als gebruikelijk dan wel ongebruikelijk aangemerkt moet worden, dient de transactie afgezet te kunnen worden tegen de activiteiten van de cliënt en de producten of diensten die de cliënt afneemt, alsook tegen het leveringskanaal en landen en geografische gebieden. Om dit volledig en adequaat te kunnen doen zijn alle gegevens die onderdeel uitmaken van een transactie relevant, alsmede de gegevens die van belang zijn om een risicoprofiel van de cliënt te bepalen.

§ 2.3.3. Voorbeelden van verplichte verwerking van bijzondere categorieën persoonsgegevens

Door de aard van de verplichtingen uit de Wwft geldt dat verwerking van alle bijzondere categorieën van persoonsgegevens aan de orde kan zijn; op voorhand is immers niet uit te sluiten dat deze gegevens onderdeel uitmaken van de informatie in een transactie of bij vastlegging van andere onderdelen van het cliëntenonderzoek. Voorbeelden van bijzondere categorieën van persoonsgegevens zijn gegevens over politieke opvattingen, godsdienst of levensovertuiging, lidmaatschap van een vakbond, gezondheid of het seksuele leven. Op grond van de verplichtingen uit de Wwft zijn instellingen verplicht informatie vast te leggen die dergelijke gegevens kunnen bevatten. Dat wil niet zeggen dat instellingen gericht bijzondere categorieën van persoonsgegevens verwerken. Al deze gegevens kunnen uiteindelijk wel relevant zijn in het kader van cliëntenonderzoek of het melden van ongebruikelijke transacties. Transacties zoals contributies voor het lidmaatschap van of donaties aan een politieke partij of een organisatie van levensbeschouwelijke of religieuze aard bevatten bijvoorbeeld bijzondere categorieën van persoonsgegevens. Het uitvoeren, vastleggen en opslaan van een dergelijke transactie is reeds verwerking van bijzondere categorieën van persoonsgegeven en is vereist om aan de Wwft te voldoen. Voor gegevens met betrekking tot lidmaatschap van een vakbond of gezondheid spelen vergelijkbare aspecten. Zo heeft de FIU-Nederland in 2018 1.300 meldingen van ongebruikelijke transacties ontvangen die te relateren waren aan zorgfraude. Hierin zag de FIU-Nederland aanleiding om hier nadrukkelijk verder in te investeren.[20] Ook in 2019 zag de FIU-Nederland dat een deel van de ongebruikelijke transacties gerelateerd aan zorgfraude, mogelijk te maken had met terrorisme financiering, hoewel dit verhoudingsgewijs wel is gedaald in vergelijking met het voorgaande jaar.[21] In een dergelijk geval kunnen transacties die medische gegevens bevatten relevant zijn bij de vaststelling dat een transactie als ongebruikelijk dient te worden beschouwd. Op dezelfde manier kan een transactie verricht in een seksclub gegevens bevatten over het seksuele gedrag of gerichtheid van een cliënt. Hoewel dergelijke informatie op zichzelf geen aanleiding geeft tot nader onderzoek, kan uit een dergelijke transactie, indien in samenhang bezien met andere risicofactoren, een ongebruikelijk transactiepatroon naar voren komen dat een indicatie kan zijn voor witwassen. Ook kunnen persoonsgegevens waar religieuze of levensbeschouwelijke overtuigingen uit blijken, een rol spelen bij de beoordeling van transacties in het kader van financieren van terrorisme, wanneer bijvoorbeeld donaties worden gedaan aan religieuze instellingen in het buitenland of radicale groeperingen. De instelling die het verzoek krijgt dergelijke transactie uit te voeren moet in staat zijn deze transactie te beoordelen, hetgeen verwerking inhoudt. Daarnaast zijn instellingen altijd verplicht om een cliënt te identificeren en doen dit middels een afschrift van een identiteitsbewijs. Het vastleggen van dit afschrift komt reeds neer op het verwerken van persoonsgegevens waaruit iemands ras of etnische afkomst kan worden afgeleid. Dit is ook het geval bij het vastleggen van camerabeelden bij pintransactie bij geldautomaten. Hierbij kan sprake zijn van verwerking van biometrische persoonsgegevens, zoals gezichtsafbeeldingen. Voorts dient een instelling de aard en het doel van een zakelijke relatie vast te stellen. In het geval dat de zakelijke relatie samenhangt met bijzondere categorieën van persoonsgegevens kan deze verplichting neerkomen op de verwerking van dergelijke gegevens. Bijvoorbeeld de oprichting van een specifieke rechtspersoon, zoals een vakbond, door een notaris. Een instelling is eveneens verplicht de

[20] Financial Intelligence Unit-Nederland, Jaaroverzicht 2018.
[21] Financial Intelligence Unit-Nederland, Jaaroverzicht 2019.

uiteindelijke belanghebbende te vast te stellen indien de cliënt een rechtspersoon is. In het geval van een religieuze of levensbeschouwelijke organisatie kan het feit dat een persoon geïdentificeerd is als UBO van deze organisatie duiden op de religie of levensbeschouwing van deze persoon. Daarnaast dienen instellingen te bepalen of een persoon een politiek prominente functie bekleedt, zowel voor een binnenlandse of buitenlandse functie.

Daarnaast is van belang om op te merken dat elke juridische entiteit of constructie misbruikt kan worden voor witwassen of financieren van terrorisme en dat transacties zo vorm gegeven kunnen worden, bijvoorbeeld door het gebruik van bijzondere categorieën van persoonsgegevens, dat de herkomst van middelen wordt verhuld. Het niet kunnen betrekken van bijzondere categorieën van persoonsgegevens bij het cliëntenonderzoek zou derhalve leiden tot een beperkte blik op de cliënt en juist openingen bieden voor criminelen om witwassen of financieren van terrorisme buiten beeld te houden.

§ 2.3.4 Persoonsgegevens van strafrechtelijke aard

Voor persoonsgegevens van strafrechtelijke aard geldt dat instellingen in de regel zeer beperkt over deze gegevens beschikken. Een melding van een ongebruikelijke transactie alsook de informatie dat een dergelijke transactie als verdacht is aangemerkt, worden niet aangemerkt als een persoonsgegeven van strafrechtelijke aard, omdat het geen verdenking in de zin van artikel 27 van het Wetboek van Strafvordering betreft. Dit neemt niet weg dat ook een instelling de beschikking kan hebben over dergelijke gegevens. Zo kan een instelling in het verleden een aangifte hebben gedaan tegen een cliënt. Het ligt voor de hand om dit gegeven ook vast te leggen. Hiermee verwerkt een instelling een gegeven van strafrechtelijke aard. Ook dienen instellingen onderzoek te doen naar cliënten door middel van openbare bronnen. Uit deze openbare bronnen kunnen veroordelingen naar voren komen. Waar deze informatie relevant is voor het onderzoek naar de risico's op witwassen en financieren van terrorisme van een cliënt, dient de instelling deze hierbij te kunnen betrekken.

Voorts dient opgemerkt te worden dat hoewel de bevoegdheid om bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard te verwerken in principe voor alle instellingen geldt, er een groot verschil is tussen de instellingen in de mate waarin zij de beschikking hebben over deze gegevens. Waar in gegevens van transacties die door banken afgehandeld worden veelvuldig dit soort gegevens voorkomt, zal een makelaar of belastingadviseur er minder snel mee in aanraking komen. Dit neemt echter niet weg dat, als een makelaar bijvoorbeeld ontdekt dat een cliënt in het verleden is veroordeeld voor een financieel misdrijf, deze informatie onmisbaar is bij het opstellen van een risicoprofiel van deze cliënt. Omdat op voorhand niet te bepalen is welke bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard voor welke instellingen noodzakelijk kunnen zijn bij de uitvoering van hun wettelijke taken, is voorzien in een wettelijke grondslag voor alle instellingen voor het verwerken van dit soort gegevens.

§ 2.3.5 Alleen indien noodzakelijk

Tot slot is van belang te herhalen dat de verwerking alleen toegestaan is indien dit noodzakelijk is om aan de verplichtingen uit de Wwft te voldoen. Het is instellingen niet toegestaan om bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard

verkregen uit basale handelingen, zoals het opslaan van een afschrift van een identiteitsbewijs of het vastleggen van transacties, verder te verwerken zolang dit niet voortvloeit uit de verplichting uit de Wwft. Voor alle gegevens verzameld in het kader van de wettelijke taken in de Wwft geldt dat deze niet voor een ander doel gebruikt mogen worden. Om dit onderdeel van de verwerkingsgrondslag te borgen zijn waarborgen opgenomen. Allereerst dient een instelling te documenteren welke bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard verwerkt worden en waarom deze verwerking noodzakelijk is om aan de verplichting te voldoen. Ten tweede dient de instelling zijn cliënten te informeren over zijn beleid ten aanzien van de eventuele verwerking van bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard. De instelling kan daarbij verwijzen naar de eerder beschreven documentatie. Hier wordt nader op ingegaan in de artikelsgewijze toelichting bij onderdeel I.

Ten overvloede zij opgemerkt dat deze bepaling geen grondslag vormt voor geautomatiseerde besluitvorming in de zin van artikel 22, eerste lid, van de AVG op grond van het profiel van een cliënt. In een dergelijke grondslag wordt niet voorzien in de Wwft.

§ 3. Gegevensbescherming

In deze paragraaf wordt ingegaan op aspecten van gegevensbescherming ten aanzien van de hierboven beschreven maatregelen. Het verbod op contante betalingen vanaf € 3.000 wordt hier buiten beschouwing gelaten, aangezien gegevensbescherming ten aanzien van dit onderdeel niet relevant is, omdat er geen sprake is van verwerking van persoonsgegevens.

Informatie over de cliënt en transactiegegevens zijn persoonsgegevens in de zin van de AVG. Onder een persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare persoon.[22] Op de verwerking van persoonsgegevens is de AVG van toepassing. Omdat de voorgestelde maatregelen, op het verbod op contante betalingen vanaf € 3.000, betrekking hebben op de verwerking van persoonsgegevens, wordt hierna op de toepasselijke privacyregelgeving ingegaan en is de AP op grond van artikel 36, vierde lid, AVG gevraagd te adviseren over een concept van dit wetsvoorstel en separaat over onder meer het gebruik van het BSN door Wwft-instellingen. Op dit advies wordt in paragraaf 3.3 ingegaan. Op de verwerking van persoonsgegevens 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 de fundamentele vrijheden en artikel 10 van de Grondwet van toepassing. Op grond van deze bepalingen bestaat een recht op bescherming van persoonsgegevens. Het recht op bescherming van persoonsgegevens is echter geen absoluut recht, onder bepaalde voorwaarden kan dit recht wordt aangetast. Dit wordt hieronder toegelicht.

De regels rond het recht op de bescherming van persoonsgegevens worden verder uitgewerkt in de AVG en in de Uitvoeringswet AVG (UAVG). Persoonsgegevens moeten op grond van deze wetgeving worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig,

[22] Zie artikel 4(1) AVG. Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

behoorlijk en transparant is. Verder 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. Ten slotte is specifiek op het gebruik van het BSN de Wet algemene bepalingen burgerservicenummer van toepassing.

§ 3.1. Gegevensbeschermingseffectbeoordeling gegevensdeling tussen instellingen bij cliëntenonderzoek

A. Verwerking van persoonsgegevens

Op grond van artikel 3 van de Wwft zijn instellingen, onder andere, verplicht om de cliënt te identificeren en diens identiteit te verifiëren, alsmede de uiteindelijk belanghebbende van de cliënt te identificeren en redelijke maatregelen te nemen om zijn identiteit te verifiëren. Daarnaast dienen instellingen het doel en de beoogde aard van de zakelijke relatie vast te stellen en een voortdurende controle op de zakelijke relatie met de cliënt en de tijdens de duur van deze relatie verrichte transacties uit te oefenen. Het doel hiervan is om te verzekeren dat deze transacties overeenkomen met de kennis die de instelling heeft van de cliënt en diens risicoprofiel. Zo nodig dient de instelling ook een onderzoek uit te voeren naar de bron van de middelen die bij de zakelijke relatie worden gebruikt. Al deze gegevens dienen te worden aangemerkt als persoonsgegevens, aangezien met deze gegevens een natuurlijke persoon direct of indirect kan worden geïdentificeerd. In artikel 33, tweede lid van de Wwft zijn de gegevens opgenomen die door instellingen bij het cliëntenonderzoek moeten worden vastgelegd. Dat zijn onder andere geslachtsnaam, voornamen, geboortedatum, adresgegevens, de aard, het nummer en de datum en plaats van uitgifte van het document met behulp waarvan de identiteit is geverifieerd. Voor vennootschappen of andere juridische entiteiten geldt dat, onder andere, de rechtsvorm, de statutaire naam en de handelsnaam dienen te worden vastgelegd.

Indien een instelling achterhaalt dat een andere instelling uit dezelfde categorie momenteel diensten verleent, heeft verleend of heeft geweigerd aan de cliënt, bestaat de verplichting om bij die andere instelling navraag te doen naar de gebleken risico's op witwassen of financieren van terrorisme. In dit geval zal de instelling de in artikel 33, tweede lid, onderdelen a en c, genoemde gegevens dienen te verstrekken om te verzekeren dat beide instellingen dezelfde cliënt voor ogen hebben en er geen gegevens gedeeld worden over een verkeerde cliënt. De grondslag voor deze gegevensverstrekking is gelegen in de wettelijke verplichting om onderzoek te doen naar dienstverlening door andere instellingen uit dezelfde categorie.

Indien een instelling een dergelijk verzoek ontvangt ten aanzien van een cliënt waarbij deze risico's op witwassen en financieren van terrorisme en maatregelen om deze risico's te beperken heeft vastgesteld, dient de instelling de vragende instelling hierover te informeren. In algemene zin betreft dit informatie die heeft geleid tot de conclusie dat de handelingen van de cliënt niet passen binnen het risicoprofiel dat deze instelling heeft opgesteld van de cliënt. Dat kunnen «gewone» transactiegegevens zijn, zoals onverklaarbare (contante) stortingen op of onverklaarbare overboekingen van en naar de betaalrekening van de cliënt. Daarnaast kunnen het ook persoonsgegevens van strafrechtelijke aard betreffen. Dit is het geval

als de instelling heeft achterhaald dat de cliënt strafrechtelijk is veroordeeld. Indien deze informatie deel uitmaakt van de bij de cliënt gebleken risico's op witwassen of financieren van terrorisme, dienen deze gegevens verstrekt te worden aan de instelling die hierom verzoekt.

B. Rechtmatigheid, noodzaak en evenredigheid gegevensverwerking

Hieronder wordt ingegaan op de rechtmatigheid, de noodzaak en de evenredigheid van de gegevensverwerking die plaatsvindt in het kader van de voorgestelde maatregel. Samengevat is de voorgestelde maatregel, te weten het delen van gebleken risico's op witwassen of financieren van terrorisme bij de cliënt, noodzakelijk voor het te bereiken doel, namelijk het voorkomen en bestrijden van witwassen en financieren van terrorisme. Daarbij is de verwerking van persoonsgegevens van strafrechtelijke aard, zoals een eerdere veroordeling voor witwassen of financieren van terrorisme, onmisbaar. De rechten van betrokkenen zijn geborgd. Een instelling is verantwoordelijk voor de verwerking van de persoonsgegevens van een cliënt. Een betrokkene kan zich daarom altijd wenden tot de instelling indien hij van mening is dat hem betreffende persoonsgegevens onrechtmatig worden verwerkt door de instelling. De gegevensdeling vindt alleen plaats in gevallen waarin er sprake is van (indicaties van) een hoger risico op witwassen of financieren van terrorisme en in principe uitsluitend tussen de instellingen die binnen dezelfde categorie vallen.

Het voorgestelde artikel regelt de bevoegdheid van instellingen om gegevens over gebleken risico's op witwassen en financieren van terrorisme van cliënten uit te wisselen met instellingen uit dezelfde categorie. Deze uitwisseling kan alleen plaatsvinden voor zover er sprake is van een zakelijke relatie of transactie die naar haar aard indicaties van een hoger risico op witwassen of financieren van terrorisme met zich meebrengt, er sprake is van de risicofactoren genoemd in bijlage III van vierde anti-witwasrichtlijn en in het kader van het verscherpt cliëntenonderzoek. Het doel van het cliëntenonderzoek is het voorkomen van witwassen en financieren van terrorisme. De voorgestelde maatregel is noodzakelijk voor dit doel, omdat instellingen bij aanvang van de dienstverlening ondanks een vergaande onderzoeksplicht niet altijd goed in staat zijn om een juist risicoprofiel van de cliënt op te stellen. Voor het vaststellen van de risico's is een instelling namelijk ook afhankelijk van informatie die door de cliënt wordt verstrekt. Criminelen spelen hierop in door bewust onvolledige of onjuiste informatie te verstrekken, die geen aanleiding geeft tot nader onderzoek. Dit leidt ertoe dat pas na verloop van tijd kan worden vastgesteld dat de handelingen van de cliënt niet passen binnen het risicoprofiel van de cliënt. In de tussentijd is de cliënt in staat de dienstverlening van de instelling – en daarmee het financiële stelsel – te misbruiken voor witwassen of financieren van terrorisme. Om dit effectief te voorkomen is het noodzakelijk dat deze informatie bij aanvang van de dienstverlening bekend is, zodat een juist risicoprofiel van de cliënt kan worden opgesteld en zodoende voorkomen kan worden dat de dienstverlening van instellingen door middel van shopgedrag tussen instellingen wordt gebruikt voor witwassen of financieren van terrorisme.

Er is voor gekozen om de uitwisseling van gegevens over gebleken risico's op witwassen of financieren van terrorisme te beperken tot die gevallen dat de zakelijke relatie of transactie naar haar aard een hoger risico met zich brengt, de risicofactoren bedoeld in bijlage III van de vierde anti-witwasrichtlijn van toepassing en als onderdeel van het verscherpt cliëntenonderzoek. Dit is een risico gebaseerde invulling van de maatregel, die aansluit op het systeem van de Wwft. De verplichting om navraag te doen geldt uitsluitend als sprake is van aanwijzingen voor een

hoger risico op witwassen of financieren van terrorisme. Om de gegevensuitwisseling te beperken tot het strikt noodzakelijke worden bij uitvoering van de verplichting alleen de voorgeschreven beperkte gegevens over de cliënt gedeeld. Hiervoor is aangesloten bij de gegevens voorgeschreven in artikel 33, tweede lid, onderdelen a en c van de wet. Deze twee onderdelen bevatten de gegevens die een instelling dient vast te leggen bij het cliëntenonderzoek van natuurlijke personen en rechtspersonen. Aansluiting bij artikel 33 is noodzakelijk op basis van twee redenen. Ten eerste wordt hiermee de set gegevens beperkt, instellingen verzamelen deze gegevens al in het kader van cliëntenonderzoek en zullen dus reeds aanwezig zijn bij zowel de verzoekende instelling als de instelling die het verzoek ontvangt. Ten tweede garandeert deze set gegevens dat beide instellingen met zekerheid kunnen vaststellen dat het om dezelfde cliënt gaat en wordt voorkomen dat er uitwisseling van de verkeerde cliënt plaatsvindt of onterecht geconstateerd wordt dat het niet dezelfde cliënt betreft.

Daarnaast wordt voorgesteld dat delen van gegevens alleen mogelijk is tussen instellingen die behoren tot dezelfde categorie. Hier is voor gekozen omdat instellingen uit dezelfde categorie over het algemeen soortgelijke producten of diensten aanbieden en daardoor ook te maken hebben met soortgelijke risico-inschattingen. Gegevensuitwisseling tussen deze instellingen zal zodoende het grootste effect sorteren. Hieruit blijkt ook de meerwaarde van deze maatregel ten opzichte van een stelsel van zwarte lijsten. Een zwarte lijst bevat namen van cliënten die geweigerd zijn of ten aanzien van wie de dienstverlening is stopgezet wegens ernstige gevallen van fraude, witwassen of financiering van terrorisme, en leent zich minder voor het opnemen van een uitgebreide, inhoudelijke motivering van de redenen waarom een cliënt op die lijst is geplaatst. Het is echter juist deze inhoudelijke motivering van de redenen die bijdraagt aan de proportionaliteit, aangezien een instelling daardoor accurater kan beoordelen of zij in staat is om de risico's te mitigeren. Dit leidt niet alleen tot het effectiever voorkomen van witwassen en financieren van terrorisme maar voorkomt ook dat instellingen ten onrechte dienstverlening weigeren aan cliënten.

Elke instelling is verplicht om, als verwerkingsverantwoordelijke in de zin van de AVG, haar cliënten te informeren over de verwerking van persoonsgegevens. Dit betekent dat ook informatie verstrekt moet worden over de verwerkingen die plaatsvinden in het kader van het uitwisselen van bij de cliënt gebleken risico's op witwassen of financieren van terrorisme. Welke informatie verstrekt moet worden dient opgenomen te worden in een privacyverklaring van de instelling. Ook kan een betrokkene de instelling verzoeken om inzage in de verwerking van de op hem betrekking hebbende persoonsgegevens.[23] Daarnaast hebben betrokkenen ook andere rechten, vermeld in hoofdstuk 2 van de AVG. Als een betrokkene van mening is dat een instelling in strijd met geldende wet- en regelgeving zijn persoonsgegevens verwerkt, kan hij een klacht indienen bij de AP.[24] Daarnaast kan een betrokkene in dat geval ook beroep instellen bij de rechter.[25]

Bij deze maatregel is steeds gekozen voor het minst vergaande alternatief. Allereerst door de deling van gegevens over gebleken risico's op witwassen en financieren van terrorisme te beperken tot die gevallen dat de zakelijke relatie of transactie naar haar aard een hoger risico op witwassen of financieren van terrorisme met zich brengt, de risicofactoren

[23] Artikel 15 AVG.
[24] Artikel 77 AVG.
[25] Artikel 79 AVG.

bedoeld in bijlage III van de vierde anti-witwasrichtlijn van toepassing en als onderdeel van het verscherpt cliëntenonderzoek en daadwerkelijk geleid hebben tot maatregelen om deze risico's te beperken. Het verdergaande alternatief zou zijn om de uitwisseling van deze gegevens niet alleen in gevallen van een hoger risico voor te schrijven, maar in alle gevallen wanneer er cliëntenonderzoek wordt verricht. Bij een hoger risico op witwassen of financieren van terrorisme is het des te meer van belang dat de afweging om aan die cliënt wel of geen dienstverlening aan te bieden wordt genomen op grond van alle informatie die daarover beschikbaar is. Ten tweede is voor het minst vergaande alternatief gekozen door alleen risico's uit te wisselen die tot concrete maatregelen hebben geleid om deze risico's te beperken, waaronder in ieder geval het beëindigen van de klantrelatie of weigeren van klant wordt verstaan. Op deze manier wordt reikwijdte van te delen risico's beperkt en gegarandeerd dat er niet willekeurige informatie wordt gedeeld. Ten derde is voor het minst vergaande alternatief gekozen door de uitwisseling van de gegevens te beperken tot instellingen behorend tot dezelfde categorie, in plaats van deze gegevensuitwisseling tussen alle instellingen mogelijk te maken. De reden hiervoor is dat er bij instellingen uit dezelfde categorie sprake is van soortgelijke dienstverlening, waardoor gegevensdeling tussen die instellingen het meest effectief zal zijn. Bovendien verklaart dit waarom niet kan worden volstaan met het alternatief van een stelsel met uitsluitend zwarte lijsten. Een dergelijk stelsel maakt het niet of slechts beperkt mogelijk om die achterliggende gebleken risico's op witwassen of financieren van terrorisme tussen instellingen te delen, terwijl juist die onderliggende motivering noodzakelijk is om een juiste inschatting te maken van deze risico's.

C. Risico's en maatregelen

In het kader van de poortwachtersfunctie die instellingen op grond van de Wwft hebben, dienen zij een inschatting te maken van het risico op witwassen of financieren van terrorisme bij het accepteren van een cliënt. Tegelijkertijd is het van belang dat cliënten niet onterecht uitgesloten worden van het financiële stelsel. Een risico van de uitbreiding van de mogelijkheid om gegevens te delen is dat het zou kunnen leiden tot meer onnodige uitsluiting van cliënten (ook bekend als *de-risking)* door instellingen. Ten aanzien van de gegevensuitwisseling tussen instellingen ten behoeve van het cliëntenonderzoek is het belangrijk om te benadrukken dat de instelling een individuele risicoafweging per cliënt dient te maken. De gegevens die een eerdere dienstverlener verstrekt dienen als een niet-bindende aanvulling op het cliëntenonderzoek en ontslaan de verzoekende instelling dus niet van de verplichting tot het maken van een eigen individuele risicoafweging en eventuele vaststelling van beheersmaatregelen.

Daarnaast zouden instellingen, om praktisch uitvoering te geven aan deze maatregel, vaker gebruik kunnen gaan maken van centrale registratiesystemen (ook wel bekend als zwarte lijsten). De maatregel zou mogelijk kunnen leiden tot een verhoging van het gebruik van centrale systemen binnen categorieën instellingen waarin risico's op witwassen en financieren van terrorisme van personen worden geregistreerd. Dit is in zichzelf niet een probleem, omdat dergelijke systemen kunnen bijdragen aan veilige en efficiënte gegevensuitwisseling. Dergelijke systemen kunnen bij verkeerd gebruik wel leiden tot onnodige uitsluiting van personen of onrechtmatige gegevensverwerking. Daarom is het gebruik van dergelijke systemen op grond van de AVG met waarborgen omkleed. Indien in deze systemen ook gegevens van strafrechtelijke aard worden verwerkt, is verkrijging van een vergunning van de AP noodzakelijk. Bovendien is in dit verband is het belangrijk te benadrukken dat het gebruik van dergelijke

registratiesystemen met waarborgen is omkleed om onterechte opname in het systeem te voorkomen. Ook kent het gebruik van dergelijke registratiesystemen rechten toe aan de personen die hierop staan, zoals het recht op rectificatie en het recht op vergetelheid. Ten slotte dient ook bij de inrichting en gebruik van dergelijke systeem gewaarborgd worden dat deze niet leiden tot gegevensverwerking buiten de voorwaarden van de verplichting, zoals beschreven in *paragraaf 2.2.1.5.*

§ 3.2 Gegevensbeschermingseffectbeoordeling gezamenlijke transactiemonitoring

A. Verwerking van persoonsgegevens

Het wetsvoorstel maakt mogelijk dat banken transactiegegevens van hun zakelijke en particuliere cliënten kunnen combineren binnen een gezamenlijke voorziening ten behoeve van gezamenlijke transactiemonitoring in het kader van de Wwft, voor zover deze transactiegegevens noodzakelijk zijn om gezamenlijk transacties te monitoren. Het derde lid van artikel 34b schrijft voor dat de transactiegegevens die gecombineerd mogen worden binnen de gezamenlijke voorziening voorgeschreven zullen worden bij algemene maatregel van bestuur en dat ze betrekking hebben op persoonsgegevens, transactie-informatie, productgegevens en door de bank reeds vastgestelde risico-indicatoren. Dergelijke transactiegegevens worden nu al gebruikt door banken om individueel transacties te monitoren. De transactiegegevens binnen de gezamenlijke voorziening zullen verder beperkt worden ten opzichte van het individuele monitoren van transacties door transacties tussen particulieren tot het bedrag van € 100 buiten de reikwijdte van de gezamenlijke voorziening te laten. Daarnaast zullen bij transacties tussen een zakelijke en een particuliere cliënt, slechts drie datavelden opgenomen worden in de gezamenlijke voorziening die zien op de particuliere cliënt: het IBAN-nummer, het BIC-nummer en de landencode.

De transactiegegevens kunnen ook bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard bevatten. Het gebruik van deze persoonsgegevens is mogelijk op grond van de in dit wetsvoorstel voorgestelde algemene grondslag voor het gebruik van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard om te voldoen aan verplichtingen gesteld bij of krachtens de Wwft. Dit is nader toegelicht in paragraaf 2.3.

B. Rechtmatigheid, noodzaak en evenredigheid gegevensverwerking

In paragraaf 2.2.2 is toegelicht dat de huidige verplichting voor banken om individueel transacties te monitoren er toe leidt dat banken slechts beperkte informatie hebben om vast te stellen dat een transactie ongebruikelijk is, met name als het gaat om transacties die via verschillende partijen en verschillende 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. Witwassen gebeurt zodoende zelden door een op zichzelf staande financiële handeling, maar overwegend via een (complex) samenstel van verschillende financiële handelingen. Doordat banken zich bij het individueel monitoren van transacties beperken tot de transacties die via hun bank gelopen zijn, kan daardoor de ongebruikelijkheid van transacties die via een groot netwerk lopen, onder de radar blijven. Een voorbeeld hiervan dat naar voren is gekomen bij de in paragraaf 2.2.2 genoemde pilot van de banken, is dat van een entiteit die actief is in de groothandel in voedingsmiddelen, waarbij transacties plaatsvinden over meerdere rekeningen bij verschillende banken. Bij verschillende banken

komen over de tijd verschillende contante stortingen binnen, die bij elkaar een significant totaalbedrag aan instroom van contact geld vormen. Daarnaast vindt bij één van de rekeningen een significante instroom plaats van zowel een branchevreemde rekening als vanaf een rekening gevestigd in Oost-Europa. Vanaf dezelfde rekening vinden ook transacties plaats naar Latijns-Amerika. Samengesteld is hiermee sprake van meerdere risicofactoren binnen een bekende witwastypologie. Als onderdeel van individuele monitoring heeft de ene bank door haar beperkte blik deze casus niet als ongebruikelijk geïdentificeerd. De andere betrokken bank heeft een deel van de risico's kunnen identificeren, maar ziet de transacties die via de andere bank lopen niet en kan daarmee niet het totaal aan risico's niet op waarde beoordelen. Doordat de risico's niet of slechts beperkt in beeld zijn, kunnen de banken noch de FIU-Nederland hier effectief op reageren. Hierdoor ontstaat een beperking die de effectiviteit van het systeem ondergraaft.

Om aan deze beperking tegemoet te komen wordt met dit voorstel een grondslag opgenomen in de Wwft voor banken om een gezamenlijke voorziening in te richten ten behoeve van de verplichting om transacties te monitoren. Door transacties van verschillende banken te combineren in de gezamenlijke voorziening, kunnen deze in samenhang gemonitord worden en kunnen netwerken die bij individuele transactiemonitoring buiten schot zouden blijven in kaart worden gebracht. Zoals toegelicht in paragraaf 2.2.2, gaat het hierbij om een meer verdergaande verwerking van gegevens door banken dan bij individuele transactiemonitoring, aangezien de transacties van de verschillende banken dienen te worden gecombineerd. Om een goede balans te treffen tussen aan de ene kant de een effectieve aanpak van witwassen en financieren van terrorisme en aan de andere kant de privacy van burgers, is bij de vormgeving van de grondslag daarom uitdrukkelijk rekening gehouden met afwegingen rond evenredigheid en proportionaliteit. De grondslag is daarom op de hieronder genoemde punten ingeperkt.

Alleen banken

De bevoegdheid om een gezamenlijke voorziening op te zetten geldt uitsluitend voor banken. Hieraan liggen zowel afwegingen rond effectiviteit als proportionaliteit ten grondslag. Bij veel transacties is een bankrekening, en daarmee ook een bank, betrokken. Zodoende hebben banken een centrale positie binnen het poortwachtersstelsel, waardoor criminele netwerken veelal gebruik maken van de diensten die banken leveren. Daarnaast is er bij banken veelal sprake van cliënten die doorlopende monitoring vereisen en is er beperkt sprake van incidentele transacties. De omvang is daarbij dusdanig, bijna 10 miljard transacties per jaar bij 35 miljoen cliënten, dat een effectievere inrichting van deze monitoring voor het stelsel voor het voorkomen van witwassen en terrorismefinanciering als geheel de meeste meerwaarde zal hebben.

Gegevens particulieren beperkt

De grondslag voor het combineren van transactiegegevens binnen de gezamenlijke voorziening geldt zowel voor zakelijke als voor particuliere relaties. Criminelen maken gebruik van verschillende soorten partijen in hun netwerken om zoveel mogelijk mist op te trekken over de herkomst van het geld. Daarom is het voor een effectieve werking van de monitoring binnen de gezamenlijke voorziening noodzakelijk om niet alleen de transacties van zakelijke relaties, maar ook die van particulieren, op te nemen. Tegelijkertijd kunnen juist de transacties van particulieren (gevoelige) persoonsgegevens bevatten. Daarom is in het kader van de hierboven genoemde afwegingen van evenredigheid en proportionaliteit,

ervoor gekozen om transacties tot het bedrag van € 100 tussen particulieren buiten de reikwijdte van de grondslag voor het gezamenlijk monitoren van transacties te laten vallen. Transacties tussen particulieren tot het bedrag van € 100 zullen dus niet gezamenlijk, maar slechts individueel, gemonitord worden door banken. Daarnaast zullen bij transacties tussen een zakelijke en een particuliere cliënt, van de particuliere cliënt slechts drie datavelden[26] opgenomen worden in de gezamenlijke voorziening. De schatting van de NVB 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.

Transactiegegevens beperkt

De huidige grondslag voor het individueel monitoren van transacties schrijft niet voor welke gegevens banken hiervoor dienen te gebruiken. Uiteraard geldt hierbij wel de algemene eis uit de AVG om de gegevensverwerking te beperken tot de gegevens die noodzakelijk zijn voor het doel, in dit geval het voorkomen van witwassen en financieren van terrorisme. Voor het combineren van transactiegegevens binnen de gezamenlijke voorziening, zal bij algemene maatregel van bestuur vastgesteld worden welke transactiegegevens gedeeld zullen mogen worden binnen de gezamenlijke voorziening. Het derde lid van artikel 34b bevat een opsomming van het soort gegevens waar het hierbij om gaat: identificerende gegevens, transactie-informatie, productinformatie en eventuele risico-indicatoren die de bank al heeft kunnen vaststellen bij het individueel monitoren van transacties. In de artikelsgewijze toelichting wordt per categorie ingegaan op de noodzaak van dit soort gegevens voor het gezamenlijk monitoren van transacties.

Waarborgen privacy

Om te beginnen dient te worden onderstreept dat de AVG uiteraard onverkort geldt voor de gegevensdeling die plaatsvindt in het kader van het gezamenlijk monitoren van transacties. Dit betekent, onder andere, dat banken voor de verwerking van persoonsgegevens in het kader van het gezamenlijk monitoren van transacties een gegevensbeschermingseffectbeoordeling (GEB)[27] dienen op te stellen, waarin onder meer de noodzaak van het gezamenlijk monitoren van transacties voor de betreffende bank wordt beoordeeld. Daarnaast geldt eveneens onverkort het *tipping-off* verbod, uit artikel 23, van de Wwft. Dit houdt in dat banken het gegeven dat van bepaalde transacties melding is gedaan bij de FIU-Nederland niet mogen delen met de gezamenlijke voorziening. Tussen banken onderling blijft de uitzondering op het *tipping-off* verbod uit artikel 23, zesde lid, onder 3°, van de Wwft overigens gewoon gelden. Op grond van deze uitzondering mogen de banken onderling het *tipping-off* verbod doorbreken, ten aanzien van een cliënt van beide banken en een transactie waar beide banken bij betrokken zijn.

Naast deze reeds bestaande waarborgen, worden met dit wetsvoorstel extra waarborgen getroffen ten aanzien van de verwerking van persoonsgegevens. In het zesde en zevende lid van artikel 34b worden verschillende maatregelen voorgeschreven die getroffen dienen te worden bij de opzet en gebruik van de gezamenlijke voorziening. Zo dienen alle persoonsgegevens die onderdeel uitmaken van de transactiegegevens die in de gezamenlijke voorziening worden opgenomen gepseudonimiseerd

[26] De drie datavelden die opgenomen zullen worden in het gezamenlijke voorziening zijn: het IBAN-nummer, het BIC-nummer en de landencode.
[27] Artikel 35 AVG.

en versleuteld te zijn. Dit betekent dat binnen de gezamenlijke voorziening het niet mogelijk is om de transacties te herleiden naar een specifiek persoon. De versleuteling kan uitsluitend buiten de gezamenlijke voorziening opgeheven worden door de individuele bank die de gegevens heeft aangeleverd. Ook dient er sprake te zijn van een adequaat beveiligingsniveau, dienen uitsluitend geautoriseerde personen toegang te hebben tot systemen waarin persoonsgegevens worden verwerkt, is geautomatiseerde besluitvorming als bedoeld in artikel 22, eerste lid, van de AVG uitgesloten en dient er een functionaris voor gegevensbescherming te worden ingesteld bij de gezamenlijke voorziening.

Rechten betrokkenen

Het uitgangspunt is dat cliënten de bank bij wie ze diensten afnemen kunnen aanspreken op de omgang van de bank met hun persoonsgegevens, ook wat betreft het combineren van transactiegegevens binnen de gezamenlijke voorziening. De banken zijn verplicht om, als verwerkingsverantwoordelijken in de zin van de AVG, hun cliënten te informeren over de verwerking van persoonsgegevens.[28] Dat betekent dat ook informatie verstrekt moet worden over de verwerkingen die plaatsvinden in het kader van (gezamenlijke) trasactiemonitoring die door banken zelf dan wel door derden (verwerkers) namens hen wordt uitgevoerd. Welke informatie verstrekt moet worden dient opgenomen te worden in een privacyverklaring van de bank. Ook kan een betrokkene zelf zijn bank verzoeken om inzage in de verwerking van op hem betrekking hebbende persoonsgegevens.[29] Daarnaast hebben betrokkenen andere rechten, vermeld in hoofdstuk 2 van de AVG, zoals het recht op rectificatie, wissing, verbetering, aanvulling, vernietiging of afscherming. Als een betrokkene van mening is dat een bank in strijd met geldende wet- en regelgeving zijn persoonsgegevens verwerkt, kan hij daartegen een klacht indienen bij de AP.[30] In dat geval kan een betrokkene ook beroep instellen bij de rechter.[31]

Een mogelijke complicerende factor bij gezamenlijke transactiemonitoring voor betrokkenen is dat het denkbaar is dat het niet direct duidelijk is welke bank een cliënt dient aan te spreken voor het gezamenlijke monitoren van transacties binnen de gezamenlijke voorziening. Dit kan zich voordoen als meerdere banken persoonsgegevens van een cliënt delen met de gezamenlijke voorziening. Om de betrokkene in een dergelijk geval te faciliteren, dienen banken de verantwoordelijkheid en aansprakelijkheid in het geval persoonsgegevens van een cliënt door meer dan één bank binnen de instelling worden gedeeld, vast te leggen en bekend te maken, zodat cliënten ermee bekend zijn en er desgewenst een beroep op kunnen doen.

Audit en evaluaties

Om te waarborgen dat er op verschillende wijzen vinger aan de pols wordt gehouden, zijn er verschillende vormen van evaluaties voorzien in het wetsvoorstel. Om te beginnen dienen de deelnemende banken zorg te dragen voor een tweejaarlijkse evaluatie van de naleving van de verplichtingen uit artikel 34b en de verplichtingen ten aanzien van het cliënten onderzoek en het melden van ongebruikelijke transacties. Daarnaast dienen de deelnemende banken jaarlijks een onafhankelijke audit uit te laten voeren naar de naleving van de regels met betrekking tot de

[28] Artikelen 12 tot en met 14 AVG.
[29] Artikel 15 AVG.
[30] Artikel 77 AVG.
[31] Artikel 79 AVG.

bescherming van persoonsgegevens. Deze audit dient tevens gedeeld te worden met de AP. Tenslotte is ook voorgeschreven dat vier jaar na inwerkingtreding van de wet, de Ministers van Financiën en Justitie en Veiligheid een evaluatie uitvoeren naar de effectiviteit van gezamenlijke transactiemonitoring en de naleving van de regels ten aanzien van de gegevensbescherming. De AP, DNB en de FIU-Nederland zullen nauw betrokken worden bij deze evaluatie in een adviserende rol. De evaluatie zal met de Staten-Generaal gedeeld worden.

Burgerservicenummer

Het wetsvoorstel maakt mogelijk dat het BSN wordt gebruikt om bij het uitvoeren van gezamenlijke transactiemonitoring de koppeling te maken tussen een cliënt die rekeningen aanhoudt bij verschillende banken om vast te kunnen stellen dat het om dezelfde persoon gaat. De AVG bepaalt dat de lidstaten zelf voorwaarden mogen stellen aan het verwerken van een nationaal identificatienummer. In Nederland is dit geregeld in de Uitvoeringswet AVG (UAVG) en de Wet algemene bepalingen BSN. Op grond van die wetten mag het BSN alleen verwerkt worden door overheidsorganen ter identificatie en, kort samengevat, door andere instellingen dan overheidsorganen wanneer dat bij wettelijke maatregel is bepaald. Banken hebben de wettelijke taak om te voorkomen dat hun dienstverlening wordt gebruikt voor witwassen en het financieren van terrorisme. Dit betreft een taak van algemeen belang. Zoals hierboven aangegeven is voor het vergroten van de effectiviteit van het uitvoeren van die taak het noodzakelijk dat banken transacties combineren om ongebruikelijke transactiepatronen naar boven te krijgen die bij individuele monitoring minder goed verkregen kunnen worden.

Het gebruik van BSN door deze afgebakende groep wordt voor deze specifieke taak als proportioneel beoordeeld. Een inrichting zonder uniek nummer zou niet effectief zijn en een verwerking van een grotere hoeveelheid data met zich brengen. Het zelf tot stand brengen van een uniek nummer wordt niet proportioneel geacht gezien de grote hoeveelheid persoonsgegevens die daarvoor nodig is en de grote investering. Daarbij is van belang dat banken reeds ervaring hebben met het gebruik van het BSN en over vereiste waarborgen beschikken om de bescherming van de gegevens te verzekeren. Een beperking van het gebruik van het BSN door deze instellingen en voor dit specifieke gebruik sluit aan op adviezen van de AP over het gebruik van het BSN.
De AP heeft erop gewezen dat het BSN kan worden opgevat als een «gevoelig» persoonsgegeven. Lidstaten kunnen op grond van de AVG voorzien in regels omtrent het gebruik. Daarbij moet rekening worden gehouden dat het risico op misbruik toeneemt naarmate het BSN breder bekend en toegankelijk is. Daarom moeten maatregelen worden getroffen om de kans op onrechtmatige verspreiding van het BSN te minimaliseren en om te voorkomen dat het BSN zich ontwikkelt tot een algemeen persoonsnummer. In de hier voorgestelde verwerking beperkt dit zich tot partijen die al over het BSN beschikken met het oog op de uitvoering van andere specifieke wettelijke taken en bewezen hebben hiermee zorgvuldig om te gaan. Tot slot is van belang dat voor de instellingen waaraan het gebruik wordt toegekend aanvullende waarborgen bestaan. Zo moeten zij over een vergunning beschikken op grond van de Wft, aan strenge bedrijfsvoeringseisen voldoen en staan zij onder toezicht van DNB.

Daarnaast mag het BSN alleen gebruikt worden in de fase van uitwisseling, verrijking en pseudonimisering van gegevens. Slechts een beperkt aantal personen heeft toegang tot de gegevens, waaronder het BSN. Deze personen zijn vooraf door de banken gescreend, hebben een geheimhou-

dingsverklaring ondertekend en al hun activiteiten binnen de gezamenlijke voorziening worden gelogd en zijn dus herleidbaar.

Bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard

De verwerking van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard ten behoeve van het monitoren van transacties door individuele banken en de noodzaak daartoe is toegelicht in paragraaf 2.3. In het kader van de voorgestelde maatregel komt daar de verwerking bij dat de individuele banken bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard, die zich in transactiegegevens bevinden, kunnen delen met andere banken die deelnemen aan een voorziening ten behoeve van het gezamenlijk monitoren van transacties. Het voorgestelde nieuwe eerste lid van artikel 34a biedt hiervoor een wettelijke grondslag.

Binnen een voorziening voor gezamenlijke transactiemonitoring worden alerts gegenereerd die zien op mogelijke ongebruikelijke transacties, zoals nu al plaatsvindt bij transactiemonitoring door individuele banken. Daarbij is het noodzakelijk dat ook bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard kunnen worden verwerkt, aangezien deze in bepaalde gevallen noodzakelijk zijn ten behoeve van het monitoren van transacties. Op de noodzaak hiervan wordt nader ingegaan in paragrafen 2.3 en 3.3. Het is vooraf niet goed te voorspellen welke bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard precies relevant zijn, aangezien dit sterk kan wisselen. Criminelen vinden telkens nieuwe manieren om illegaal verkregen gelden wit te wassen of om gelden voor terroristische aanslagen door te sluizen. Elke categorie bijzondere persoonsgegevens kan daarbij relevant zijn. Het is daarom aan de individuele banken om, voorafgaand aan een voorgenomen gebruik van bepaalde bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard, een GEB uit te voeren en aan de hand daarvan te onderbouwen waarom het gebruik van die gegevens noodzakelijk en proportioneel is, en zo nodig voorafgaand aan de verwerking de AP te raadplegen conform artikel 36, eerste lid, AVG. In deze onderbouwing door individuele banken dient ook te worden ingegaan op de maatregelen die worden genomen om de rechten van de betrokkenen te waarborgen, onder meer waar het gaat om de bescherming van persoonsgegevens.

C. Risico's en maatregelen

De risico's die zich kunnen voordoen bij gezamenlijke transactiemonitoring zien op legitimiteit, privacy en informatiebeveiliging. Bij risico's die zien op legitimiteit moet gedacht worden aan het risico dat banken ook andere gegevens combineren in de gezamenlijke voorziening dan de transactiegegevens die toegestaan zijn op grond van de wet. Bij privacy gerelateerde risico's kan gedacht worden aan het risico dat via gezamenlijke transactiemonitoring gegevens van een persoon gekoppeld worden aan de gegevens van een andere persoon, waardoor een onjuist beeld ontstaat van de betreffende cliënt(en). Risico's betreffende informatiebeveiliging zien bijvoorbeeld op de toegang tot gedeelde transactiegegevens door derden of onbevoegde medewerkers. Om dergelijke risico's te mitigeren is bij de vormgeving van de grondslag voor gezamenlijke monitoring beperkt en zijn er extra waarborgen getroffen. Op deze beperkingen en waarborgen is hierboven uitgebreid ingegaan.

§ 3.3 Verduidelijking verwerking bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard

A. Verwerking van persoonsgegevens

Deze maatregel ziet op de verwerking van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard, voor zover dit noodzakelijk is om te kunnen voldoen aan de verplichtingen die voortvloeien uit de Wwft ter voorkoming van witwassen en financieren van terrorisme, te weten het verrichten van (doorlopend) cliëntenonderzoek en het melden van ongebruikelijke transacties.

B. Rechtmatigheid, noodzaak en evenredigheid gegevensverwerking

In paragraaf 2.3 is ingegaan op de noodzaak voor instellingen om bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard te verwerken. Bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard zijn onontbeerlijk voor het uitvoeren van het (doorlopend) cliëntenonderzoek en het melden van ongebruikelijke transacties. Met name bij het monitoren van transacties en het opstellen van een effectief risicoprofiel (dit is een onderdeel van het cliëntenonderzoek op grond van artikel 3, tweede lid, onder d, van de Wwft) kan het noodzakelijk zijn om deze gegevens te verwerken. Hierbij is van belang dat een specifieke categorie bijzondere persoonsgegevens of een persoonsgegeven van strafrechtelijke aard in de regel op zichzelf geen aanleiding zal zijn een transactie als ongebruikelijk te beoordelen. Zo zal uitsluitend het gegeven dat iemand een bepaalde godsdienst aanhangt of politieke opvatting heeft een transactie niet ongebruikelijk maken. In de regel zal juist de combinatie van dit gegeven met andere gegevens die een instelling heeft over een cliënt, de doorslag geven bij de beoordeling of een transactie ongebruikelijk is.

C. Risico's en maatregelen

De verwerking van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard is uitdrukkelijk alleen toegestaan indien dat noodzakelijk is om te voldoen aan de verplichtingen uit de Wwft. Instellingen dienen in het kader van hun dienstverlening zelfstandig te beoordelen welke vorm van verwerking noodzakelijk is om te voldoen aan verplichtingen uit de wet. Hierbij dienen specifieke en passende waarborgen, te worden geboden ter bescherming van de rechten en vrijheden van betrokkenen.

Om de risico's van de verwerking van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard te mitigeren, wordt een documentatieplicht ingesteld voor instellingen en dienen instellingen hun cliënten te informeren over hun beleid ten aanzien van de verwerking van bijzondere categorieën van persoonsgegeven en persoonsgegevens van strafrechtelijke aard. Daarnaast worden middels een delegatiebepaling waarborgen gesteld aan, in ieder geval, de beveiliging van persoonsgegevens en de uitoefening van rechten van betrokkenen. Hier wordt nader op ingegaan in paragraaf 2.3 van de toelichting en de artikelsgewijze toelichting bij onderdeel I.

§ 3.4 Adviezen Autoriteit Persoonsgegevens[32]

De AP heeft twee adviezen uitgebracht die relevant zijn voor dit wetsvoorstel. Hieronder worden deze adviezen afzonderlijk besproken.

[32] Tevens ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

§ 3.4.1 Advies conceptwetsvoorstel

Op 12 maart 2020 heeft de AP geadviseerd over twee maatregelen uit het conceptwetsvoorstel plan van aanpak. Het ging hierbij om de introductie van de verplichting om onderzoek te doen naar eerdere dienstverlening en gegevens uit te wisselen en de introductie van de mogelijkheid om gezamenlijk transacties te monitoren.

§ 3.4.1.1 Gegevensdeling tussen instellingen bij cliëntenonderzoek

De AP wijst in haar advies op het ontbreken van de noodzaak voor de maatregel die ziet op het delen van risico's die geconstateerd zijn bij het cliëntenonderzoek tussen instellingen uit dezelfde categorie, thans opgenomen in het nieuwe voorgestelde artikel 3b van de wet. De AP merkt op dat de omvang van het probleem en de bestaande mogelijkheden om dit te adresseren, waaronder het stelsel van «zwarte lijsten», in de toelichting niet worden besproken. Naar aanleiding van de opmerkingen van de AP is in de toelichting de rol van zwarte lijsten in het kader van deze maatregelen verduidelijkt. Hierbij is tevens van belang dat het hanteren van zwarte lijsten geen verplichting is en er beperkt gebruik wordt gemaakt van deze mogelijkheid. Voorts merkt de AP op dat het verstrekkende gevolgen kan hebben voor een persoon indien deze op een zwarte lijst is geplaatst of instellingen die de persoon eerder diensten hebben verleend geconstateerde integriteitsrisico's met andere instellingen zullen delen. Naar aanleiding van deze opmerkingen is de reikwijdte van de maatregel beperkt tot instellingen behorend tot dezelfde categorie om de evenredigheid te borgen, zie paragraaf3.1 voor nadere toelichting. Daarnaast merkt de AP op dat de toelichting om de maatregel op te nemen als onderdeel van verscherpt cliëntenonderzoek niet overtuigend is. Om shopgedrag effectief tegen te gaan, is het noodzakelijk dat instellingen niet alleen navraag doen als er een hoger risico is vastgesteld ten aanzien van een bepaalde cliënten of transacties, maar juist ook in die gevallen waarin een instelling indicaties heeft van een hoger risico, maar over onvoldoende gegevens beschikt om dit vast te kunnen stellen. Een navraag bij een andere instelling uit dezelfde categorie kan in deze gevallen juist leiden tot de vaststelling dat een verscherpt cliëntenonderzoek nodig is, terwijl zonder deze gegevens het hoge risico dat de cliënt of de transactie met zich meebrengt later (of mogelijk helemaal niet) naar boven zou komen. Daarom is in dit wetsvoorstel bepaald dat een instelling navraag dient te doen wanneer de zakelijke relatie of de transactie naar haar aard een indicatie van een hoger risico met zich meebrengt, de risicofactoren bedoeld in bijlage III van de vierde anti-witwasrichtlijn van toepassing en als onderdeel van het verscherpt cliëntenonderzoek.

Voorts merkt de AP op dat het open begrip «integriteitsrisico's» ruimer is dan het primaire doel is van de Wwft. Naar aanleiding van deze opmerking is het wetsvoorstel aangepast. In artikel 3b, vierde lid, is het begrip «integriteitsrisico's» vervangen door «risico's op witwassen of het financieren van terrorisme». Ook wijst de AP erop dat het concept geen beperking naar tijd bevat, hetgeen disproportioneel is. Naar aanleiding van deze opmerking is de toelichting op deze maatregel aangepast. In de toelichting is verduidelijkt dat de verplichting zich beperkt tot vijf jaar, overeenkomstig de bewaartermijn uit artikel 33, derde lid, van de wet. Daarnaast geldt de verplichting om geconstateerde risico's te delen met een verzoekende instellingen uit artikel 3b, derde lid, niet met terugwerkende kracht. In artikel III is daarom opgenomen dat deze verplichting niet geldt voor informatie gebleken voor inwerkingtreding van de wet.

Ten slotte merkt de AP op dat in de toelichting aandacht besteed zou moeten worden aan de gevolgen van de maatregel voor de betrokkene. Naar aanleiding hiervan is de toelichting in paragrafen 2.2.1.4 en 3.1 aangepast.

§ 3.4.1.2 Gezamenlijke transactiemonitoring door banken

De AP wijst er in haar advies op dat de gezamenlijke monitoring van alle transacties van alle instellingen een gigantische beperking van de bescherming van persoonsgegevens tot gevolg heeft, omdat hierdoor de gehele financiële handel en wandel van betrokkene en al zijn binnenlandse transacties bij alle WWFT-instellingen tezamen worden gemonitord, temeer in combinatie met het voorstel om de transactiemonitoring uit te besteden aan een derde partij. Het AP wijst er daarbij op dat dit «mass surveillance-karakter» voor het Hof van Justitie EU een belangrijk punt vormde om de dataretentierichtlijn onrechtmatig te verklaren. Daarnaast merkt de AP op dat onduidelijk is waarom de maatregel voor alle instellingen moet gelden.

Naar aanleiding van deze opmerkingen is het wetsvoorstel aangepast. Ten eerste is de mogelijkheid om transacties te delen beperkt tot banken. Daarnaast is deze bevoegdheid verbonden aan de voorwaarde dat deze plaatsvindt in een gezamenlijke voorziening waarvoor aanvullende voorwaarden gelden om de bescherming van persoonsgegevens te borgen. Naar aanleiding van het advies is in artikel 10 de grondslag voor de uitbesteding van transactiemonitoring aangepast en is toegevoegd dat bij algemene maatregel van bestuur aanvullende regels kunnen worden gesteld aan deze vorm van uitbesteding. Tot slot dient jaarlijks verslag te worden uitgebracht over de effectiviteit van de voorziening en zal na twee jaar na ingebruikname een onafhankelijke audit plaatsvinden of regels betreffende gegevensbescherming worden nageleefd. In paragraaf 3.2 wordt de noodzaak en evenredigheid nader toegelicht en bij artikel I, onderdeel J, wordt ingegaan op de waarborgen. Voorts merkt de AP op dat de noodzaak voor het verwerken van bijzondere persoonsgegevens bij het delen van transacties onduidelijk is en wijst de AP erop dat het delen niet beperkt is naar tijd. Naar aanleiding van deze opmerking is het wetsvoorstel aangepast door middel van de toevoeging van een nieuw artikel 34a, eerste lid. In paragrafen 2.3 en 3.3 wordt de noodzaak voor de verwerking van bijzondere persoonsgegevens of persoonsgegevens van strafrechtelijke aard om te voldoen aan de verplichtingen uit de Wwft, nader toegelicht. Daarnaast is in artikel 34b, vierde lid, opgenomen dat de verwerking wordt beëindigd indien dat niet langer noodzakelijk is om te voldoen aan de meldplicht. Tot slot valt het de AP op dat de grondslag voor de algemene maatregel van bestuur om nadere regels te stellen over het delen van transactiegegevens facultatief is, en niet dwingend. Mede naar aanleiding hiervan is in het wetsvoorstel een imperatieve grondslag opgenomen voor een algemene maatregel van bestuur voor het stellen van regels ten aanzien van het gebruik van bijzondere persoonsgegevens en persoonsgegevens van strafrechtelijke aard.

§ 3.4.1.3 Evenredigheid en bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard

De AP plaatst in haar advies vraagtekens bij de evenredigheid van de voorgestelde maatregelen om persoonsgegevens te delen en wijst daarbij op een aantal andere maatregelen die op moment van het advies in behandeling waren: de implementatiewet wijziging vierde anti-witwasrichtlijn; de implementatiewet registratie uiteindelijk belanghebbenden van vennootschappen en andere juridische entiteiten; en het verwijzingsportaal bankgegevens. Dit maakt dat ook moet worden

gekeken naar de evenredigheid van dit wetsvoorstel in relatie tot het stelsel van wettelijke maatregelen in het kader van de aanpak van witwassen. In dat kader is van belang dat de Europese Commissie uiterlijk op 11 januari 2022 en vervolgens om de drie jaar een verslag opstelt over de toepassing van de vierde anti-witwasrichtlijn. Dit verslag legt zij voor aan het Europees Parlement en de Raad. Het verslag zal onder meer een evaluatie bevatten van de wijze waarop de in het Handvest van de grondrechten van de Europese Unie erkende grondrechten en beginselen zijn geëerbiedigd. De AP heeft in haar advies van 7 maart 2019 over het wetsvoorstel ter implementatie van de gewijzigde vierde anti-witwasrichtlijn onder meer geadviseerd om daarbij naar vermogen te bevorderen dat bij die gelegenheid de evenredigheid van de vierde anti-witwasrichtlijn in relatie tot het recht op bescherming van persoonsgegevens ten gronde wordt geadresseerd.

Bij de beoordeling van de evenredigheid van de voorgestelde maatregelen is de effectiviteit van de maatregelen van belang. Uit de hiervoor genoemde proef blijkt dat het gezamenlijk monitoren van transacties effectiever is. In het wetsvoorstel is een verplichting opgenomen voor banken die deelnemen aan een gezamenlijke voorziening voor transactiemonitoring om jaarlijks een verslag te maken over de naleving van de regels gesteld bij of krachtens de hoofdstukken 2 en 3 van de Wwft met het oog op de beoordeling van de effectiviteit van de maatregel. Daarnaast wordt voorgesteld dat banken verplicht twee jaar na inwerkingtreding van deze wet en vervolgens elke vijf jaar, een onafhankelijke audit uitvoeren ten aanzien van de werking van de gezamenlijke voorziening. Deze audit heeft in elk geval betrekking op de naleving van de regels gesteld bij of krachtens de artikelen 10, 34a en 34b en de regels met betrekking tot de bescherming van persoonsgegevens. De verslagen en resultaten van de audits dienen vervolgens als input voor een evaluatie op nationaal niveau van de wijze waarop de in het Handvest van de grondrechten van de Europese Unie erkende grondrechten en beginselen zijn geëerbiedigd.

De AP wijst in haar advies verder op het ontbreken van een duidelijke grondslag voor het verwerken van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard. In haar advies op de implementatiewet wijziging van de vierde anti-witwasrichtlijn stipte de AP eerder aan dat de richtlijn geen onderscheid maakt naar de aard en mate van gevoeligheid van gegevens.[33] In navolging van deze opmerkingen is in dit wetsvoorstel een expliciete wettelijke grondslag opgenomen voor het door instellingen verwerken van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard, voor zover dat noodzakelijk is om te voldoen aan de verplichtingen uit de wet. In paragraaf 2.3 en 3.3 wordt deze grondslag nader toegelicht.

Deze en de in de vorige paragraaf genoemde aanpassingen maken dat de door de AP genoemde vergelijking met het *mass surveilance*-karakter van de dataretentierichtlijn voor de voorgestelde maatregel niet opgaat.

§ 3.4.2 Advies gebruik BSN, BRP, UBO-register

Als onderdeel van het plan van aanpak witwassen is aan de AP advies gevraagd over de toegang van poortwachters tot een aantal bronnen om hun informatiepositie te verbeteren en zo de effectiviteit van de uitvoering van hun wettelijke taak te vergroten. Dit betrof gebruik van het BSN, toegang tot de Basisregistratie personen en toegang tot de afgesloten

[33] Advies conceptvoorstel Implementatiewet wijziging vierde anti-witwasrichtlijn.

gegevens in het UBO-register. Op 16 december 2019 heeft de AP advies uitgebracht.[34]

Naar aanleiding van het advies is besloten om met dit wetsvoorstel te voorzien in het gebruik van het BSN door banken die gebruikmaken van een gezamenlijke voorziening voor transactiemonitoring. Hieronder wordt ingegaan op het advies van de AP over gebruik van het BSN en de wijze waarop hieraan gevolg is gegeven. Daarnaast wordt, aan de hand van het advies, de toegang voor banken en notarissen tot BRP-gegevens in de vorm van een *hit/no hit*-voorziening nader onderzocht. Bij een dergelijke voorziening ontvangt de instelling na invoering van een adres het bericht of dit adres overeen komt met het adres in het BRP. Dit vereist een wijziging van het Besluit basisregistratie personen en de bouw van de technische voorziening, in lijn met het beginsel van dataminimalisatie. In de toelichting bij de wijziging van dat besluit zal nader ingegaan worden op het advies van de AP. Tot slot is besloten om vooralsnog niet te voorzien in toegang voor poortwachters tot de afgesloten gegevens in het UBO-register. De noodzaak voor toegang zou vooral gelegen zijn in een juiste uitvoering van de verplichting om discrepanties in het register te melden. De vraag is of hiervoor de set openbare gegevens niet al voldoende is. Samen met de banken zal gemonitord worden of de enkele toegang tot de openbare gegevens voldoende is voor het melden van discrepanties.[35]

§ 3.4.2.1 Overwegingen AP bij het gebruik van het BSN

Aan de AP is gevraagd om een beoordeling van de proportionaliteit en subsidiariteit van het verwerken van het BSN door de instellingen voor het uitvoeren van de wettelijke taak tot het voorkomen van het gebruik van het financieel stelsel voor witwassen, de onderliggende delicten en financieren van terrorisme. Aanvullend is gevraagd of in het geval sprake is van voldoende noodzaak, het gebruik verplichtend voorgeschreven moet worden of dat kan worden volstaan met het uitsluitend regelen van de bevoegdheid tot het gebruik.

In haar advies geeft de AP als algemene opmerking mee om de omvang en aard van de problemen en bij welke instellingen zij zich voordoen, nader in kaart te brengen, alsmede mogelijke oplossingen door een beter gebruik of uitvoering van het bestaande instrumentarium aan te geven alvorens tot wetgeving over te gaan. Ten aanzien van het gebruik van het BSN overweegt de AP dat het BSN kan worden opgevat als een «gevoelig» persoonsgegeven, met name gelet op de mogelijkheid in de AVG dat lidstaten kunnen voorzien in regels daaromtrent. Het risico op misbruik neemt toe naarmate het BSN breder bekend en breder toegankelijk is. De AP wijst er daarbij op dat de groep instellingen zeer omvangrijk en divers is en dat een groot deel van deze groep geen ervaring heeft met de verwerking van dit gevoelige gegeven, hetgeen extra risico's met zich brengt. In dat verband acht de AP de noodzaak om ten behoeve van de algemene naleving van de Wwft het BSN te gebruiken onvoldoende onderbouwd.

Daarnaast merkt de AP op dat uit de adviesaanvraag niet bleek of minder ingrijpende alternatieven onderzocht zijn. De AP denkt aan het gebruik van het rekeningnummer van banken of meer inzet van personeel bij

---

[34] Zie bijlage 3 bij Kamerstukken II 2019/20, 31 477, nr. 50.

[35] Hiermee wordt tevens toezegging T003194 afgedaan. Tijdens het Commissiedebat van 9 september 2021 heeft de Minister van Financiën aan de heer Heinen toegezegd de analyse op basis van het AP-advies inzake de uitbreiding van gegevensuitwisseling met de Tweede Kamer te delen, tegelijk met het wetsvoorstel plan van aanpak witwassen.

cliënten met hoge risico's. Daarbij geeft de AP aan dat overeenkomstig uitspraken van het Europees Hof van Justitie bij de afweging met alternatieven een «extreem verschil» in kosten een relevante factor kan zijn. Verder merkt de AP op dat in de adviesaanvraag niet is ingegaan op de waarborgen tegen oneigenlijk gebruik. Het gaat dan om het voorkomen van gebruik door onbevoegden of voor andere werkzaamheden.

Ten aanzien van het voorschrijven als een verplichting of als een bevoegdheid geeft de AP aan dat het in de wetgeving op beide manieren gebeurd en dat bepalend is wat passender is in het licht van het doel en de reikwijdte.

§ 3.4.2.2 Verwerking opmerkingen AP

Aan de hand van de opmerkingen van de AP is het gebruik van het BSN enerzijds beperkt tot een concrete wettelijke taak binnen de Wwft en anderzijds tot een beperkte groep. Het gebruik van het BSN is in dit wetsvoorstel enkel toegestaan voor transactiemonitoring en dan alleen in het geval dit is ingericht met een gezamenlijke voorziening. In de toelichting is opvolging gegeven aan de opmerking van de AP om de noodzaak nader te onderbouwen. Zonder uniek nummer is gezamenlijke monitoring niet effectief. Daarbij is ook ingegaan op de mogelijke alternatieven. Deze alternatieven zijn beperkt in effectiviteit, vergen meer verwerkingen van persoonsgegevens en vragen een aanzienlijke investering, zeker als een eigen systeem opgezet zou moeten worden om overkoepelend unieke nummers uit te geven.

De verwerking van het BSN is uitsluitend toegestaan voor banken die aan de gezamenlijke voorziening voor transactiemonitoring deelnemen. Daarmee is de groep instellingen beperkt en is geen sprake meer van een omvangrijke en diverse groep. Vooralsnog betreft het initiatief voor de gezamenlijke transactiemonitoring vijf banken. Daarnaast betreft dit instellingen die, zoals de AP ook aangeeft, ervaring hebben met het verwerken van dit gegeven. Dit brengt met zich dat er geen nieuwe instellingen zijn die het BSN gaan verwerken en dat deze instellingen ervaring hebben met het beveiligen en zorgvuldig gebruik van het BSN. In deze toelichting is daarnaast nader ingegaan op de waarborgen die de banken treffen voor onbevoegd gebruik.

§ 4. Uitvoering en handhaafbaarheid

DNB en BTWwft hebben een uitvoeringstoets uitgevoerd naar aanleiding van dit wetsvoorstel. Hieronder zal ingegaan worden op de uitvoeringstoetsen van beide toezichthouders. Daarnaast wordt ingegaan op het effect dat het verbod op contante betalingen vanaf € 3.000 zal hebben op de taakuitoefening van de FIU-Nederland.

§ 4.1 Bureau Toezicht Wwft

BTWwft heeft naar aanleiding van dit wetsvoorstel in juli 2020 een uitvoeringstoets uitgevoerd voor het verbod op contante betalingen vanaf € 3.000 euro voor handelaren. In 2022 heeft een herijking plaatsgevonden van de uitvoeringstoets. Uit de uitvoeringtoets volgt dat het verbod uitvoerbaar is, mits de benodigde capaciteit op tijd kan worden geworven en de benodigde IV-capaciteit beschikbaar is.

De uitvoeringstoets stelt dat het verbod in zijn algemeenheid een barrière opwerpt tegen witwassen en het financieren van terrorisme. Wel benoemt BTWwft in de uitvoeringstoets een aantal risico's. Het risico bestaat dat

kwaadwillenden naar andere mogelijkheden zullen zoeken om contante transacties boven het drempelbedrag uit te voeren en dat illegale geldstromen daardoor buiten het gezichtsveld kunnen raken. Dit kan bijvoorbeeld door contante transacties boven de € 3.000 buiten de administratie te houden, transacties op te knippen, een transactie te presenteren als een transactie tussen twee particulieren terwijl er in feite een handelaar betrokken is, of door een mogelijke verschuiving van transacties in goederen naar dienstverlening tegen vergoeding in contanten. Ook vraagt BTWwft in de uitvoeringstoets aandacht voor de territoriale werkingssfeer van het verbod. BTWwft adviseert om het verbod te laten gelden indien handelaren in Nederland transacties in contanten verrichten of indien een in Nederland woonachtige of gevestigde handelaar transacties in contanten verricht. Op die manier wordt (deels) voorkomen dat het verbod omzeild wordt door transacties net over de grens te verrichten of te stellen dat transacties net over de grens zijn verricht (dit laatste is niet te controleren door de toezichthouder). De wetstekst is aangepast naar aanleiding hiervan.

Ontwijken van het verbod op contante betaling in Nederland zou echter nog steeds mogelijk zijn door «over de grens» een rechtspersoon op te richten. Omdat een nationaal verbod criminelen niet verhindert hun activiteiten over de grens voort te zetten, maakt het kabinet zich daarom in EU-verband sterk voor een EU-breed verbod. Een voorbeeld hiervan is het non-paper dat Nederland, samen met België, Frankrijk, Italië en Spanje op expertniveau heeft ingediend bij de Europese Commissie[36]. Voorts voorziet dit wetsvoorstel in een evaluatie over vijf jaar van de effectiviteit het verbod waarbij ook methoden om het verbod te omzeilen zullen worden betrokken.

§ 4.2 De Nederlandsche Bank t.a.v. samenwerking en informatie-uitwisseling instellingen

DNB heeft een uitvoeringstoets uitgevoerd naar aanleiding van dit wetsvoorstel.[37] Ten aanzien van de uitvoerbaarheid en handhaafbaarheid van de uitbreiding van gegevensuitwisseling in het kader van het cliëntenonderzoek, heeft DNB aangegeven een aantal knelpunten te signaleren. Het voorstel en de toelichting zijn op een aantal punten aangepast om deze knelpunten weg te nemen. Om te beginnen is artikel 3b aangepast zodat er niet meer naar «integriteitsrisico's» wordt verwezen, maar naar «risico's op witwassen of financieren van terrorisme», aangezien de term integriteitsrisico's breder opgevat zou kunnen worden dan is bedoeld.

Daarnaast heeft DNB verzocht om de verwijzing naar het verscherpt cliëntenonderzoek te veranderen in een meer risico gebaseerde onderzoeksplicht, om beter aan te sluiten bij de systematiek van de Wwft en de wijze waarop DNB toezicht houdt. Volgens DNB wordt het vraagstuk van risicovolle cliënten die steeds wisselen van instelling, beter geadresseerd indien een instelling ook navraag kan doen als daar een redelijke aanleiding toe is, maar er (nog) geen sprake is van een verscherpt cliëntenonderzoek. Om hieraan tegemoet te komen is ervoor gekozen om de verplichting om navraag te doen in te stellen voor de gevallen waarin sprake is van indicaties van een hoger risico op witwassen of financieren van terrorisme, de risicofactoren bedoeld in bijlage III van de vierde anti-witwasrichtlijn van toepassing en als onderdeel van het verscherpt cliëntenonderzoek. Hiermee wordt een meer risico gebaseerde

[36] Kamerstukken II 2020/2021, 21 501-07, nr. 1778.
[37] Tevens ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

benadering gekozen, terwijl de evenredigheid van de maatregel ermee is gediend.

DNB heeft ook verzocht om meer invulling te geven in de toelichting aan de onderzoeksplicht. De toelichting is hierop uitgebreid. Hierbij dient wel aangemerkt te worden dat de aanvulling handreikingen betreft. Aangezien deze verplichting geldt voor verschillende instellingen, is het niet mogelijk en wenselijk om op voorhand aan te geven hoe de onderzoeksplicht eruit dient te zien voor de verzoekende instelling en de instelling die bevraagd wordt. Aangezien redelijkheid hierbij leidend is, kan het per soort instelling en per geval verschillen. Om deze reden wordt «onverwijld» ook niet vervangen door een vaste termijn, ondanks de wens van DNB hiertoe.

Voorts heeft DNB aangegeven het wenselijk te vinden dat bij de uitbreiding van de mogelijkheid tot uitbesteding, net als in het reeds bestaande artikel hieromtrent, in het wetsvoorstel wordt geëxpliciteerd dat de verantwoordelijkheid voor de naleving van de wettelijke verplichtingen altijd bij de uitbestedende instelling blijft. Hieraan is tegemoet gekomen. DNB heeft aangegeven dat het wenselijk is om een grondslag op te nemen voor nadere regelgeving met aanvullende voorwaarden voor deze vorm van uitbesteding. Hier is gevolg aan gegeven door een grondslag op te nemen voor een algemene maatregel van bestuur om aanvullende regels te stellen voor deze uitbesteding in verband met het toezicht, de beheersing van risico's en de voorwaarden voor de overeenkomst om uit te besteden.

DNB merkt op dat de bevoegdheid om gegevens te delen in het gezamenlijke transactiemonitoring zich niet slechts dient uit te strekken tot het melden van bancaire transacties, maar ook tot transactiemonitoring. Dit is verduidelijkt in het wetsvoorstel en de toelichting. Ten slotte is de reikwijdte van artikel 34b, dat ziet op het gezamenlijk monitoren van transacties verduidelijkt.

§ 4.3 Financial Intelligence Unit en het verbod op contante betalingen vanaf € 3.000

Met de invoering van het verbod voor handelaren op contante betalingen vanaf € 3.000, komt de meldplicht voor handelaren te vervallen. Zoals FIU ook aangeeft in zijn consultatiereactie, ligt het in de lijn der verwachting dat er hiermee minder ongebruikelijke transacties gemeld zullen worden voor deze groep. Tegelijkertijd kunnen andere partijen uit de Wwft-keten nog wel melding maken over deze groep en kan er door invoering van een verbod sprake zijn van een waterbedeffect naar andere sectoren, waardoor er mogelijk juist meer meldingen van ongebruikelijke transacties zullen plaatsvinden. Om die reden is het onduidelijk wat het uiteindelijke effect zal zijn van het verbod op het totale aantal ongebruikelijke transacties en op de taakuitoefening van de FIU.

§ 5. Financiële gevolgen en regeldruk

Hieronder zal opeenvolgend ingegaan worden op de gevolgen van dit wetsvoorstel voor het bedrijfsleven en de adviezen van het Adviescollege Toetsing en Regeldruk.[38]

[38] Tevens ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

§ 5.1 Gevolgen voor het bedrijfsleven

In het navolgende wordt toegelicht welke gevolgen en nalevingskosten dit wetsvoorstel met zich mee brengt voor het bedrijfsleven. Dit wetsvoorstel bevat twee nieuwe verplichtingen voor instellingen, namelijk (1) het verbod op contante betalingen vanaf € 3.000 voor beroeps- of bedrijfsmatige handelaren van goederen, en (2) de verplichting voor instellingen om in het kader van het cliëntenonderzoek navraag te doen naar gebleken risico's op witwassen en financieren van terrorisme bij eerdere dienstverlening.

§ 5.1.1 Verbod op contante betalingen vanaf € 3.000

Het verbod op contante betalingen vanaf € 3.000 voor beroeps- of bedrijfsmatige handelaren als kopers en verkopers in goederen heeft gevolgen voor de regeldruk. De huidige verplichtingen uit de Wwft, die gelden voor deze handelaren indien zij contante betalingen verrichten van € 10.000 of meer, komen te vervallen. Dit betekent dat deze handelaren geen cliëntenonderzoek meer hoeven te verrichten en geen ongebruikelijke transacties meer hoeven te melden bij de FIU-Nederland. Het vervallen van deze verplichtingen brengt voor die handelaren een vermindering van de structurele nalevingskosten met zich. De vermindering van deze structurele regeldrukkosten wordt geschat op € 93 per cliënt (twee uur per cliënt, uitgaande van een uurtarief tussen € 39 en € 54). Op dit moment ligt het aantal handelaren onder toezicht op circa 95.000. Dit zou betekenen dat er een totale vermindering van structurele regeldrukkosten is van € 8,8 miljoen.

Wel moeten deze handelaren zich houden aan het verbod op contante betalingen vanaf € 3.000. De verwachting is dat dit verbod niet leidt tot eenmalige of structurele administratieve lasten voor deze handelaren. Het verbod heeft immers tot gevolg dat contante betalingen vanaf € 3.000 moeten worden geweigerd, dan wel dat deze betalingen anderszins op legale wijze moeten plaatsvinden. Gezien het huidige Nederlandse betaallandschap is het aannemelijk dat het bij deze handelaren ook mogelijk is om giraal te betalen.

§ 5.1.2 Gegevensdeling tussen instellingen bij cliëntenonderzoek

Het wetsvoorstel voorziet daarnaast in een verplichte gegevensdeling bij cliëntenonderzoek tussen instellingen die behoren tot dezelfde categorie. Deze verplichting leidt tot structurele nalevingskosten. In de eerste plaats wordt het cliëntenonderzoek verzwaard indien de instelling indicaties van een hoger risico op witwassen of financieren van terrorisme vaststelt bij een cliënt, de risicofactoren bedoeld in bijlage III van de vierde anti-witwasrichtlijn van toepassing zijn en als onderdeel van het verscherpt cliëntenonderzoek. Er wordt namelijk van instellingen verlangd dat zij in dergelijk gevallen nagaan of de cliënt de afgelopen vijf jaar gebruik heeft gemaakt van dienstverlening van een andere instelling behorend tot dezelfde categorie. De invulling van deze onderzoeksplicht dient redelijk te zijn en hangt af van de context van de situatie. Het is aannemelijk dat de onderzoeksplicht in ieder geval een extra verzoek om informatie aan de cliënt behelst. De structurele nalevingskosten hiervan worden geschat op ongeveer € 11,63 per keer (een kwartier per cliëntenonderzoek met een hoger risico op witwassen of financieren van terrorisme, uitgaande van een uurtarief tussen € 39 en € 54). Daarnaast bestaat de verplichting voor instellingen om navraag te doen naar gebleken risico's op witwassen of financieren van terrorisme bij de instelling waar de cliënt diensten afneemt of heeft afgenomen of waar deze is geweigerd. Die instelling is vervolgens verplicht om de informatie

over deze risico's te delen met de instelling die hierom verzoekt. De structurele nalevingskosten voor de instelling die om informatie verzoekt, worden geschat op € 23,25 (een half uur per cliënt, uitgaande van een uurtarief tussen € 39 en € 54). De structurele nalevingskosten voor de instelling die het verzoek ontvangt en die de beschikbare informatie moet verstrekken, worden geschat op € 46,50 (een uur per cliënt, uitgaande van een uurtarief tussen € 39 en € 54). Daarmee komen de totale structurele nalevingskosten per cliëntenonderzoek met een hoger risico op witwassen of financieren van terrorisme neer op € 69,75. Omdat het op voorhand onduidelijk is bij hoeveel transacties of zakelijke relaties instellingen zullen vaststellen dat deze binnen de reikwijdte van dit artikel vallen, zijn de totale kosten van de verplichting niet kwantificeerbaar. Dit is in hoge afhankelijk van een aantal specifieke factoren die per instelling sterk verschillen zoals het soort dienstverlening, de mate waarin deze dienstverlening blootstaat aan risico's en de beoordeling van risico's door de instelling.

§ 5.2 Adviescollege Toetsing en Regeldruk

Het Adviescollege Toetsing en Regeldruk heeft in haar advies aandacht gevraagd voor de eerste twee onderdelen van het wetsvoorstel. Om te beginnen adviseert het college om na de invoering van het verbod op contante betalingen vanaf € 3.000 te monitoren in hoeverre het verbod werkbaar is voor de cliënten van handelaren voor wie dit verbod geldt. Mede naar aanleiding van dit advies, is besloten om deze maatregel vijf jaar na inwerkingtreding te evalueren. Hierbij zal ook oog zijn voor de gevolgen voor de cliënten.

Daarnaast adviseert het college om, in het kader van de maatregel die ziet op het mogelijk maken van gegevensuitwisseling tussen instellingen bij het cliëntenonderzoek, ondersteuning te organiseren voor cliënten van instellingen aan wie vanwege de poortwachtersfunctie ten onrechte dienstverlening is geweigerd. Om hieraan tegemoet te komen is in de toelichting verduidelijkt dat de individuele risicoafweging nog steeds leidend is bij een gegevensuitwisseling tussen instellingen. Dit betekent dat de gegevens die een dienstverlener aanreikt slechts dienen als een aanvulling en de instelling dus niet van de verplichting ontslaan tot het maken van een eigen individuele risicoafweging. Overigens kunnen consumenten en kleinzakelijke ondernemers die onterecht zijn uitgesloten van dienstverlening, een klacht indienen bij het Klachteninstituut Financiële Dienstverlening.

Het college adviseert ten slotte ook om de analyse van de regeldrukeffecten uit te werken conform de Rijksbrede methodiek. In reactie op dit advies is de berekening in de voorgaande paragraaf aangepast.

§ 6. Openbare consultatie

In de periode van 2 december 2019 tot en met 14 januari 2020 is een concept van dit onderdeel van het wetsvoorstel publiek geconsulteerd. Naar aanleiding van de publieke consultatie zijn 67 reacties ontvangen, waarvan er 62 openbaar zijn. De reacties komen van uiteenlopende partijen. Reacties zijn ingestuurd door toezichthouders, zoals de Kansspelautoriteit, alsook een aantal andere publieke partijen, zoals het Openbaar Ministerie, de G4 en de FIU-Nederland. Daarnaast hebben veel branche- en vakorganisaties gereageerd op het conceptwetsvoorstel, zoals Detailhandel NL, de NVB, de Nederlandse Vereniging voor Rechtspraak en Netwerk Notarissen. Ook individuele instellingen hebben gebruik gemaakt van de gelegenheid om een reactie in te sturen, waaronder advocatenkan-

toren, accountancykantoren en Holland Casino. Ten slotte heeft ook een aantal particulieren een reactie gegeven op het conceptwetsvoorstel.

Naar aanleiding van de consultatiereacties zijn de wettekst en de memorie van toelichting op verscheidene punten aangepast en aangevuld. Hierna zullen de ontvangen reacties, voor zover relevant voor dit wetsvoorstel, per thema worden beschreven.

§ 6.1 Algemeen

Enkele respondenten geven aan dat de inzet van de overheid in de strijd tegen witwassen achterblijft en dat er te veel wordt verwacht van de poortwachters. In haar plan van aanpak witwassen – waar dit wetsvoorstel een uitwerking van is – heeft het kabinet aangegeven dat het voorkomen en bestrijden van witwassen een gezamenlijke opgave is van zowel publieke als private partijen. Daarom is in de aanloop naar het plan uitgebreid gesproken met verschillende betrokken partijen. Zij scharen zich achter dit plan. Met dit wetsvoorstel krijgen poortwachters bevoegdheden die hun poortwachtersrol zullen versterken en hen zullen helpen bij de invulling van deze rol.

In een van de reacties wordt verzocht om de informatie-uitwisseling voor poortwachters verder uit te breiden om het tegengaan van witwassen te faciliteren. Met dit wetsvoorstel worden stappen gezet in deze richting. Bij uitbreiding van informatie-uitwisseling is van belang rekening te houden met het recht op privacy en gegevensbescherming. De nut, noodzaak, subsidiariteit en proportionaliteit zal bij elke uitbreiding van de bevoegdheden op het gebied van informatie-uitwisseling nauwkeurig onderzocht moeten worden.

In een aantal reacties wordt verzocht om bepaalde andere beroepsgroepen onder de reikwijdte van de Wwft te brengen of om bepaalde instellingen extra bevoegdheden te geven in het kader van de Wwft. Aangezien dit buiten de reikwijdte van dit wetsvoorstel valt, worden deze reacties hier buiten beschouwing gelaten.

§ 6.2 Verbod op contante betalingen vanaf € 3.000

Een aantal respondenten gaf aan dat het onvoldoende duidelijk is voor wie het verbod geldt en wanneer er sprake is van samenhangende transacties. Deze punten zijn verduidelijkt in paragraaf 2.1 van de toelichting. Daarnaast is een omissie bij de beschrijving van de objectieve indicator in paragraaf 2.1 rechtgezet.

Uit een aantal reacties kwam naar voren dat er onvoldoende bewijs is dat contant geld een risico vormt voor witwassen en het nut van het verbod daarom onvoldoende onderbouwd is. Hoewel er geen precieze cijfers beschikbaar zijn van de bijdrage van contant geld in het witwasprobleem, wordt in de meest recente National Risk Assessment (NRA) aangegeven dat contant geld witwassen via diensten/goederen van (grootwaarde)handelaren door experts als een van de witwasdreigingen met de grootste potentiële impact wordt gezien.[39] Ook bij andere risico's op witwassen die genoemd worden in de NRA wordt contant geld veelvuldig genoemd.

Daarnaast wijzen verschillende partijen op het belang van contant geld in de samenleving – zoals het borgen van anonimiteit, de mogelijkheid tot betalen voor toeristen, de terugvalfunctie en contant geld als oppotmiddel

[39] National Risk Assessment, *Wetenschappelijk Onderzoek- en documentatiecentrum*, Cahier 2020–11, p. 52.

– en vragen zij zich af in hoeverre de effectiviteit van dit verbod opweegt tegen de beperking van de hiervoor genoemde rollen van contant geld. Een respondent gaf aan het brede debat over contant geld te missen. Binnen het Maatschappelijk Overleg Betalingsverkeer (MOB) vindt het maatschappelijk debat plaats over (het gebruik van) contant geld en de functies die contant geld vervult. Ook het Ministerie van Financiën, aanwezig bij het MOB, is zich bewust van de functies van contant geld en hecht hier ook belang aan. Daarnaast hecht het kabinet ook aan het tegengaan van witwassen en is het dus belangrijk om hier een balans in te vinden. Daar is bij de invulling van deze maatregel, bijvoorbeeld bij de vaststelling van de grens van € 3.000, rekening mee gehouden.

Veel van de reacties zien op de gekozen grens van het verbod en de reikwijdte van de maatregel en vragen om uitbreiding of juist uitzondering van bepaalde diensten (zoals het huren, verhuren en leasen van luxegoederen en diensten) of sectoren (cryptocurrency, waardetransport). Zoals beschreven in paragraaf 2.1 van deze toelichting, zijn deze keuzes gemaakt vanuit het oogpunt van effectiviteit en uitvoerbaarheid en is er bovendien rekening gehouden met het belang van en toegankelijk betalingsverkeer in de samenleving. Ook geven diverse partijen aan dat onvoldoende bewezen is dat deze maatregel effectief zal zijn en dat er gekeken moet worden naar een Europees verbod gezien het mogelijk optreden van waterbedeffecten naar andere landen en sectoren. Hoewel een Europees verbod de voorkeur heeft van het kabinet en het kabinet zich hard maakt voor een verbod op Europees niveau, is bij gebrek hieraan op dit moment gekozen voor een nationaal verbod zoals in het merendeel van de andere lidstaten al van toepassing is. Om tegemoet te komen aan deze reacties en na te gaan of de invulling van de maatregel ook het meest effectief is in de praktijk, is besloten om een evaluatiebepaling op te nemen, waarbij binnen vijf jaar na inwerkingtreding van het wetsvoorstel, het verbod geëvalueerd zal worden op effectiviteit en uitvoerbaarheid. Indien de evaluatie daar aanleiding toe geeft, kan de reikwijdte van de bepaling aangepast worden.

Een aantal partijen merkt op dat dit wetsvoorstel onvoldoende uitvoerbaar is, waarbij zowel de uitvoerbaarheid vanuit de toezichthouder als de uitvoerbaarheid door de winkelier benoemd wordt. Daarnaast wordt gesteld dat er geen extra middelen gereserveerd zijn voor overheidsinstellingen zoals de FIU-Nederland, politie en het Openbaar Ministerie. In paragraaf 4 van deze toelichting is aandacht besteed aan de uitvoerbaarheid en handhaving van deze maatregel. Een verbod dient goed gehandhaafd te worden. Om het witwasprobleem zo goed mogelijk aan te pakken zijn er binnen het plan van aanpak witwassen reeds extra middelen toegekend voor overheidsinstellingen zoals de FIU-Nederland, de politie, en het Openbaar Ministerie. Wat betreft de uitvoerbaarheid voor de winkelier, zou het verbod juist kunnen leiden tot een vermindering aan administratieve lasten. Er hoeft tenslotte geen cliëntenonderzoek meer verricht te worden en er hoeven geen ongebruikelijke transacties meer gemeld te worden bij de FIU-Nederland. Bij de evaluatie van de maatregel zal ook aan deze punten aandacht worden besteed.

§ 6.3 Gegevensdeling tussen instellingen bij cliëntenonderzoek

Veel van de reacties zien op de invulling van de onderzoeksplicht. In reactie hierop is de memorie van toelichting aanzienlijk uitgebreid ten aanzien van deze maatregel. Respondenten gaven, onder andere, aan dat de administratieve lasten onredelijk hoog zouden liggen, aangezien instellingen verplicht worden om bij alle instellingen uit dezelfde categorie navraag te doen. In de wetstekst en toelichting is verduidelijkt dat de onderzoeksplicht een inspanningsverplichting is en dat instellingen

uitsluitend redelijke maatregelen dienen te nemen in het kader van hun onderzoeksplicht. Ter illustratie zijn in de toelichting voorbeelden gegeven van hetgeen als redelijk verondersteld kan worden en waar dat niet voor geldt. Ook gaven respondenten aan dat het onduidelijk is hoe snel een eerdere dienstverlener dient te reageren, welke gegevens uitgewisseld dienen te worden, de relatie met het tipping-off verbod en wat er wordt bedoeld met «gebleken risico's». Ook ten aanzien van deze punten is de memorie van toelichting aangevuld.

Een aantal respondenten geeft aan dat de beperking van deze maatregel tot het verscherpt cliëntenonderzoek onvoldoende risico gebaseerd is en ertoe zou kunnen leiden dat instellingen minder geneigd zouden zijn om verscherpt cliëntenonderzoek uit te voeren. Om tegemoet te komen aan deze reacties is allereerst de tekst van het wetsvoorstel aangepast. De maatregel is uitgebreid naar gevallen waarin een zakelijke relatie of transactie naar haar aard een hoger risico op witwassen of financieren van terrorisme met zich meebrengt, de risicofactoren bedoeld in bijlage III van de vierde anti-witwasrichtlijn van toepassing zijn en als onderdeel van het verscherpt cliëntenonderzoek. Hiermee sluit deze maatregel meer aan bij de risico gebaseerde benadering van de Wwft.

Sommige respondenten stellen voor om onderscheid te maken tussen de verschillende instellingen door de reikwijdte van de maatregel te beperken tot een aantal instellingen of sommige instellingen in plaats van een onderzoeksplicht op te leggen, de bevoegdheid te geven om navraag te doen. De maatregel geldt voor alle instellingen, omdat shopgedrag in alle sectoren voor kan komen. Bovendien zou een beperking tot bepaalde instellingen mogelijk tot een waterbedeffect kunnen leiden. Aangezien de maatregel slechts verplicht tot het treffen van redelijke maatregelen in het kader van de onderzoeksplicht, geeft dit verschillende instellingen ruimte om deze plicht in te richten op een bij de soort instelling passende wijze. Zodoende is de brede reikwijdte van de maatregel gerechtvaardigd. Daarnaast is in de toelichting naar aanleiding van deze reacties aandacht besteed aan de reden voor de keuze voor een onderzoeksplicht in plaats van een bevoegdheid tot het doen van onderzoek. Een verplichting is niet alleen een geëigend middel in het kader van het tegengaan van shopgedrag, het is bovendien noodzakelijk voor de grondslag voor het delen van persoonsgegevens.

Daarnaast geeft een paar respondenten aan een voorkeur te hebben voor een verplichting om een register te voeren. In de toelichting is verduidelijkt dat de huidige wet- en regelgeving er niet aan in de weg staat dat instellingen een gezamenlijk register opstellen en dat dit een effectief middel kan zijn om te voldoen aan de onderzoeksplicht. Een respondent vroeg of de opvolger van een oud notaris verplicht is te voldoen aan de plicht om geconstateerde »risico's op witwassen of financieren van terrorisme te delen indien een andere instelling dat verzoekt. Aangezien de opvolger het cliëntendossier en bijbehorende aktes onder zich heeft gekregen, heeft deze daarmee ook de plicht verkregen om de geconstateerde risico's die uit het dossier blijken te delen met de verzoekende partij.

Voorts stelt een aantal respondenten voor om de mogelijkheid om gegevens te delen te verruimen naar andere categorieën instellingen. Vanwege de proportionaliteit van de maatregel is ervoor gekozen om de maatregel te beperken tot dezelfde categorie instelling. Aangezien het denkbaar is dat in de praktijk blijkt dat gegevensuitwisseling tussen specifieke verschillende categorieën van instellingen wenselijk is, is een grondslag opgenomen in het wetsvoorstel om dergelijke uitzonderingen mogelijk te maken bij lagere regelgeving om tegemoet te komen aan deze

reacties. Daarnaast stelt een aantal respondenten dat onduidelijk is wanneer instellingen tot dezelfde categorie behoren, in het bijzonder de bemiddelaars in uiteenlopende volumineuze goederen uit artikel 1a, vierde lid, onderdeel h. Om hieraan tegemoet te komen, is gekozen om, op basis van de voornoemde grondslag, ook mogelijk te maken om binnen de huidige categorieën nadere groepen instellingen als afzonderlijke categorie aan te wijzen.

Ten slotte vraagt een aantal respondenten aandacht voor de bescherming van cliënten tegen onnodige uitsluiting door instellingen. In reactie hierop wordt in de toelichting aandacht besteed aan dit risico.

§ 6.4 Gezamenlijke transactiemonitoring door banken

Een respondent heeft de suggestie gedaan om aan artikel 10 toe te voegen dat bij verwerking betrokkenen op de hoogte worden gesteld, conform de artikelen 1 tot en met 14 van de AVG. Aangezien de eisen van de artikelen 12 tot en met 14 van de AVG sowieso gelden, is het niet nodig deze nogmaals te regelen in het voorgestelde artikel 10. In de toelichting bij artikel 10 is hier overigens wel naar verwezen.

Een respondent adviseert om de uitbesteding van het cliëntenonderzoek van toepassing te laten zijn op het gehele artikel 3, in plaats van alleen op het eerste en tweede lid van dat artikel. Dit is niet nodig, omdat in de rest van artikel 3 steeds wordt verwezen naar het cliëntenonderzoek als bedoeld in het eerste lid. Daarmee is het hele artikel 3 gedekt als het gaat om de mogelijkheid van uitbesteding aan een derde.

In een van de reacties werd de suggestie gedaan om de mogelijkheid van gezamenlijke transactiemonitoring onder te brengen bij een overheidsentiteit. Hier is niet voor gekozen, aangezien het hierbij gaat om het profiel van de cliënt, die poortwachters kennen en overheidsinstanties niet. Op basis van dat profiel kan een poortwachter het beste beoordelen wat wel en niet gebruikelijk is.

Een van de respondenten stelt voor om in het wetsvoorstel expliciet op te nemen dat de entiteit die de gezamenlijke transactiemonitoring uitvoert, ongebruikelijke transacties mag melden aan de FIU-Nederland en om dit onderdeel van het wetsvoorstel na twee jaar te evalueren. Het eerste voorstel is overgenomen, met de kanttekening dat artikel 33 van de vierde anti-witwasrichtlijn voorschrijft dat instellingen individueel verantwoordelijk zijn voor het melden van ongebruikelijke transacties aan de FIU-Nederland. Naar aanleiding van het tweede voorstel uit deze reactie en het AP-advies is in wetsvoorstel is opgenomen dat bij algemene maatregel van bestuur regels worden gesteld over monitoring van deze maatregel. Dit zal plaatsvinden in de vorm van een verplichting voor banken die deelnemen aan gezamenlijke transactiemonitoring om jaarlijks een verslag te publiceren over de resultaten van de gezamenlijke transactiemonitoring en uit een vijfjaarlijks uit te voeren audit naar de werking van de maatregel.

§ 6.5 Gegevensbescherming

§ 6.5.1 Gegevensdeling tussen instellingen bij cliëntenonderzoek

Een aantal respondenten verzocht om verduidelijking ten aanzien van de gegevensdeling, zoals welke instellingen gegevens dienen uit te wisselen en welke gegevens dienen te worden uitgewisseld. De toelichting is op dit punt aangevuld.

Een aantal respondenten gaf terecht aan dat de verplichte uitwisseling van gegevens een doorbreking vormt van de geheimhoudingsplicht van advocaten en notarissen en dat dit expliciet geregeld dient te worden. Het wetsvoorstel is hierop aangepast.

Ten slotte werd door een aantal van de respondenten aandacht gevraagd voor de positie van de cliënt. In reactie hierop is in de toelichting aandacht besteed aan de verplichting voor instellingen, op grond van de AVG, om hun cliënten te informeren over de verwerking van hun persoonsgegevens en het risico op onnodige uitsluiting van dienstverlening.

§ 6.5.2 Gezamenlijke transactiemonitoring door banken

Een van de respondenten heeft opgemerkt dat omdat het voorgestelde artikel 34b, eerste lid, niet geformuleerd is als een verplichting, artikel 6 eerste lid, onderdeel c, van de AVG niet als grondslag kan dienen. Anderzijds merkte de respondent op dat een verplichting onwerkbaar is. In artikel 3, eerste lid, onderdeel d, is de verplichting voor onder meer banken opgenomen om transacties te monitoren ten behoeve van het uitvoeren van cliëntenonderzoek. Het in het wetsvoorstel voorgestelde artikel 34b maakt het uitsluitend voor banken mogelijk om in het kader van het verplichte cliëntenonderzoek transactiegegevens te delen met andere banken ten behoeve van het gezamenlijk uitvoeren van transactiemonitoring met het oog op het melden van ongebruikelijke transacties aan de FIU-Nederland. Dit vormt een voldoende grondslag voor het verwerken van persoonsgegevens op basis van artikel 6, eerste lid, onderdeel c, AVG. De grondslag is in paragraaf 3.2 onder het kopje «Noodzaak» verduidelijkt.

Een aantal partijen heeft aangegeven dat in het wetsvoorstel te weinig aandacht is besteed aan subsidiariteit en proportionaliteit van de voorgestelde gegevensverwerking voor transactiemonitoring. Naar aanleiding hiervan is in paragraaf 3.2 ingegaan op de afweging van een aantal alternatieve maatregelen voor gezamenlijke transactiemonitoring in het kader van de subsidiariteitstoets. In paragraaf 3.2 is ook de proportionaliteitstoets inzake transactiemonitoring meer uitgebreid. Zo is onder meer aangegeven dat de maatregel beperkt is tot banken.

Een aantal partijen heeft de suggestie gedaan om de onderwerpen die genoemd zijn in het voorgestelde artikel 34b, vierde lid, op te nemen in het wetsvoorstel en niet in een algemene maatregel van bestuur. Het wetsvoorstel regelt een deel van de hier bedoelde onderwerpen thans alleen waar het gaat om de verwerking van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard (voorgesteld artikel 34a, eerste lid, Wwft). Het is niet noodzakelijk en ook niet wenselijk deze onderwerpen geheel te regelen op wetsniveau, aangezien het hier gaat om maatregelen van technische en administratieve aard die mogelijk met enige regelmaat zullen wijzigen en aangepast moeten kunnen worden aan technische ontwikkelingen, zoals op het gebied van gegevensbeveiliging. Regeling op het niveau van een algemene maatregel van bestuur ligt in dat geval meer voor de hand.

Een aantal partijen heeft gewezen op de relatie van de voorgestelde maatregel met het beroepsgeheim van het notariaat en de advocatuur. Nu de voorgestelde maatregel in het wetsvoorstel is beperkt tot banken, en geen betrekking heeft op de advocatuur en notariaat, is deze relatie niet meer aan de orde.

Een respondent heeft gevraagd of poortwachters ook het BSN mogen verwerken in het kader van gezamenlijke transactiemonitoring. Het wetsvoorstel is op dit punt aangepast in de zin dat daarin wordt voorgesteld dat banken die gebruik maken van gezamenlijke transactiemonitoring daarbij ook gebruik mogen maken van het BSN, voor zover zij daar al over beschikken. Dit is toegelicht in paragraaf 3.2 van deze toelichting.

Verder heeft een respondent aangegeven een GEB en een oordeel van de AP onlogisch te vinden, aangezien het parlement op dit punt de afweging maakt. Op grond van artikel 35 van de AVG is het in dit geval verplicht om zowel voor het wetsvoorstel als voor de uitvoering van de maatregel een gegevensbeschermingseffectbeoordeling uit te voeren. Aangezien de voorgestelde maatregel een regeling betreft die gevolgen heeft voor de verwerking van persoonsgegevens, dient het wetsvoorstel voor advies voorgelegd te worden aan de AP. Inmiddels heeft de AP advies uitgebracht.

In een van de reacties werd de suggestie gedaan om de principes en bepalingen van de AVG en UAVG specifiek uit te werken in dit wetsvoorstel, zodat rechtsbescherming en bescherming van persoonsgegevens al in het wetgevingsproces uitgewerkt zijn. In paragraaf 3.2 van deze toelichting is een meer uitgebreide beoordeling en afweging opgenomen van de aspecten en beginselen van gegevensbescherming uit de AVG en de UAVG. Daarbij is met name ingegaan op de beginselen van proportionaliteit en subsidiariteit. Daarnaast is ingegaan op de diverse onderdelen van de voor dit onderdeel van het wetsvoorstel uitgevoerde gegevensbeschermingseffectbeoordeling. Aangezien het wetsvoorstel alleen het delen van transactiegegevens tussen banken ten behoeve van gezamenlijke transactiemonitoring mogelijk maakt, maar niet de uitvoering daarvan regelt, is het aan banken om de principes en bepalingen uit de AVG en UAVG concreet uit te werken en toe te passen bij de uitvoering van de maatregel, indien zij daarvan gebruik willen maken.

Een respondent heeft opgemerkt dat er geen waarborgen in het wetsvoorstel zijn opgenomen voor de verwerking van gegevens van strafrechtelijke aard. Bij algemene maatregel van bestuur zullen onder meer regels worden gesteld over waarborgen op dit punt.

Verder heeft een respondent gevraagd waarom sprake is van een zwaarwegend algemeen belang waardoor instellingen bijzondere categorieën van persoonsgegevens mogen uitwisselen. In paragraaf 2.3. van deze toelichting is de verwerking van bijzondere categorieën van persoonsgegevens en de noodzaak daarvan voor transactiemonitoring toegelicht. Tevens is toegelicht waarom hierbij sprake is van een zwaarwegend algemeen belang. In par. 3.3 is toegelicht waarom verwerking van deze gegevens ook noodzakelijk is voor gezamenlijke transactiemonitoring.

De betreffende respondent heeft verder de suggestie gedaan om het vereiste van strikte noodzakelijkheid van inbreuken op digitale grondrechten toe te passen door nader te specificeren welke bijzondere categorieën van persoonsgegevens noodzakelijk zijn voor transactiemonitoring. In paragraaf 2.3. is aan de hand van voorbeelden toegelicht dat in beginsel verwerking van alle bijzondere categorieën persoonsgegevens aan de orde kunnen zijn voor transactiemonitoring en dat daarom niet op voorhand bepaalde categorieën zijn aan te wijzen die daarvoor gebruikt mogen worden.

Tot slot heeft een aantal partijen gevraagd wat persoonsgegevens van strafrechtelijke aard zijn en waarom deze moeten worden uitgewisseld. Bij persoonsgegevens van strafrechtelijke aard kan in dit verband gedacht worden aan transactiegegevens waaruit blijkt dat de betrokkene strafrechtelijk is veroordeeld. Het is van belang dat deze gegevens kunnen worden uitgewisseld voor gezamenlijke transactiemonitoring, omdat dit gegeven in combinatie met andere gegevens kan leiden tot het oordeel of een transactie als ongebruikelijk aangemerkt moet worden voor een betrokkene.

ARTIKELSGEWIJS

ARTIKEL I *(wijziging Wet ter voorkoming van witwassen en financieren van terrorisme)*

Onderdeel A *(wijziging artikel 1)*

In verband met de vernummering van artikel 1f tot 1g wordt de verwijzing in de definitie van nationale risicobeoordeling gewijzigd.

Onderdeel B *(wijziging artikel 1a)*

Artikel 1a bevat een opsomming van alle instellingen waarop de Wwft van toepassing is. Beroeps- of bedrijfsmatige handelaren in goederen, voor zover zij transacties verrichten boven € 10.000, zijn opgenomen in het vierde lid, onderdeel i. Door het verbod op contante betalingen vanaf € 3.000 voor handelaren in goederen wijzigt de regelgeving voor deze categorie instellingen. Voortaan geldt voor deze categorie instellingen alleen het verbod op het verrichten van contante betalingen vanaf € 3.000, opgenomen in het nieuwe artikel 1f. De overige verplichtingen uit de Wwft komen voor deze categorie instellingen te vervallen. Dit wordt tot uitdrukking gebracht door toevoeging van de zinsnede aan het eerste lid van artikel 1a. In het nieuwe vierde lid, onderdeel i, wordt de Wwft van toepassing verklaard op alle natuurlijke personen, rechtspersonen of vennootschappen die beroeps- of bedrijfsmatig handelen als koper of verkoper van goederen. Nu voor deze groep instellingen de bepalingen uit de Wwft niet meer gelden, behoudens het verbod opgenomen in het nieuwe artikel 1f, is de grens van transacties boven € 10.000 in contanten niet meer relevant, deze vervalt daarom.

Onderdeel C *(nieuw artikel 1f)*

Het nieuwe artikel 1f bevat het verbod, voor natuurlijke personen, rechtspersonen of vennootschappen die beroeps- of bedrijfsmatig handelen als koper of verkoper van goederen, om betaling van deze goederen in contanten voor een bedrag vanaf € 3.000 te verrichten, ongeacht of de transactie plaatsvindt in een handeling of door middel van meer handelingen waartussen een verband bestaat. Het verbod geldt uitsluitend voor natuurlijke personen, rechtspersonen of vennootschappen die beroeps- of bedrijfsmatig handelen als koper of verkoper van goederen. Deze categorie instellingen is opgenomen in artikel 1a, vierde lid, onderdeel i. Op dit moment geldt nog dat deze categorie instellingen, voor zover zij transacties verrichten boven € 10.000 in contanten, aan de verplichtingen uit de Wwft dienden te voldoen met betrekking tot het cliëntenonderzoek en het melden van ongebruikelijke transacties. Met dit wetsvoorstel geldt voor hen op grond van de Wwft alleen nog het verbod om contante betalingen vanaf € 3.000 te verrichten. Naast de algemene categorie handelaren geldt het verbod ook voor handelaren in kunstvoorwerpen en pandhuizen, opgenomen in artikel 1a, vierde lid, onderdelen k en p, voor zover zij goederen aan- of verkopen in

contanten. Aangezien deze instellingen ook voor andere handelingen dan contante transacties onder de wet vallen worden zij niet geheel uitgezonderd (zie toelichting onderdeel B).

Het verbod geldt niet voor particulieren onderling, maar alleen bij transacties tussen ondernemers onderling en tussen ondernemers en consumenten. Er mogen bij een bedrag vanaf € 3.000 geen contante betalingen meer worden verricht, ongeacht of de transactie plaatsvindt door middel van een enkele handeling of door middel van meerdere handelingen waartussen een verband bestaat. Deze eisen zijn identiek aan de huidige grens van € 10.000 in contanten voor deze categorie. De koper of verkoper van goederen moet bij het vaststellen van de hoogte van het bedrag, kijken of er sprake is van meerdere handelingen waartussen een verband bestaat. Indien er voor een instelling aanwijzingen zijn dat er een transactie plaatsvindt door middel van meerdere handelingen waartussen een verband bestaat, dient de instelling zich ervan te vergewissen dat er geen sprake is van een samengestelde transactie voordat de instelling de transacties uitvoert. Dit is om te voorkomen dat het verbod wordt omzeild door transacties op te splitsen. Dit element is reeds opgenomen in het artikel 1a, vierde lid, onder i, waar is opgenomen op welke transacties de Wwft van toepassing is en blijft ook van toepassing op transacties die vallen onder het verbod. Om handvatten te bieden bij de vaststelling of er sprake is van een samengestelde transactie, is in het tweede lid een grondslag opgenomen om bij algemene maatregel van bestuur een niet-limitatieve lijst van indicatoren vast te stellen die hierop kunnen wijzen.

Het verbod geldt voor betalingen in contanten die in of vanuit Nederland worden verricht. Voor de uitleg van «in of vanuit Nederland» geldt dezelfde maatstaf als reeds opgenomen in artikelen 3 en 23a van de wet. Een transactie wordt «in of vanuit» Nederland verricht wanneer (een deel van) de transactie in Nederland plaatsvindt. Hierbij wordt benadrukt dat «transactie» breder is dan de betaling. Het ziet op de volledige handeling van aanbieden van een goed in ruil voor contant geld. Zo is het verbod van toepassing indien een in Nederland geregistreerde instelling in Nederland goederen aanbiedt en de betaling in Nederland plaatsvindt. Het verbod is tevens van toepassing indien een instelling in Nederland geregistreerd is en vanuit Nederland goederen aanbiedt, ook als de betaling over de grens geschiedt. Het verbod is eveneens van toepassing als de instelling in het buitenland geregistreerd is en vanuit het buitenland goederen aanbiedt en de betaling in Nederland plaatsvindt. In de laatste twee gevallen vindt een deel van de transactie in Nederland plaats, waardoor het verbod van toepassing is.

Onderdeel D *(wijziging artikel 3)*

In artikel 3 vervalt het zesde lid, waarin de verplichtingen uit de Wwft voor instellingen als bedoeld in artikel 1a, vierde lid, onderdeel i zijn neergelegd. In navolging hiervan worden het zevende tot en met het veertiende lid vernummerd tot het zesde tot en met het dertiende lid.

Onderdeel E *(nieuw artikel 3b)*

Het nieuwe artikel 3b bevat de verplichting voor instellingen om bij cliëntenonderzoek te onderzoeken of de cliënt heeft verzocht om dienstverlening bij een instelling uit dezelfde categorie, indien een instelling indicaties heeft dat de zakelijke relatie of transactie naar haar aard een hoger risico op witwassen of financieren van terrorisme met zich brengt. Wanneer dit het geval is moet de instelling navraag doen bij die

instelling. Een vergelijkbare regeling is opgenomen in artikel 68 van de Wet toezicht trustkantoren 2018, deze bepaling blijft gelden voor trustkantoren.

De verplichting opgenomen in het eerste lid bestaat uit verschillende componenten, deze worden hieronder toegelicht. Een instelling dient op grond van artikel 3 van de wet voorafgaand aan het aangaan van de zakelijke relatie of transactie een inschatting te maken van de risico's op witwassen of financieren van terrorisme die dit met zich brengt. Wanneer er sprake is van verhoogd risico is omschreven in het eerste lid, onder a tot en c. Indien er sprake is van indicaties van een hoger risico, dient de instelling te onderzoeken of de cliënt eerder bij een andere instelling diensten heeft afgenomen of is geweigerd. Deze onderzoeksplicht van het eerste lid van de voorgestelde bepaling is een inspanningsverplichting. Dit houdt in dat een instelling redelijke maatregelen moet nemen om deze te achterhalen. Wat redelijk is hangt af van de context, voor de hand ligt dat de instelling in ieder geval bij de cliënt zelf informeert. Voorts kan een instelling gebruik maken van openbare bronnen of binnen een bepaalde beroepsgroep aanwezige registers. Zie paragraaf 2.2.1.2 van het algemeen deel voor verdere toelichting op de inspanningsverplichting. Deze verplichting ontstaat op het moment dat de instelling op grond van zijn eigen risico gebaseerde reguliere cliëntenonderzoek indicaties heeft dat de zakelijke relatie of transactie naar haar aard een hoger risico op witwassen of financieren van terrorisme met zich meebrengt, omschreven onder punten a tot en met c. Niet alleen bij aanvang van de zakelijke relatie, maar ook gedurende die zakelijke relatie kan er aanleiding bestaan om de cliënt aan een aanvullend onderzoek te onderwerpen, als er indicaties opkomen van betrokkenheid bij witwassen of financieren van terrorisme. Dit volgt uit de bestaande verplichting van artikel 3, elfde lid, om de gegevens verzameld in het kader van het cliëntenonderzoek te actualiseren. Ook in de gevallen dat een instelling gedurende de zakelijke relatie cliëntenonderzoek verricht en indicaties heeft dat er sprake zou kunnen zijn van een hoger risico, moet deze instelling onderzoek doen naar eerdere dienstverlening door andere instellingen uit dezelfde categorie.

Indien een instelling vaststelt dat bij een zakelijke relatie of transactie indicaties zijn van een hoger risico op witwassen of financieren van terrorisme, dient een instelling redelijke maatregelen te nemen om te onderzoeken of een instelling uit dezelfde categorie diensten verleent of heeft verleend, dan wel heeft geweigerd, aan deze cliënt. De verplichting is geen onderdeel van regulier cliëntenonderzoek, maar alleen indien in het kader daarvan indicaties op een hoger risico worden vastgesteld. Daarmee resulteert deze verplichting in wezen tot een nieuwe categorie cliëntenonderzoek tussen het reguliere cliëntenonderzoek en het verscherpt cliëntenonderzoek in.

Deze verplichting geldt in drie gevallen gegeven in onderdelen a tot en met c, te weten: a) indien 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, welke is 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. Het eerste geval wanneer de verplichting geldt, onderdeel a, is een subjectieve indicator. Hier is sprake van wanneer een instelling indicaties

heeft dat een zakelijke relatie of transactie een hoger risico op witwassen of financieren van terrorisme met zich brengt. Deze toets is vergelijkbaar met de subjectieve indicator voor ongebruikelijk transacties, waarbij van de instelling zelf gevergd wordt een inschatting te maken. Het tweede geval wanneer deze verplichting geldt, onderdeel b, is indien de in bijlage III van de vierde anti-witwasrichtlijn genoemde risicofactoren van toepassing zijn op de zakelijke relatie of transactie. Hierbij is sprake van meer objectieve indicaties op een hoger risico. Dit zijn bijvoorbeeld indien een cliënt afkomstig uit een hoog-risico land of indien een transactie in contanten plaatsvindt. Tot slot dient een instelling de verplichting altijd uit te voeren als onderdeel van het verscherpt cliëntenonderzoek. Bij verscherpt cliëntenonderzoek heeft een instelling immers reeds vastgesteld dat er sprake van een hoog risico. Dit is vastgelegd in onderdeel c.

De verplichting tot onderzoek strekt zich alleen uit tot instellingen behorend tot dezelfde categorie als de instelling zelf. Voor de indeling van deze categorieën wordt aangesloten bij de indeling uit artikel 1a, tweede, derde en vierde lid, van de Wwft. Banken als bedoeld in artikel 1a, tweede lid, van de Wwft worden als één categorie aangemerkt. Voor de financiële ondernemingen zoals opgesomd in de subonderdelen van artikel 1a, derde lid, van de Wwft geldt dat elk subonderdeel als afzonderlijke categorie wordt aangemerkt. Voor de overige instellingen zoals opgesomd in de subonderdelen van artikel 1a, vierde lid, geldt eveneens dat elk subonderdeel als afzonderlijke categorie wordt aangemerkt.

Het derde lid schrijft voor welke gegevens de verzoekende instelling dient te verstrekken ter mogelijke identificatie van de cliënt. Hiervoor is aangesloten bij de gegevens voorgeschreven in artikel 33, tweede lid, onderdelen a en c van de wet. Deze twee onderdelen bevatten de gegevens die een instelling dient vast te leggen bij het cliëntenonderzoek van natuurlijke personen en rechtspersonen. Deze omvatten voor natuurlijke personen onder meer de naam, geboortedatum, adres, woonplaats alsmede de gegevens van het document waarmee de persoon is geïdentificeerd. Voor rechtspersonen omvatten deze onder meer de naam, adres, land van statutaire zetel en, indien van toepassing, het registratienummer bij de Kamer van Koophandel. Daarnaast geldt dat ook de geregistreerde bestuurders van de rechtspersoon worden verstrekt. Aansluiting bij artikel 33 is noodzakelijk op basis van twee redenen. Ten eerste wordt hiermee de set gegevens beperkt, instellingen verzamelen deze gegevens immers al in het kader van cliëntenonderzoek en zullen dus reeds aanwezig zijn bij zowel de verzoekende instelling als de instelling die het verzoek ontvangt. Ten tweede garandeert deze set gegevens dat beide instellingen met zekerheid kunnen vaststellen dat het om dezelfde cliënt gaat en wordt voorkomen dat er uitwisseling van de verkeerde cliënt plaatsvindt of onterecht geconstateerd wordt dat het niet dezelfde cliënt betreft.

Het vierde lid schrijft voor dat een instelling die door een andere instelling wordt verzocht om informatie over een (eerdere) cliënt, is gehouden informatie over gebleken risico's op witwassen of financieren van terrorisme onverwijld te verstrekken indien deze hebben geleid tot maatregelen om deze risico's te beheersen, waaronder in ieder geval wordt verstaan het weigeren of beëindigen van de dienstverlening. Voor zover er informatie over geconstateerde risico's wordt gedeeld, is het mogelijk dat hier persoonsgegevens van strafrechtelijke aard onderdeel van uitmaken. Dergelijke gegevens zijn relevant bij de afweging of de cliënt wel of niet aanvaard kan worden. Op grond van artikel 33, tweede lid, onderdeel a, van de UAVG is het instellingen toegestaan om zelf persoonsgegevens van strafrechtelijke aard te verwerken om te kunnen beoordelen of op grond van de Wwft diensten verleend kunnen worden

aan de cliënt. Het kunnen delen van die persoonsgegevens van strafrechtelijke aard met andere instellingen is echter een afzonderlijke verwerking waarvoor een aparte grondslag is vereist. Het derde lid bevat die grondslag. Deze wettelijke grondslag past binnen de uitzonderingen om persoonsgegevens van strafrechtelijke aard te verwerken in artikel 10 van de AVG. Voorts geldt de bewaartermijn van minimaal vijf jaar, opgenomen in artikel 33, derde lid, van de Wwft onverkort. Voor de termijn tot wanneer deze verplichting geldt wordt daarom aangesloten bij deze termijn. Dat houdt in dat een instelling die een verzoek ontvangt alleen hoeft te informeren over geconstateerde risico's tot vijf jaar na beëindiging van de zakelijke relatie. Daarnaast heeft deze verplichting geen terugwerkende kracht, zie daarvoor de toelichting op artikel III.

Omdat het hier vertrouwelijke gegevens over individuele cliënten betreft, dienen de cliënten van instellingen alvorens een zakelijke relatie aan te gaan met de instelling van de diensten geïnformeerd te worden over deze wettelijke verplichting voor instellingen. Dit wordt voorgeschreven in het vijfde lid. Ook reeds bestaande cliënten dienen hierover geïnformeerd te worden. Dit kan individueel of middels een wijziging van de algemene voorwaarden. Zodoende wordt voorkomen dat het nakomen van deze verplichting kan leiden tot een schending van een contractuele verplichting tot vertrouwelijkheid van deze cliënten. Daarbij is van belang dat de verplichting alleen geldt voor risico's op witwassen of financieren van terrorisme die na inwerkingtreding van dit wetsvoorstel zijn gebleken.

In het zesde lid is een grondslag opgenomen om bij algemene maatregel van bestuur de groep instellingen waarbij een instelling onderzoek moet doen over gebleken risico's op witwassen of financieren van terrorisme bij een cliënt te beperken of te verruimen. Ten eerste kan deze groep beperkt worden tot een specifieke groep instellingen binnen een bestaande categorie. Zo bestaat de mogelijkheid dat instellingen ingedeeld zijn in een categorie omdat zij vergelijkbare diensten aanbieden, maar dat deze instellingen in de praktijk in een andere sector opereren en een andere clientèle bedienen. In een dergelijk geval heeft de verplichting om geconstateerde risico's op witwassen of financieren van terrorisme uit te wisselen vermoedelijk weinig meerwaarde en kan deze verplichting onnodig belastend zijn voor de instellingen in kwestie. Hierbij kan gedacht worden aan de categorie «bemiddelaars», uit artikel 1a, vierde lid, onderdeel j, waar zowel bemiddelaars in schepen als juweliers onder vallen. Daarnaast kan de groep instellingen uitgebreid worden naar andere categorieën. Indien instellingen onderverdeeld in verschillende categorieën vergelijkbare diensten aanbieden en daarbij vergelijkbare cliënten bedienen dan kan dit wenselijk zijn. Een voorbeeld hiervan is het aanbieden van beleggingsdiensten die door zowel beleggingsondernemingen, beleggingsinstellingen en banken kunnen worden aangeboden. In dergelijke gevallen is het denkbaar dat risico's op witwassen of financieren van terrorisme geconstateerd bij een cliënt door een instelling uit een categorie relevant zijn voor de risicoafweging voor een instelling uit een andere categorie.

In het zevende lid is opgenomen dat de geheimhoudingsplicht voor advocaten en notarissen niet van toepassing is bij het voldoen aan een verzoek van een verzoekende instelling als bedoeld in het derde lid. Aangezien de verplichting alleen geldt voor instellingen uit dezelfde categorie onderling zal de verzoekende instelling altijd, respectievelijk, een andere advocaat of notaris zijn. Advocaten en notarissen zijn respectievelijk volgens artikel 11a van de Advocatenwet en artikel 22 van de Wet op het notarisambt gehouden aan een geheimhoudingsplicht. In afwijking van de geheimhoudingsplicht, dient de advocaat of notaris bij een verzoek als bedoeld in het derde lid de risico's op witwassen of

financieren van terrorisme bij de cliënt gebleken uit het cliëntenonderzoek in kwestie te verstrekken aan de verzoekende instelling. Artikel 1a, vijfde lid, schrijft voor dat de verplichtingen uit de Wwft niet van toepassing zijn in de gevallen waarin een advocaat of notaris wanneer zij voor een cliënt werkzaamheden verrichten betreffende de bepaling van diens rechtspositie, diens vertegenwoordiging en verdediging in rechte, het geven van advies voor, tijdens en na een rechtsgeding of het geven van advies over het instellen of vermijden van een rechtsgeding. Gegevens die daarmee verband houden mogen niet gedeeld worden. Advocaten en notarissen zijn vanwege hun geheimhoudingsplicht ook uitgezonderd van de mogelijkheid om bij algemene maatregel van bestuur categorieën instellingen aan te wijzen waarvoor de verplichting zich ook uitstrekt tot andere categorieën instellingen gegeven in het zesde lid.

Onderdeel F *(wijziging artikel 5)*

De vernummeringen in artikel 5 hangen samen met het vervallen van de verplichtingen uit de Wwft voor instellingen om cliëntenonderzoek en meldingen te doen, als bedoeld in artikel 1a, vierde lid, onderdeel i.

Onderdeel G *(wijziging artikel 10)*

Op grond van artikel 10 van de Wwft is het instellingen toegestaan om onderdelen van het cliëntenonderzoek uit te besteden aan een derde partij. Van belang daarbij is dat de verantwoordelijkheid bij de uitbestedende instelling blijft liggen; alles wat de derde partij doet, doet deze namens de uitbestedende instelling. Op grond van de huidige Wwft is het niet mogelijk om het uitoefenen van de voortdurende controle op de zakelijke relatie en tijdens de duur van deze relatie verrichte transacties, uit te besteden. De (gewijzigde) vierde anti-witwasrichtlijn staat niet in de weg aan het uitbesteden van dit onderdeel van het cliëntenonderzoek, waaronder de transactiemonitoring. Middels de wijziging van artikel 10 wordt het nu mogelijk gemaakt voor banken als bedoeld in artikel 34b, eerste lid, om een gezamenlijke voorziening voor het monitoren van transacties op te richten of eraan deel te nemen. Hiertoe wordt in het nieuwe tweede lid banken die de gezamenlijke voorziening op hebben gericht of die eraan deelnemen de bevoegdheid gegeven om transactiemonitoring, opgenomen in artikel 3, tweede lid, onderdeel d, uit te besteden aan de gezamenlijke voorziening. Het uitgangspunt dat de instelling zelf verantwoordelijk is, blijft ongewijzigd.

Indien een instelling verplichtingen uitbesteed waarbij persoonsgegevens worden verwerkt, wordt deze verwerking door een derde partij namens de verwerkingsverantwoordelijke verricht. De instelling blijft bij uitbesteding immers de verwerkingsverantwoordelijke. De partij waaraan de gegevensverwerking wordt uitbesteed is de verwerker. Indien meerdere instellingen dezelfde verplichtingen uitbesteden aan dezelfde partij, verdient dit vereiste extra aandacht. Bij dergelijke afspraken dienen de zelfstandige verantwoordelijkheden van de instellingen adequaat afgebakend van elkaar vastgelegd te worden. Daarbij is het van belang dat de instelling die verplichtingen uitbesteedt, dit ook periodiek controleert. Zowel de instelling als de derde partij dienen zich hierbij te houden aan artikel 28 en de overige relevante voorschriften van de AVG. In dat kader geldt onder meer dat instellingen ook verplicht zijn betrokkenen te informeren over de uitbesteding van de verwerking aan een derde, conform de artikelen 12 tot en met 14 van de AVG.

Aan het uitbesteden van werkzaamheden zijn risico's verbonden die adequaat moeten worden beheerst. Dit geldt voor alle vormen van uitbesteding, in het bijzonder voor controle op de zakelijke relatie en

transactiemonitoring. Controle op de zakelijke relatie en transactiemonitoring is geen momentopname, maar betreft een voortdurend proces. Tevens worden er in dit kader voortdurend persoonsgegevens van de cliënt verwerkt. Uitbesteding van dit onderdeel van het cliëntenonderzoek aan een derde partij dient daarom met extra waarborgen omkleed te zijn. Daartoe kan bij of krachtens algemene maatregel van bestuur nader worden bepaald onder welke voorwaarden de uitbesteding van werkzaamheden kan plaatsvinden in het nieuwe vierde lid. Ten eerste kan het hierbij gaan om voorwaarden om adequaat toezicht door de Wwft-toezichthouder op de naleving van de verplichting te garanderen. Voorts kunnen aanvullende waarborgen worden voorgeschreven om risico's die voortkomen uit de uitbesteding adequaat te beheersen. Tot slot kunnen nadere regels gesteld worden over de uitbestedingsovereenkomst.

Onderdeel H *(wijziging artikel 16)*

In verband met de vernummering van de leden in artikel 3 wordt de verwijzing naar artikel 3, veertiende lid, vervangen door dertiende lid.

Onderdelen I en J *(wijzigingen artikelen 29 en 30)*

In deze onderdelen wordt geregeld dat bij overtreding van de verplichtingen in de nieuw voorgestelde artikelen 1f, 3b, 34b en het gewijzigde artikel 10, derde en vierde lid van de Wwft, de aangewezen toezichthouder een last onder dwangsom of een bestuurlijke boete kan opleggen. Het betreft overtredingen van het verbod voor beroeps- en bedrijfsmatige handelaren als kopers en verkopers in goederen om contante betalingen vanaf een bedrag vanaf € 3.000 te verrichten uit het voorgestelde artikel 1f, de verplichting voor een instelling om onderzoek te doen naar eerdere dienstverlening door andere instellingen uit het voorgestelde artikel 3b, de verplichtingen voor instellingen in het kader van gezamenlijke transactiemonitoring uit artikel 34b en de voorgestelde verplichtingen omtrent uitbesteding uit artikel 10.

Onderdeel K *(wijziging artikel 34a)*

Middels het voorgestelde nieuwe eerste lid in artikel 34a wordt de grondslag voor het verwerken van persoonsgegevens in het kader van deze wet verduidelijkt. Daarbij wordt geregeld dat het toegestaan is om bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard te verwerken indien dit noodzakelijk is voor een instelling om te voldoen aan de verplichtingen van de wet. Op grond van artikel 9, tweede lid, onderdeel g, van de AVG is het verbod om bijzondere categorieën van persoonsgegevens als bedoeld in artikel 1 van de UAVG te verwerken niet van toepassing indien de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht. Het voldoen aan de verplichtingen van de Wwft is aan te merken als een zwaarwegend algemeen belang. Op grond van artikel 10 van de AVG is het verwerken van persoonsgegevens van strafrechtelijke aard slechts mogelijk in een beperkt aantal gevallen, waaronder indien dat is toegestaan bij lidstatelijke bepalingen. Met het voorgestelde nieuwe eerste lid van artikel 34a wordt van de in artikel 9, tweede lid, onderdeel g, en artikel 10 van de AVG geboden uitzonderingsmogelijkheden gebruik gemaakt.

De kern van het voorgestelde nieuwe eerste lid is dat de verwerking alleen toegestaan is indien dit noodzakelijk is voor het uitvoeren van een verplichting uit de Wwft, te weten het (doorlopend) cliëntenonderzoek uit hoofdstuk 2 of het melden van ongebruikelijke transacties uit hoofdstuk 3.

Het uitgangspunt van de Wwft is dat instellingen zelf risico's in hun dienstverlening identificeren en daarop hun cliëntenonderzoek aanpassen. De aard en achtergrond van de risico's kunnen niet op voorhand voorspeld worden en zijn voortdurend aan veranderingen onderhevig. Criminelen zijn immers voortdurend op zoek naar nieuwe kanalen en constructies om toegang te verkrijgen tot het financiële stelsel. Van instellingen wordt verwacht dat zij hierop inspelen. Hieruit kan volgen dat op basis van de geconstateerde risico's de gerichte verwerking van specifieke gegevens noodzakelijk is of dat de geconstateerde risico's bij een specifieke cliënt samenhangen met bijzondere categorieën persoonsgegevens of persoonsgegevens van strafrechtelijke aard. Zie voor een uitgebreide toelichting op deze verplichtingen paragrafen 2.3 en 3.3 van het algemeen deel van deze toelichting. Uit het bovenstaande volgt dat het voor instellingen alleen is toegestaan om bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard te verwerken indien dat noodzakelijk is om aan de verplichtingen te voldoen, gesteld bij of krachtens deze wet. Instellingen dienen zelfstandig te beoordelen in welke mate gegevensverwerking noodzakelijk is om aan die verplichtingen te voldoen.

Met het voorgestelde vijfde lid wordt instellingen de verplichting opgelegd om mogelijke verwerking van bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard te documenteren en de noodzakelijkheid van de verwerking om aan de verplichtingen uit de wet te voldoen te onderbouwen. Allereerst dient een instelling zelfstandig na te gaan of hij bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard (mogelijk) verwerkt om te voldoen aan de verplichtingen van de Wwft. Indien dit het geval is dient een instelling deze verwerking(en) te documenteren. In deze documentatie dient, in ieder geval, te worden opgenomen welke bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard de instelling verwerkt, de wijze van verwerking, de verplichting op grond waarvan deze verwerking plaatsvindt en waarom de verwerking van bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard daarvoor noodzakelijk is. Deze documentatie hoeft niet afzonderlijk per verwerking plaats te vinden. De documentatie dient inzichtelijk te maken waarom, gelet op aard en omvang van de dienstverlening en afhankelijk van de specifieke dienstverlening, de instelling bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard worden verwerkt of verwacht te verwerken om aan de verplichtingen van de Wwft te voldoen. Een algemeen voorbeeld van dergelijke noodzakelijke verwerking is het monitoren van transacties waarin bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard (kunnen) voorkomen die met name voor betaaldienstverleners opgeld doet. Een specifiek voorbeeld zou kunnen zijn dat een instelling op basis van risicoprofielen extra aandacht heeft voor bepaalde categorieën van persoonsgegevens, bijvoorbeeld in het kader van zorgfraude. Voor een verdere toelichting wordt nogmaals verwezen naar paragrafen 2.3 en 3.3 van het algemeen deel van deze toelichting. Het voorgestelde zesde lid verplicht de instelling om cliënten te informeren over mogelijke verwerking van bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard conform artikelen 13 en 14 van de AVG. Het gaat hierbij niet zozeer over elke specifieke verwerking van de persoonsgegevens van de betreffende cliënt, maar hoe en waarom de instelling in het kader van zijn dienstverlening en verplichting op grond van de Wwft in zijn algemeenheid genoodzaakt kan zijn bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard te verwerken. Hierbij kan verwezen worden naar de eerder beschreven documentatie. De instelling dient de cliënt te informeren voor

aanvang van de dienstverlening en – indien van toepassing – gedurende de dienstverlening bij wijziging van het beleid.

Met het voorgestelde zevende lid van artikel 34a wordt invulling gegeven aan het bepaalde in artikel 9, tweede lid, onderdeel g, van de AVG betreffende passende en specifieke maatregelen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene en het bepaalde in artikel 10 van de AVG, betreffende passende waarborgen voor de rechten en vrijheden van de betrokkenen. Het betreft hier een uitwerking van de regels ter waarborging van de persoonlijke levenssfeer van de betrokkene, zoals gegeven in de AVG en UAVG. Bij de bij algemene maatregel van bestuur te stellen regels over de beveiliging van persoonsgegevens kan gedacht worden aan regels over de toegang tot bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard. Bij te stellen regels over de uitoefening van rechten van betrokkenen kan gedacht worden aan regels over de wijze waarop betrokkenen hun recht op inzage, rectificatie, verwijdering en beperking van de verwerking van hun gegevens (hoofdstuk III AVG) kunnen uitoefenen en bij welke partij, alsmede aan de openstaande rechtsbescherming tegen een beslissing op de uitoefening van een recht als hiervoor genoemd.

Onderdeel L *(nieuw artikel 34b)*

Het nieuwe artikel 34b voorziet in een kader voor een gezamenlijke voorziening opgezet door banken ten behoeve van transactiemonitoring. Op grond van het eerste lid kunnen banken een gezamenlijke voorziening oprichten of eraan deelnemen om te voldoen aan de verplichting uit artikel 3, tweede lid, onderdeel d, om transacties voortdurend te controleren. De zinssnede «of aan een gezamenlijke voorziening deelnemen» expliciteert dat het ook mogelijk is voor banken die niet betrokken zijn bij de oprichting van de gezamenlijke voorziening deel te nemen aan het gezamenlijk monitoren van transacties binnen de gezamenlijke voorziening. Alle verplichtingen van artikel 34b zijn ook en in dezelfde mate van toepassing op de banken die na de oprichting toetreden tot de gezamenlijke voorziening. Dit betekent dat hun rol binnen de voorziening zodanig dient te zijn vormgegeven, dat zij aan deze verplichtingen dienen te kunnen voldoen.

De voorgestelde maatregel schrijft voor dat indien banken gezamenlijke transactiemonitoring willen gaan uitvoeren, dit plaats dient te vinden binnen een daartoe opgerichte gezamenlijke voorziening. Hier is voor gekozen, omdat de bestaande systemen van banken voor het uitvoeren van transactiemonitoring niet ontworpen zijn voor gedecentraliseerde transactiemonitoring en gedecentraliseerde systemen onvoldoende geschikt zijn voor complexe analyses van grote hoeveelheden gegevens die zich op verschillende locaties bevinden. Daarnaast betekent een gedecentraliseerd systeem dat grote hoeveelheden gegevens vanuit verschillende locaties geïntegreerd en beveiligd moet worden, hetgeen zeer complex en kostbaar is. Een gecentraliseerd model heeft derhalve minder impact op de bestaande systemen van banken. Het gebruik van een dergelijke voorziening is een vorm van uitbesteding door de deelnemende banken op grond van artikel 10, tweede lid. De activiteiten van de gezamenlijke voorziening zien immers op de verplichting om een voortdurende controle op de zakelijke relatie en de tijdens de duur van deze relatie verrichte transacties uit te oefenen en zijn daarmee onderdeel van de verplichting opgenomen in artikel 3, tweede lid, onderdeel b. Aangezien het oprichten van een gezamenlijke voorziening geldt als uitbesteding, houdt dit tevens in dat hoofdstuk 5 van het Besluit prudentiële regels van toepassing is op de uitbesteding. Het lid heeft de vorm

van een bevoegdheid in plaats van een verplichting, omdat banken zelf het beste in staat zijn om op basis van hun cliëntenbestand en de door hun cliënten verrichte transacties in te schatten wat de mogelijke risico's zijn op witwassen en terrorismefinanciering en hoe deze risico's gemitigeerd dienen te worden, is het aan de individuele banken om te bepalen of het gezamenlijk monitoren van transacties voor hen noodzakelijk is om te voldoen aan genoemde wettelijke verplichtingen van de Wwft.

In het tweede lid is opgenomen dat banken binnen deze gezamenlijke voorziening gegevens betreffende transacties kunnen combineren. Uit de twee eerste leden volgt dat de gegevens alleen voor het uitvoeren van transactiemonitoring mogen worden gebruikt. Ingevolge de richtlijn blijft de uitbestedende instelling verantwoordelijk voor het uitvoeren van deze verplichting. Het eerste en tweede lid van artikel 34b bieden ook geen grondslag voor verdere verwerking van transactiegegevens voor andere (commerciële) doeleinden. In de leden drie tot en met zeven wordt dit kader nader ingevuld door voor te schrijven welke gegevens gecombineerd mogen worden, welke beperkingen hier aan verbonden zijn, welke waarborgen in acht dienen te worden genomen, hoe verantwoording plaatsvindt en enkele specifieke organisatorische waarborgen.

Het zogenaamde *tipping-off* verbod uit artikel 23 van de Wwft is onverminderd van toepassing op meldingen die zijn gedaan op basis van dit artikel. Dit betekent dat als een transactie als ongebruikelijk wordt aangemerkt, bijvoorbeeld omdat deze als zodanig kwalificeert ten opzichte van transacties of gegevens bij andere banken en die transactie bij de FIU-Nederland wordt gemeld, de banken elkaar hier niet over mogen informeren, behoudens de uitzonderingen zoals opgenomen in het zesde lid van voornoemd artikel van de Wwft. Het melden van ongebruikelijke transacties blijft de verantwoordelijkheid van de individuele instellingen.

In het algemeen deel van de toelichting is reeds opgemerkt dat het combineren van transactie van meerdere banken risico's voor de bescherming van persoonsgegevens met zich brengt, onder andere omdat het kan gaan om grote hoeveelheden data. Het is daarom van wezenlijk belang dat de voorschriften van de AVG hierbij in acht worden genomen. Hiervoor wordt verwezen naar paragraaf 3.2 van het algemeen deel van deze toelichting. Het is te allen tijde de verantwoordelijkheid van de bank om volledig te voldoen aan de eisen van de AVG en overige regelgeving ter bescherming van persoonsgegevens. Op grond van artikel 9 en 10 van de AVG dienen de banken waarborgen te garanderen met betrekking tot de beveiliging van gegevens, de bewaartermijn en hoe de uitoefening van de rechten van betrokkenen kan worden geborgd en wie waar verantwoordelijk voor is. Met betrekking tot de verwerking van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard geldt daarbij ingevolge voornoemde artikelen ook dat specifieke en passende maatregelen dan wel passende waarborgen moeten worden geboden ter bescherming van de rechten en vrijheden van betrokkenen.

In het derde lid is een grondslag voorzien om bij algemene maatregel van bestuur de gegevens vast te stellen welke binnen de gezamenlijke voorziening gecombineerd mogen worden. Alleen deze gegevens kunnen binnen de gezamenlijke voorziening gecombineerd worden. In het tweede lid is dit reeds beperkt tot alleen die gegevens die noodzakelijk zijn om te voldoen aan de verplichting om transacties te controleren. In het derde lid is voorgeschreven waarop deze gegevens uitsluitend betrekking hebben. Dit zijn ten eerste de gegevens die reeds onderdeel uitmaken van de reguliere transactiegegevens, deze zijn gegeven in onderdelen a tot en met d. Onderdeel a ziet op gegevens ten aanzien van de identiteit van de

cliënt, waaronder bijvoorbeeld de naam en adresgegevens kunnen vallen. Deze gegevens zijn vereist om te verzekeren dat de gecombineerde transacties binnen de voorziening daadwerkelijk verband met elkaar houden en niet personen met dezelfde naam of adresgegevens onterecht gekoppeld worden. Het komt namelijk voor dat personen dezelfde voor- en achternaam delen. Daarnaast kunnen personen hetzelfde adres delen omdat ze samenwonen of men een verhuizing niet aan de bank heeft doorgegeven. In principe verzekert het gebruik van het BSN binnen de voorziening onterechte koppeling, maar niet elke cliënt beschikt over een BSN. Indien deze gegevens niet gecombineerd zouden kunnen worden, zou dit er toe kunnen leiden dat transacties ten onrechte aan elkaar gekoppeld worden, hetgeen de werking van de voorziening fundamenteel zou ondermijnen. Deze gegevens worden binnen de voorziening gepseudonimiseerd en versleuteld, zie daarvoor de toelichting op het vierde lid. Onderdeel b en c betreffen de transactie- en productinformatie. Transactie-informatie houdt onder meer de hoogte van de transactie, de valuta waarin de transactie wordt uitgevoerd en welke bank de transactie uitvoert in. Deze informatie is essentieel om binnen de gezamenlijke voorziening adequaat de transacties te kunnen beoordelen om vast te stellen dat er sprake is van mogelijke indicaties op witwassen en deze terug te koppelen aan de betrokken bank. Productinformatie betreft de producten waar de transactie direct aan verbonden is, bijvoorbeeld betaalrekeningen, beleggingsrekeningen, spaarrekeningen en leningen. Deze informatie is van belang om context te geven aan de transactie en nodig om vast te stellen of er indicaties zijn van ongebruikelijke transactiepatronen. Transactiepatronen van een reguliere betaalrekening en een beleggingsrekening lopen immers uiteen. Tot slot is in onderdeel d gegeven dat ook door de instelling reeds vastgestelde risico-indicatoren binnen de voorziening gecombineerd bij algemene maatregel van bestuur vastgesteld worden. Aangezien binnen de voorziening de transactiegegevens gepseudonimiseerd zijn en het niet is toegestaan andere informatie over de cliënt te verwerken, zal dit betekenen dat niet alle mogelijke reeds geïdentificeerde risico's naar voren komen op basis van louter de transactiegegevens. Deze zijn echter wel relevant voor het effectief identificeren van ongebruikelijke transactiepatronen. Teneinde hieraan tegemoet te komen, kunnen deze risico-indicatoren bij algemene maatregel van bestuur vastgesteld worden. Deze indicatoren dienen generiek te worden omschreven en niet herleidbaar te zijn tot personen. Voorbeelden hiervan zijn indicatoren dat een cliënt actief is een bepaalde hoog-risicosector, afkomstig is uit een hoog-risico jurisdictie of onderdeel uitmaakt van een ondoorzichtige bedrijfsstructuur.

In het vierde lid is een beperking opgenomen ten aanzien van verwerking van transactiegegevens van particuliere personen binnen de gezamenlijke voorziening. Onder particuliere personen worden verstaan: natuurlijke personen die transacties uitvoeren voor niet-zakelijke doeleinden. In de praktijk komt dit neer op transacties uitgevoerd vanaf een privérekening. De verwerking van de gegevens voor deze transacties wordt op twee manieren beperkt. Ten eerste is het niet toegestaan om binnen de voorziening transactiegegevens van transacties tussen particulieren onderling onder de € 100 te combineren. Dit zijn bijvoorbeeld overmakingen tussen kennissen onderling. Deze beperking is gegeven onder a. Deze transacties blijven dus geheel buiten de voorziening. Daarnaast wordt het combineren van de transactiegegevens van transacties tussen particuliere personen en een zakelijke rekening onder de € 100 beperkt. Van deze transacties mogen van de particulier uitsluitend het IBAN-nummer (het rekeningnummer), het BIC-nummer (de bank identificatie code) en de landencode gecombineerd worden. Dit is gegeven onder b. Deze beperkte set gegevens is vereist om mogelijk relevante transactiepatronen vanaf een zakelijke rekening te kunnen

herkennen. Bijvoorbeeld wanneer een onderneming zeer regelmatig kleine overboekingen doet naar dezelfde privérekening die tezamen een aanzienlijk bedrag vertegenwoordigen, hetgeen een indicatie kan zijn van witwassen, of wanneer een zakelijke rekening regelmatig kleine overboekingen doet naar landen met een erkend hoog risico op terrorisme, hetgeen kan duiden op terrorismefinanciering.

In het vijfde lid is de grondslag opgenomen voor het gebruik van het BSN binnen de gezamenlijke voorziening. Het BSN mag alleen gebruikt worden indien banken reeds over dit nummer beschikken en het BSN mag alleen gebruikt worden ten behoeve van het controleren van transacties. Dat betekent dat banken alleen het BSN mogen gebruiken als identificatienummer om de persoon achter de transactie te identificeren en transacties afkomstig uit verschillende systemen te koppelen aan de juiste persoon. Zij mogen het BSN niet gebruiken voor andere doeleinden.

In het zesde lid zijn aanvullende verplichtingen opgenomen ten aanzien van de verwerking van persoonsgegevens binnen de gezamenlijke voorziening. De deelnemende instellingen zijn als verwerkingsverantwoordelijken ieder zelfstandig verantwoordelijk voor de naleving van deze voorwaarden door de voorziening, zij gelden immers als verwerkingsverantwoordelijken in de zin van artikel 4, onderdeel 7, van de AVG. Onder a is gegeven dat de persoonsgegevens gepseudonimiseerd en versleuteld moeten zijn. Dit leidt er toe dat binnen de gezamenlijke voorziening de identiteit van de persoon of onderneming, waarvan de transactie binnen de voorziening gecombineerd wordt, niet vastgesteld kan worden. Alleen de individuele bank wiens cliëntgegevens het betreft kan, na het ontvangen van een alert van de voorziening over deze cliënt, zien door of met wie de transactie is uitgevoerd. Onderdeel b schrijft voor dat er geen sprake mag zijn van geautomatiseerde besluitvorming als bedoeld in artikel 22, eerste lid van de AVG. Dit betekent dat cliënten van deelnemende banken niet mogen worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder profilering, gebaseerd besluit waaraan voor hen rechtsgevolgen zijn verbonden of die hen anderszins in aanmerkelijke mate treffen naar aanleiding van de transactiemonitoring in de gezamenlijke voorziening. Onderdeel c schrijft voor dat voor de analyse geen algoritmes gehanteerd mogen waarvan de uitkomsten niet navolgbaar en controleerbaar zijn. Onderdeel d schrijft voor dat de systemen die de verwerking uitvoeren voorzien moeten zijn van een adequaat beveiligingsniveau. Het beveiligingsniveau wordt niet voorgeschreven. Het kader van de AVG en de UAVG biedt reeds regels voor de beveiliging van persoonsgegevens. Zo dienen de verwerkingsverantwoordelijke en de verwerker, op grond van artikel 32 van de AVG, passende technische en organisatorische maatregelen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. In onderdelen e en f zijn organisatorische waarborgen opgenomen zodat alleen geautoriseerde personen toegang hebben tot de gegevens en de verwerking niet verder verwerkt worden dan het doel op grond van het eerste lid van dit artikel. Onderdeel g schrijft voor dat de gegevensverwerking wordt vastgelegd (logging) dit is noodzakelijk voor controle en toezicht op de verwerking. Dit houdt in dat bijgehouden wordt wie wanneer welke gegevens heeft ingezien. In onderdeel h is opgenomen dat de onderlinge verstrekking van de gegevens, bedoeld in het eerste lid, dient te worden beëindigd als die verstrekking niet langer noodzakelijk dan om te voldoen aan het bepaalde in artikel 34. De gegevens dienen op dat moment vanzelfsprekend te worden verwijderd. Op grond van onderdeel i dienen de instellingen zorg te dragen voor de schriftelijke vastlegging van de hierboven gegeven waarborgen.

In het zevende lid zijn verplichtingen opgenomen omtrent de verantwoording van de activiteiten van de voorziening en de bepaalde organisatorische verplichtingen waarvoor de instellingen verantwoordelijk zijn. In onderdelen a en b is opgenomen dat de instellingen betrokken bij de gezamenlijke voorziening zorgdragen voor een jaarlijks verslag omtrent de effectiviteit van de voorziening en een periodieke onafhankelijke audit omtrent de naleving van de regels met betrekking tot gegevensbescherming. Het jaarlijkse verslag dient duidelijk te maken hoe effectief de gezamenlijke voorziening is in het kader van de uitvoering van de Wwft. Hierbij dient in ieder geval inzichtelijk te worden gemaakt welke gevolgen het gezamenlijk monitoren van transacties heeft op de «alerts» en ongebruikelijke transacties, ten opzichte van de individuele monitoring voorafgaand aan de inwerkingtreding van dit wetsvoorstel. Voorts dient het verslag in te gaan in hoeverre de informatie afkomstig van de voorziening heeft geleid tot herbeoordeling van cliënten en het beëindigen van zakelijke relaties. De onafhankelijke audit onderzoekt in hoeverre de gezamenlijke voorziening voldoet aan de regels voor uitbesteding, gesteld in artikel 10, en de regels omtrent gegevensbescherming, neergelegd in artikel 34a, en de AVG en UAVG. Omdat deze vorm van uitbesteding en gegevensdeling bijzonder gevoelig is, dient de eerste audit plaats te vinden een jaar na ingebruikname van de voorziening. Daarna dient deze ieder jaar plaats te vinden. Het jaarverslag en de resultaten van de onafhankelijke audit dienen openbaar te worden gepubliceerd. In onderdelen c en d worden enkele specifieke organisatorische verplichtingen voorgeschreven waarvoor de instellingen zorg moeten dragen binnen de voorziening. Onderdeel c stelt dat er tenminste één functionaris dient te worden aangewezen die verantwoordelijk is voor de gegevensbescherming binnen de voorziening. Daarnaast dienen de instellingen zorg te dragen voor een orgaan dat de verantwoordelijkheid en aansprakelijkheid vaststelt van de instellingen. De afzonderlijke instellingen zijn verwerkingsverantwoordelijken voor de verwerking binnen de voorziening. Door de gegevens binnen de voorziening te combineren, echter, kan deze verantwoordelijkheid onduidelijk worden. De voorziening verwerkt immers gegevens van de verschillende verwerkingsverantwoordelijke instellingen. Dit kan het voor de betrokkene mogelijk complex maken om zijn rechten uit te oefenen ten aanzien van de verwerkingsverantwoordelijken. Om dit te waarborgen zijn de instelling daarom verplicht een orgaan in te stellen dat bij klachten vaststelt welke instellingen als verwerkingsverantwoordelijke gelden.

ARTIKEL II *(wijziging Wet op de economische delicten)*

In de Wet op de economische delicten is een aantal bepalingen van de Wwft strafbaar gesteld. Met dit artikel worden hier twee toevoegingen aan gedaan. Het gaat om strafbaarstelling van het verbod voor beroeps- en bedrijfsmatige handelaren als kopers en verkopers van goederen om contante betalingen vanaf € 3.000 te verrichten uit het voorgestelde artikel 1f en om strafbaarstelling van niet naleving van de verplichting om onderzoek te doen naar eerdere dienstverlening bij andere instellingen in geval er sprake is van een hoger risico op witwassen of financieren van terrorisme uit het voorgestelde artikel 3b. Bij de strafbaarstelling is zoveel mogelijk aangesloten bij de strafbaarstelling van soortgelijke voorschriften uit, met name, de Wet toezicht trustkantoren 2018.

ARTIKEL III *(overgangsrecht informatie-uitwisseling o.g.v. artikel I, onderdeel D)*

Het voorgestelde artikel 3b, derde lid, bepaalt dat de instelling die een verzoek van een andere instelling ontvangt om informatie over gebleken risico's op witwassen of financieren van terrorisme te verstrekken,

onverwijld moet voldoen aan dit verzoek. Dit artikel regelt als overgangsrecht dat een instelling geen informatie over risico's op witwassen of financieren van terrorisme hoeft te verstrekken als deze informatie is gebleken voor inwerkingtreding van artikel I, onderdeel D, van deze wet.

ARTIKEL IV *(evaluatiebepaling artikel I, onderdelen A en B)*

Het eerste lid van dit artikel bevat de evaluatiebepaling voor het verbod voor handelaren om contante transacties te verrichten vanaf € 3.000, opgenomen in artikel I, onderdelen A en B. Deze evaluatie wordt vijf jaar na inwerkingtreding uitgevoerd. Bij deze evaluatie wordt de effectiviteit van de maatregel en de gevolgen in de praktijk bezien.

Het tweede lid van dit artikel bevat de evaluatiebepaling voor gezamenlijke transactiemonitoring, opgenomen in artikel I, onderdeel L. Deze evaluatie wordt vier jaar na inwerkingtreding uitgevoerd. Uit het derde lid volgt dat bij de evaluatie in ieder geval de effectiviteit van het gezamenlijk monitoren van transacties en de bescherming van persoonsgegevens binnen de gezamenlijke voorziening betrokken dienen te worden. Ten slotte wordt in het vierde lid de toegang tot de benodigde gegevens om deze evaluatie uit te kunnen voeren verzekerd. Ook wordt verzekerd dat de verkregen gegevens niet voor andere doeleinden dan het uitvoeren van de evaluatie worden gebruikt.

ARTIKEL V *(inwerkingtredingsbepaling)*

Dit artikel regelt de inwerkingtreding. Het wetsvoorstel treedt in werking op een bij koninklijk besluit te bepalen tijdstip. Dit tijdstip kan verschillen voor de verschillende onderdelen van het wetsvoorstel, aangezien het wijziging van meerdere wetten betreft. Bij aanvaarding zal een geschikt inwerkingtredingsmoment moeten worden bepaald.

De Minister van Financiën,
S.A.M. Kaag