

Wijziging van de Wet ter voorkoming van witwassen en financieren van terrorisme en de Wet toezicht trustkantoren 2018 in verband met het verbod op contante betalingen voor goederen vanaf 3.000 euro, het uitbreiden van de mogelijkheden voor informatie-uitwisseling ten behoeve van de poortwachtersfunctie en de aanscherping van de regels voor trustkantoren (Wet plan van aanpak witwassen)

MEMORIE VAN TOELICHTING

ALGEMEEN

§1. Inleiding

Het voorkomen en bestrijden van witwassen en terrorismefinanciering 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 terrorismefinanciering. 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), de Wet toezicht trustkantoren 2018 (Wtt 2018) en de Wet op economische delicten.

Dit wetsvoorstel is onder te verdelen in vijf 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 terrorismefinanciering;
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 terrorismefinanciering;
5. Aanvullende maatregelen om de integriteitsrisico's bij trustdienstverlening te beheersen.

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

¹ Kamerstukken II 2018/19, 31477, nr. 41.

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 verhuilen. 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 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 terrorismefinanciering verbonden zijn. Bovendien heeft het merendeel van de Europese lidstaten maatregelen getroffen om risico's bij lagere contante betalingen aan te pakken. In 2020 zijn er in totaal zestien 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

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.

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.

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 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 alleen 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.

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 gezien, alsmede de uitvoering en de handhaving van het verbod.

§2.2. Vergroten samenwerking en informatie-uitwisseling instellingen

Instellingen⁸ vervullen een poortwachtersfunctie ten behoeve van de bescherming van de integriteit van het financiële stelsel. Deze poortwachtersfunctie wordt internationaal en Europees

⁷ Leidraad Wet ter voorkoming van witwassen en financieren van terrorisme: richtlijnen voor kopers en verkopers van goederen, december 2018.

⁸ Met 'instellingen' wordt in dit wetsvoorstel bedoeld 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.

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 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 terrorismefinanciering 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 terrorismefinanciering, 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 terrorismefinanciering 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 uit het cliëntendossier 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 terrorismefinanciering. 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 terrorismefinanciering met zich meebrengt, te onderzoeken of de cliënt eerder om dienstverlening heeft verzocht, eerder dienstverlening heeft afgenomen of op dit moment afneemt bij een andere instelling van dezelfde categorie. Wanneer er indicaties zijn voor een hoger risico op witwassen of terrorismefinanciering, dient de instelling navraag te doen bij de vroegere dienstverlener naar gebleken risico's op witwassen of terrorismefinanciering. Indien de vroegere 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. Instelling dienen, 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 lagere regelgeving uitwisseling tussen verschillende categorieën van instellingen mogelijk kunnen te maken.

§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.

Een ander middel om na te gaan of een andere instelling gegevens zou kunnen hebben die relevant zijn voor het cliëntenonderzoek is het raadplegen van een zwarte lijst met personen bij wie risico's op witwassen of terrorismefinanciering zijn vastgesteld. Deze moet dan wel vastgesteld zijn door de categorie instellingen of hun brancheverenigingen. Indien een dergelijke zwarte lijst persoonsgegevens van strafrechtelijke aard bevat, dient hiervoor een vergunning aangevraagd te worden bij de Autoriteit Persoonsgegevens.⁹ Eenmaal vastgesteld, kan een dergelijke lijst 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 gegevens met een langere tijdsperiode dan vijf jaar. 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 toelichting onder *Hoger risico witwassen of terrorismefinanciering*) en dat bij navraag enkel de gegevens mogen worden verstrekt waar de instelling na inwerkingtreding van dit wetsvoorstel de beschikking over heeft verkregen.

⁹ Artikel 33, vierde lid, onder c, van de UAVG.

§2.2.1.3 Indicaties van een hoger risico witwassen of terrorismefinanciering

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 terrorismefinanciering met zich meebrengt. Hier zal in ieder geval sprake van zijn als er een hoger risico op witwassen of terrorismefinanciering is vastgesteld, waarna een verscherpt cliëntenonderzoek dient te worden verricht. Maar hier kan ook sprake van zijn als het risico nog niet is vastgesteld, maar er wel indicaties zijn van een hoger risico. Indien uit de navraag bij een andere instelling relevante informatie wordt aangeleverd over risico's die zijn geconstateerd in het verleden, kan dit een aanleiding vormen voor de vaststelling van een hoger risico, waarna alsnog een verscherpt cliëntenonderzoek plaats dient te vinden. Deze risico gebaseerde benadering van de maatregel past binnen de systematiek van de Wwft. 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 de risico's op witwassen of terrorismefinanciering. Deze gegevensdeling zal in de regel leiden tot lastenverlichting voor de vragende instelling, aangezien de instelling gebruik kan maken van de informatie die de eerdere dienstverlener 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. Het cliëntenonderzoek dient immers, met inachtneming van het risicoprofiel van de cliënt, voortdurend te worden uitgevoerd door instellingen. 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 terrorismefinanciering zijn, moet deze instelling onderzoek doen naar eerdere dienstverlening door andere instellingen uit dezelfde categorie en kunnen er gegevens gedeeld worden indien er sprake is van gebleken risico's op witwassen of terrorismefinanciering. De instelling 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

De instelling bij wie navraag wordt gedaan over een bepaalde cliënt, deelt uitsluitend informatie uit het cliëntendossier in het geval dat deze risico's op witwassen of terrorismefinanciering heeft geconstateerd ten aanzien van de cliënt. Hierbij worden uitsluitend de gegevens gedeeld die destijds relevant waren voor deze constatering. Het desgevraagd delen van deze gegevens is een verplichting voor de eerdere dienstverlener. Deze verplichting ontslaat de eerdere dienstverlener echter niet van het tipping-off verbod neergelegd in artikel 23 van de Wwft. Dit betekent dat die dienstverlener 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 betrokken kunnen worden bij het cliëntenonderzoek. Als deze gegevens te lang op zich laten wachten, wordt deze doelstelling ondergraven.

De instelling die de gegevens ontvangt, kan deze gebruiken ten behoeve van haar eigen afweging ten aanzien van de risico's op witwassen of terrorismefinanciering 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 zijn eigen risicobeoordeling vast te stellen of zijn eigen dienstverlening zodanig is ingericht dat de risico's afdoende te mitigeren zijn. Dat kan bijvoorbeeld betekenen dat de bevroegde 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.

§2.2.2. Gezamenlijke transactiemonitoring door banken

Op grond van de Wwft hebben instellingen de plicht om de transacties van hun cliënten te monitoren en ongebruikelijke transacties te melden bij de FIU-Nederland. 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 diverse (bijzondere) opsporingsinstanties en inlichtingen- en veiligheidsdiensten. Adequate en volledige melding van ongebruikelijke transacties is derhalve van belang voor onderzoeken door voornoemde autoriteiten.

Om vast te stellen of er sprake is van een ongebruikelijke transactie monitoren banken 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 indicatoren zijn die duiden op het vermoeden van witwassen of terrorismefinanciering. Banken baseren zich daarvoor op dit moment alleen op hun eigen en openbare informatie. Door transacties te combineren, hebben banken meer informatie tot hun beschikking. Hierdoor kunnen ongebruikelijke transacties vaker en eerder worden ontdekt. Ook kunnen transacties die op basis van de eigen informatie onterecht als ongebruikelijk gekwalificeerd zouden worden, in het licht van de informatie van andere banken niet als zodanig gekwalificeerd hoeven te worden. Zodoende kan de kwaliteit van de meldingen verhoogd worden en kan voorkomen worden dat criminelen de monitoring omzeilen door transacties te verspreiden of via een groot aantal banken te laten lopen. Daarnaast biedt het de mogelijkheid om uniforme alerts in te stellen, die snel en voor veel transacties aangepast kunnen worden als er nieuwe indicatoren voor witwassen of financieren van terrorisme zijn ontwikkeld.

Een vijftal banken heeft aangegeven gezamenlijk transacties te willen monitoren in een gezamenlijke voorziening, ook wel het initiatief Transactie Monitoring Nederland (TMNL) genoemd.¹⁰ De verantwoordelijkheid voor de inrichting van deze voorziening ligt bij de banken zelf, maar de wet staat op twee punten deze organisatie van transactiemonitoring en het doen meldingen in de weg, namelijk op het punt van uitbesteding en ten aanzien van het delen van transacties. Met dit wetsvoorstel worden deze belemmeringen specifiek voor banken weggenomen. 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. Daarbij speelt de hierboven genoemde problematiek in het bijzonder bij banken. Criminelen gebruiken verschillende rekeningen en verschillende banken om al dan niet via een opeenvolging van transacties de herkomst van het illegaal verkregen vermogen te verhullen. Daarbij is van belang dat bij banken in de regel sprake is van zakelijke relaties die doorlopende monitoring vereisen en beperkt sprake is 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

¹⁰ Persbericht NVB, *Nederlandse banken bundelen krachten tegen witwassen*, 13 september 2019.

van witwassen en terrorismefinanciering als geheel de meeste meerwaarde zal hebben.

§2.2.2.1 Weg te nemen wettelijke belemmeringen

Ten eerste wordt met dit wetsvoorstel voor banken mogelijk gemaakt om het monitoren van transacties uit te besteden. Het huidige verbod hierop uit de Wwft volgt niet uit de (gewijzigde) vierde anti-witwasrichtlijn. De richtlijn laat ruimte voor uitbesteding bij transactiemonitoring en het melden van transacties 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.¹¹ 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 wettelijke verplichtingen. Een bank kan zodoende te allen tijde aangesproken worden als de derde aan wie de uitvoering is uitbesteed niet voldoet aan de verplichtingen van de wet.

Ten tweede wordt expliciet geregeld dat binnen de gezamenlijke voorziening gegevens betreffende transacties kunnen worden gedeeld. De Wwft kent een algemene plicht voor instellingen om transacties voortdurend te monitoren. Bij het gezamenlijk monitoren van transacties worden gegevens van verschillende banken bij elkaar gebracht en gecombineerd. Omdat hierbij persoonsgegevens worden verwerkt en het delen van transactiegegevens een nieuwe verwerking van persoonsgegevens is, is hiervoor een verwerkingsgrondslag nodig. De gedeelde 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 toegelicht in paragraaf 2.3. Hiermee mogen ook bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard worden gedeeld voor het uitvoeren van (gezamenlijke) transactiemonitoring. In paragraaf 3 en in het artikelsgewijze deel van deze toelichting wordt verder ingegaan op de gevolgen hiervan voor de bescherming van persoonsgegevens. Van belang is om te vermelden dat voor het delen van transactiegegevens tussen banken strikte voorwaarden gelden. Allereerst geldt een specifieke doelbinding voor gedeelde transacties. Deze mogen enkel en alleen worden gebruikt voor het monitoren van transacties op witwassen en financieren van terrorisme en het melden van ongebruikelijke transacties. Dit betekent dat deze informatie niet gebruikt mag worden voor andere doeleinden. De banken zijn op grond van de AVG gehouden om hier waarborgen voor in te bouwen. Daarnaast moet het tipping-off verbod zijn gewaarborgd. Dit houdt in dat binnen de gezamenlijke voorziening alleen transactiegegevens mogen worden gedeeld en niet (ook) het gegeven dat van bepaalde transacties melding is gedaan bij de FIU-Nederland. In dit kader is de uitzondering op het tipping-off verbod uit artikel 23, zesde lid, onder 3° van de Wwft relevant. 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. Tot slot wordt gewezen op het feit dat banken voor de verwerking van persoonsgegevens in het kader van het gezamenlijk uitvoeren van transactiemonitoring een gegevensbeschermingseffectbeoordeling (GEB)¹² moeten opstellen, waarin zij onder meer de noodzaak van het gezamenlijk uitvoeren van transactiemonitoring voor de betreffende bank beoordelen.

§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 retailklanten, die over één of meer (al dan

¹¹ Zie artikel 29 van de vierde anti-witwasrichtlijn.

¹² Artikel 35 AVG.

niet aan elkaar gekoppelde) rekeningen beschikken. Per jaar vinden er thans 9,8 miljard transacties vanaf die rekeningen plaats. 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 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. Allereerst 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 terrorismefinanciering (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.

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 waarmee die gegevens in bepaalde gevallen onlosmakelijk verbonden zijn. Hieronder 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

Om witwassen en terrorismefinanciering 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 terrorismefinanciering 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 terrorismefinanciering 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 terrorismefinanciering.

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 persoonsgegevens 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.¹³ 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.¹⁴ 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 leven. Hoewel dergelijke informatie op zichzelf geen aanleiding geeft tot nader onderzoek, kan uit een dergelijke transactie, indien in samenhang gezien met andere risicofactoren, een ongebruikelijk patroon naar voren komen dat een indicatie kan zijn voor witwassen. Ook kunnen religieuze aspecten een rol spelen bij de beoordeling van transacties in het kader van terrorismefinanciering, wanneer bijvoorbeeld donaties worden gedaan aan religieuze instellingen in het buitenland. 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. 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 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 terrorismefinanciering en dat transacties zo vorm gegeven kunnen worden, bijvoorbeeld door het gebruik van bijzondere categorieën van persoonsgegevens, dat de herkomst van middelen wordt verhuuld. 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 terrorismefinanciering 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 op te nemen in het cliëntendossier. Hiermee verwerkt een instelling een gegeven van strafrechtelijke aard. Ook dienen instellingen onderzoek te doen naar cliënten door middel van openbare bronnen. Uit deze

¹³ Financial Intelligence Unit-Nederland, Jaaroverzicht 2018.

¹⁴ Financial Intelligence Unit-Nederland, Jaaroverzicht 2019.

openbare bronnen kunnen veroordelingen naar voren komen. Waar deze informatie relevant is voor het onderzoek naar de risico's op witwassen en terrorismefinanciering 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.

§2.4 Aanvullende maatregelen trustdienstverlening

Met dit wetsvoorstel wordt tevens Wtt 2018 op enkele punten gewijzigd, ten einde de integriteit van het financiële stelsel in Nederland te bevorderen. De voorgestelde wijzigingen zijn onderdeel van het plan van aanpak witwassen.¹⁵ Ook passen deze maatregelen in het kader van de maatregelen die recent getroffen zijn door het kabinet in het kader van het tegengaan van belastingontwijking en belastingontduiking in Nederland.¹⁶

Met ingang van 1 januari 2019 zijn de regels voor trustdienstverlening aanzienlijk aangescherpt met de Wtt 2018. Die aanscherpingen volgden op verschillende onderzoeken van DNB waaruit bleek dat de sector de integriteitsrisico's onvoldoende beheerste. Daarbij is de samenleving in 2015 geconfronteerd met de kwetsbaarheden van de trustsector door de onthulling van de Panama Papers. Uit deze gelekte stukken bleek dat verschillende Nederlandse trustkantoren betrokken waren bij het bedienen van malafide structuren. De onthullingen rond de Panama Papers en het onderzoek van de parlementaire ondervragingscommissie Fiscale constructies dat daarop volgde, hebben een belangrijke rol gespeeld in de verdere regulering van de trustsector.

Dienstverlening door trustkantoren gaat vaak gepaard met hoge integriteitsrisico's. Er worden diensten verleend aan internationale structuren en de dienstverlening is in veel gevallen fiscaal gedreven. Hierbij worden vaak complexe en ondoorzichtige structuren bediend, hetgeen een hoger risico op betrokkenheid bij financieel economische criminaliteit met zich meebrengt.

Bij de behandeling van de Wtt 2018 is aan het parlement toegezegd de sector nauwgezet te monitoren en steeds na te gaan of de getroffen maatregelen afdoende zijn. In de agenda financiële sector¹⁷, waarin de integriteit van de financiële sector één van de centrale domeinen is, is

¹⁵ Kamerstukken II 2019/20, 31477, nr. 51.

¹⁶ Kamerstukken II 2017/18, 25087, nr. 188.

¹⁷ Kamerstukken II 2018/19, 32013, nr. 200.

aangegeven dat DNB, de toezichthouder op trustkantoren, gevraagd zou worden om in de jaarlijkse ZBO-verantwoording uitgebreid te informeren over de ontwikkelingen in de trustsector en het toezicht op de naleving van de nieuwe wetgeving. Ook is destijds aangegeven dat indien er geen sprake is van voldoende verbetering, nadere maatregelen onderzocht zouden worden.

De afgelopen jaren is meerdere malen gebleken dat de aanpak van witwassen in Nederland te kort schiet. Om de aanpak te verbeteren en te intensiveren is het plan van aanpak witwassen opgesteld. In het kader van het plan van aanpak witwassen is DNB gevraagd eerder te rapporteren over de trustsector, dan bij de jaarlijkse ZBO-verantwoording. DNB heeft eind 2019 het "Toezichtbeeld trustkantoren 2019"¹⁸ uitgebracht, waarin een eerste analyse is gedaan van de naleving van de striktere eisen die per 1 januari 2019 zijn ingevoerd voor de trustsector. De conclusie van het rapport is dat gedurende 2019, DNB heeft vastgesteld dat de sector nog niet klaar is met het incorporeren van de nieuwe aangescherpte eisen. Belangrijke gemene deler bij de uitkomst van onderzoeken is dat er nog regelmatig tekortkomingen worden aangetroffen in de uitvoering van het verplichte cliëntenonderzoek en de vastlegging ervan. De vereiste 'due diligence' is niet altijd aanwezig waardoor in sommige gevallen integriteitsrisico's niet in beeld zijn of lager worden ingeschat dan ze zijn. Soms wordt of de effectiviteit van mitigerende maatregelen ook te laag ingeschat.

Gezien de incidenten in het verleden en het toezichtbeeld van DNB, is besloten om de sector verder te reguleren. Besloten is om dienstverlening waaraan bijzondere hoge integriteitsrisico's verbonden zijn, te verbieden. Dit betreft het aanbieden van doorstroomvennootschappen en trustdienstverlening met betrokkenheid¹⁹ van derde-hoogrisicolanden of van landen die op de lijst staan van non-coöperatieve landen op belastinggebied.

§2.4.1 Doorstroomvennootschappen

Onder de huidige Wtt 2018 is het ten behoeve van een cliënt gebruik maken van een doorstroomvennootschap gekwalificeerd als een trustdienst.²⁰ Het gaat hierbij om rechtspersonen of vennootschappen die behoren tot de groep van het trustkantoor, die gebruikt worden om gelden "doorheen te laten stromen" voor fiscale doeleinden. Hierbij kan bijvoorbeeld worden gedacht aan dividenden of royalty's. Het ter beschikking stellen van een doorstroomvennootschap dient vooral fiscale doelen en leidt tot intransparantie.

Dit kabinet heeft al verschillende maatregelen genomen om belastingontwijking en -ontduiking in Nederland aan te pakken. Een van deze maatregelen is de invoering van een bronbelasting op renten en royalty's naar laagbelastende jurisdicties en in misbruiksituaties die op 1 januari 2021 in werking treedt. Deze maatregel dient ertoe het risico van belastingontwijking door het verschuiven van (Nederlandse) belastinggrondslag naar laagbelastende jurisdicties te verkleinen. In de strijd tegen belastingontduiking en ontwijking is het echter onwenselijk dat er nog beroeps- of bedrijfsmatig doorstroomvennootschappen worden aangeboden in Nederland. Daarom is er voor gekozen de trustdienst "*om ten behoeve van een cliënt gebruik te maken van een doorstroomvennootschap*" te schrappen en tegelijkertijd een algeheel verbod op te nemen in de wet voor het beroeps- of bedrijfsmatig gebruik te maken van doorstroomvennootschappen. Met deze maatregel wordt tevens uitvoering gegeven aan de motie Omtzigt en Van Weyenberg.²¹

In artikel 5 van de Wtt 2018 is de mogelijkheid opgenomen om bij ministeriële regeling een vrijstelling te regelen van het verbod. Bepaalde vormen van dienstverlening, zoals een stichtingen administratiekantoor, zouden voor een vrijstelling in aanmerking kunnen komen omdat de dienstverlening los staat van het verbod en de risico's die daarbij horen.

¹⁸ Zie bijlage 3 bij kamerstukken II 2019/20, 31477, nr. 50.

¹⁹ Met "betrokkenheid" wordt bedoeld cliënten, doelvennootschappen, uiteindelijk belanghebbenden van cliënten en uiteindelijk belanghebbenden van doelvennootschappen uit de betreffende landen.

²⁰ Zie onderdeel c van "trustdienst" in artikel 1, eerste lid, van de Wtt 2018.

²¹ Kamerstukken II 2018/19, 34566, nr. 11.

§2.4.2 Dienstverlening waarbij landen betrokken zijn die op de lijst van derde-hoog risicolanden staan

Op basis van de huidige Wtt 2018²² dienen trustkantoren verscherpt cliëntenonderzoek te verrichten indien de staat waar de cliënt, de doelvennootschap of de uiteindelijk belanghebbende van de cliënt of doelvennootschap woonachtig of gevestigd is of zijn zetel heeft, in een door de Europese Commissie aangewezen staat met een hoger risico op witwassen of financieren van terrorisme. Op grond van artikel 9 van de vierde anti-witwasrichtlijn is de Europese Commissie bevoegd hoog risico derde landen aan te wijzen middels gedelegeerde handelingen. Het gaat hierbij om landen die in hun nationale wetgeving ter voorkoming van witwassen en financieren van terrorisme strategische tekortkomingen vertonen, waardoor die landen een aanzienlijke bedreiging vormen voor het financieel stelsel van de Europese Unie.

Bij trustdienstverlening zijn vaak complexe structuren betrokken en worden tussen vennootschappen grote sommen geld verplaatst. Indien hier landen bij betrokken zijn met strategische tekortkomingen op het gebied van hun anti-witwasbeleid, stapelen de integriteitsrisico's zich op. De combinatie van trustdienstverlening met deze hoog risicolanden, zorgt voor onverantwoord hoge integriteitsrisico's. Daarom wordt met dit wetsvoorstel dienstverlening door trustkantoren verboden indien de cliënt, de doelvennootschap of de uiteindelijk belanghebbende van de cliënt of doelvennootschap woonachtig of gevestigd is of zijn zetel heeft in een derde hoog risicoland.

§2.4.3 Dienstverlening waarbij landen betrokken zijn die op de lijst van non-coöperatieve landen op belastinggebied staan.

Trustdiensten zijn veelal fiscaal gedreven en vaak vindt er verplaatsing van grote vermogensbestanddelen plaats tussen vennootschappen binnen een structuur die het trustkantoor bedient. Daarom dienen trustkantoren bijzondere aandacht te hebben voor het risico dat hun diensten worden gebruikt voor belastingontduiking of belastingontwijking. In dat kader zijn structuren met betrokkenheid van landen die op de lijst van non-coöperatieve landen op belastinggebied staan²³, op basis van de huidige wet een belangrijke indicator voor verscherpt cliëntenonderzoek.

Trustdienstverlening gecombineerd met structuren waarbij betrokkenheid is van landen die op de lijst van non-coöperatieve landen op belastinggebied staan, leidt tot een cumulatie van de fiscale integriteitsrisico's. Daarom wordt middels dit wetsvoorstel in dit kader een verbod ingevoerd. Het verbod ziet op dienstverlening aan cliënten, doelvennootschappen, uiteindelijk belanghebbenden van cliënten en doelvennootschappen uit landen die op de lijst van non-coöperatieve landen op belastinggebied staan.

§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 en de aanvullende maatregelen voor de trustsector worden hier buiten beschouwing gelaten, aangezien gegevensbescherming ten aanzien van deze onderdelen niet relevant is, omdat er geen sprake is van verwerking van persoonsgegevens.

Gegevens in een cliëntendossier en transactiegegevens zijn persoonsgegevens in de zin van de AVG. Onder een persoonsgegeven wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare persoon.²⁴ Op de verwerking van persoonsgegevens is de AVG van toepassing.

²² Artikel 33, eerste lid, sub b, van de Wtt 2018.

²³ Deze lijst is te vinden op: <https://www.consilium.europa.eu/nl/policies/eu-list-of-non-cooperative-jurisdictions/timeline-eu-list-of-non-cooperative-jurisdictions/>

²⁴ 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 identifier zoals een naam, een identificatienummer, locatiegegevens, een

Omdat de voorgestelde maatregelen, op het verbod op contante betalingen vanaf € 3.000 en de aanvullende maatregelen voor de trustsector na, 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, 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 genoemde gegevens maken onderdeel uit van het dossier dat een instelling heeft van een cliënt en dienen te worden aangemerkt als persoonsgegevens, aangezien met deze gegevens een natuurlijke persoon direct of indirect kan worden geïdentificeerd. In artikel 33, tweede lid, onderdeel a en b, 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. Van de uiteindelijk belanghebbende dient ook tenminste de geslachtsnaam en voornamen te worden vastgelegd alsmede de gegevens en documenten die zijn vergaard op basis van de redelijke maatregelen die zijn genomen om de identiteit van de uiteindelijk belanghebbende te verifiëren.

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 terrorismefinanciering. In dit geval zal de instelling ten minste de geslachtsnaam en voornaam van de cliënt dienen te verstrekken. Indien twijfel bestaat over de identiteit van de cliënt, zal de

online identicator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

instelling aanvullende gegevens dienen te verstrekken, zoals de geboortedatum en adresgegevens, om vast te stellen dat het dezelfde cliënt betreft. De grondslag voor deze gegevensverstrekking is gelegen in de wettelijke verplichting om onderzoek te doen naar eerdere dienstverlening.

Indien een instelling een dergelijk verzoek ontvangt ten aanzien van een cliënt waarbij deze risico's op witwassen en terrorismefinanciering heeft vastgesteld, dient de instelling de vragende instelling hierover te informeren. In algemene zin betreft dit informatie over de reden waarom 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 terrorismefinanciering, 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 uitwisselen van gebleken risico's op witwassen of terrorismefinanciering bij de cliënt, noodzakelijk voor het te bereiken doel, namelijk het voorkomen en bestrijden van witwassen en terrorismefinanciering. 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 verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens van een cliënt. Een betrokkene kan zich daarom altijd wenden tot de instelling indien hij van mening is dat hem betreffende persoonsgegevens rechtmatig worden verwerkt door de instelling. Deze gegevensdeling vindt alleen plaats in gevallen waarin er indicaties zijn van een hoger risico op witwassen of financieren van terrorisme en in principe uitsluitend tussen de instellingen die binnen dezelfde categorie vallen.

Noodzaak

Het voorgestelde artikel regelt de bevoegdheid van instellingen om gegevens over gebleken risico's op witwassen en terrorismefinanciering 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 een hoger risico op witwassen of terrorismefinanciering met zich brengt en voor zover die uitwisseling noodzakelijk is om te kunnen voldoen aan de verplichting om cliëntenonderzoek te verrichten als bedoeld in artikel 3 van de Wwft. 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 onvolledige of onjuiste informatie te verstrekken, die geen alarmbellen doet rinkelen. 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 gebruiken 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 wordt voorkomen dat de dienstverlening van instellingen door middel van shopgedrag tussen instellingen wordt gebruikt voor witwassen of terrorismefinanciering.

Proportionaliteit

Er is voor gekozen om de uitwisseling van gegevens over gebleken risico's op witwassen of terrorismefinanciering te beperken tot die gevallen dat de zakelijke relatie of transactie naar haar

aard een hoger risico met zich brengt. Dit is een risico gebaseerde invulling van de maatregel, die aansluit op het systeem van de Wwft. Daarnaast wordt voorgesteld dat de uitwisseling van die gegevens alleen mogelijk is tussen instellingen die behoren tot dezelfde categorie. Omdat er bij instellingen uit dezelfde categorie sprake is van soortgelijke dienstverlening, hebben de risico's op witwassen en terrorismefinanciering die bij de ene instelling zijn gebleken ook daadwerkelijk materiële betekenis voor de andere instelling. Dit leidt ertoe dat die andere instelling een beter gefundeerde risico inschatting kan maken van de risico's op witwassen en financieren van terrorisme en een accurater risicoprofiel van de cliënt kan opstellen. Hieruit blijkt ook de meerwaarde van deze maatregel ten opzichte van een stelsel van zwarte lijsten. Een zwarte lijst bevat de namen van cliënten die geweigerd zijn of ten aanzien van wie de dienstverlening is stopgezet, en leent zich minder voor het opnemen van een uitgebreide, inhoudelijke motivering van de redenen waarom een cliënt op die lijst is geplaatst. Dit is onwenselijk omdat juist deze motivering 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.

Rechten van betrokkenen

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 terrorismefinanciering. 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.²⁵ Daarnaast hebben betrokkenen ook nog 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 daartegen een klacht indienen bij de AP.²⁶ Daarnaast kan een betrokkene in dat geval ook beroep instellen bij de rechter.²⁷

Subsidiariteit

Bij deze maatregel is steeds gekozen voor het minst vergaande alternatief. Allereerst door de uitwisseling van gegevens over gebleken 'risico's op witwassen en terrorismefinanciering te beperken tot die gevallen dat de zakelijke relatie of transactie naar haar aard een hoger risico op witwassen of terrorismefinanciering met zich brengt. 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 terrorismefinanciering 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 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 terrorismefinanciering 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 zelf een inschatting te maken van het risico op witwassen of terrorismefinanciering bij het

²⁵ Artikel 15 AVG.

²⁶ Artikel 77 AVG.

²⁷ Artikel 79 AVG.

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 (derisking) door instellingen. Ten aanzien van de gegevensuitwisseling tussen instellingen ten behoeve van het cliëntenonderzoek is het belangrijk om te benadrukken dat de individuele risicoafweging die de instelling per cliënt maakt nog steeds leidend is. De gegevens die een eerdere dienstverlener aanreikt dienen als een niet-bindende aanvulling en ontslaan de verzoekende instelling dus niet van de verplichting tot het maken van een eigen individuele risicoafweging. De maatregel zou mogelijk kunnen leiden tot een verhoging van het gebruik van zwarte lijsten met personen bij wie een hoger risico op witwassen of terrorismefinanciering is vastgesteld. In dit verband is het belangrijk te benadrukken dat het gebruik van dergelijke lijsten met waarborgen is omkleed om onterechte opname op een lijst te voorkomen. Zo moeten instellingen alvorens zij overgaan tot het aanleggen van een zwarte lijst een gerechtvaardigd belang hebben, moet de noodzaak om persoonsgegevens te verwerken duidelijk zijn en moet er sprake zijn van een zwaarwegend belang. Ook kent het gebruik van zwarte lijsten rechten toe aan de personen die hierop staan. Zoals het recht op rectificatie en het recht op vergetelheid.

§3.2 Gegevensbeschermingseffectbeoordeling gezamenlijke transactiemonitoring

A. Verwerking van persoonsgegevens

Het wetsvoorstel maakt mogelijk dat banken transactiegegevens met elkaar kunnen delen ten behoeve van het gezamenlijk uitvoeren van transactiemonitoring, al dan niet door een derde partij. Hoewel het wetsvoorstel niet voorschrijft welke persoonsgegevens precies kunnen worden gedeeld, zullen dit geen andere gegevens zijn dan die welke banken nu al gebruiken voor de door hen individueel uitgevoerde transactiemonitoring op grond van artikel 3, tweede lid, onderdeel d, van de Wwft. Daarbij kan gedacht worden aan basale cliëntgegevens, zoals NAW-gegevens, en transactiegegevens van de cliënt. Deze gegevens kunnen ook bijzondere categorieën van persoonsgegevens bevatten alsmede persoonsgegevens van strafrechtelijke aard. Ook schrijft het wetsvoorstel niet de wijze voor waarop banken transacties gezamenlijk kunnen monitoren. Het is aan de banken om, als zij van deze mogelijkheid gebruik willen maken, hieraan invulling te geven in overeenstemming met de geldende wet- en regelgeving op het gebied van gegevensbescherming. Ten aanzien van deze invulling zijn banken op grond van artikel 35 van de AVG verplicht een GEB uit te voeren.

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 kan de voorgestelde maatregel, te weten het delen van transactiegegevens door banken ten behoeve van het uitvoeren van gezamenlijke transactiemonitoring, noodzakelijk zijn voor het te bereiken doel, namelijk het voorkomen van witwassen en terrorismefinanciering. Of de noodzaak voor gezamenlijke transactiemonitoring bestaat is aan het oordeel van de banken gelaten, aangezien zij hun cliëntenbestand het beste kennen. De reikwijdte van de maatregel is beperkt tot banken. Door het gebruik van het BSN bij het koppelen van een bepaalde persoon aan gegevens van die persoon bij diverse banken, vindt dataminimalisatie plaats. De rechten van betrokkenen zijn geborgd. De banken zijn verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens van hun cliënten ten behoeve van (gezamenlijke) transactiemonitoring. Betrokkenen kunnen zich daarom altijd wenden tot hun bank indien zij van mening zijn dat hen betreffende persoonsgegevens door hun bank niet rechtmatig worden verwerkt. Dit geldt ook in geval van gezamenlijke transactiemonitoring door een derde partij. Minder vergaande alternatieven zijn overwogen, maar blijken onvoldoende geschikt voor het doel en kostbaar.

Noodzaak

Het voorgestelde artikel 34b regelt de bevoegdheid van banken om gegevens te kunnen delen met andere banken, voor zover dat noodzakelijk is om te kunnen voldoen aan de verplichting tot een voortdurende controle van transacties, bedoeld in artikel 3, tweede lid, onderdeel d, Wwft en het

melden van ongebruikelijke transacties, bedoeld in artikel 16 Wwft. Het doel van deze verplichtingen is het voorkomen van witwassen en financieren van terrorisme. De grondslag voor het verwerken van persoonsgegevens voor dit doel is derhalve het voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust (namelijk artikel 3 van de Wwft) als bedoeld in artikel 6, eerste lid, onderdeel c, AVG. De voorgestelde maatregel is noodzakelijk voor dit doel, omdat banken nu bij de beoordeling van transacties slechts een deel zien van wat de cliënt doet, namelijk dat deel van de transactie dat door de betreffende bank zelf wordt uitgevoerd. Criminelen spelen hierop in door transacties zodanig over instellingen te verspreiden dat daardoor de ongebruikelijkheid van die afzonderlijke transacties niet altijd opvalt. Zo kan een persoon bij verschillende banken een rekening aanhouden die hij voor verschillende activiteiten gebruikt. Individueel is bij die rekeningen niets ongebruikelijks te zien, maar de combinatie van het gebruik van die rekeningen kan wel degelijk als ongebruikelijk worden gekwalificeerd. Om een vollediger beeld te krijgen van door hun cliënten verrichte transacties kan het noodzakelijk zijn dat banken een gezamenlijke voorziening opzetten, waarin banken de transactiegegevens van hun cliënten delen. Alleen zo kunnen die ongebruikelijke transacties en transactiepatronen in beeld komen, waarbij gebruik wordt gemaakt van meerdere banken. Omdat banken zelf het beste in staat zijn om op basis van hun klantenbestand en de door hun klanten 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.

Bij een recent door een aantal banken uitgevoerde proef is gebleken dat met gezamenlijke monitoring van transacties ongebruikelijke transacties in kaart gebracht kunnen worden die bij monitoring per individuele bank niet zichtbaar zijn, dat patronen van financiële criminaliteit scherper (minder ruis/false positives) in beeld gebracht kunnen worden en zijn voorbeelden gevonden van nieuwe inzichten die eerder niet mogelijk waren en die bruikbaar zijn in het tegengaan van witwassen. Daarbij kan gedacht worden aan het voorbeeld 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 cash instroom 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 reguliere monitoring heeft de ene bank door haar beperkte blik deze casus niet als ongebruikelijk geïdentificeerd. Met een bredere blik zou dit zeer waarschijnlijk wel het geval zijn geweest. 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 beoordelen. Een ander voorbeeld betreft een dienstverlener in de landbouwsector, met rekeningen bij drie banken, waarbij door een opeenvolging van gebeurtenissen bij meerdere banken sprake is van een risico op witwassen. Daarnaast zijn er relevante nieuwe inzichten verkregen met betrekking tot risicovolle landen, die alleen interbancair in beeld gebracht kunnen worden en die kunnen helpen bij het voorkomen van witwassen.

Proportionaliteit

Er is voor gekozen om de voorgestelde maatregel te beperken tot transacties van Nederlandse banken en op in Nederland gevestigde bijkantoren van buiten Nederland gevestigde banken. Hoewel bekend is dat witwassen en terrorismefinanciering een internationaal fenomeen is, neemt dat niet weg dat nationale maatregelen effect kunnen sorteren, zoals blijkt uit de hiervoor genoemde proef. Om de effectiviteit te meten is voorzien in de verplichting voor banken om jaarlijks een verslag te maken over onder meer het aantal meldingen van ongebruikelijke transacties die het gezamenlijk monitoren van transacties heeft opgeleverd.

In de huidige situatie vindt transactiemonitoring ten aanzien van een individuele cliënt plaats door

elke individuele bank waar een cliënt een rekening aanhoudt en op meerdere locaties. De voorgestelde maatregel maakt het mogelijk dat transactiemonitoring slechts door één partij en op één plek plaatsvindt. Hierbij is van belang te onderstrepen dat bij uitbesteding de bank altijd zelf verantwoordelijk blijft voor de naleving van de wettelijke verplichtingen.

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 transacties en patronen 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 geheimhoudingsverklaring 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. Daarbij is van belang dat het proces van (gezamenlijke) transactiemonitoring uit meerdere fasen bestaat. Fase 1 betreft het (gezamenlijk) genereren van alerts die mogelijk wijzen op een ongebruikelijke transactie. Deze fase vindt bij gezamenlijke transactiemonitoring plaats binnen de gezamenlijke voorziening. Fase 2 betreft het nader – door menselijke tussenkomst – onderzoeken van alerts door de individuele bank, teneinde te bepalen of al dan niet sprake is van een ongebruikelijke transactie die gemeld moet worden aan de FIU. Daarbij wordt bijvoorbeeld ook gekeken naar het klantdossier en de transactiehistorie van de betrokken klant. In geval van gezamenlijke transactiemonitoring vindt dit plaats buiten de gezamenlijke voorziening, nadat de betrokken individuele bank een melding heeft ontvangen van een alert vanuit de gezamenlijke voorziening. In fase 3 vindt de melding van ongebruikelijke transacties plaats aan de FIU. Het wetsvoorstel voorziet in de mogelijkheid voor banken om een gezamenlijke voorziening op te zetten voor het voldoen aan de verplichting tot een voortdurende controle van transacties (fase 1) en het melden van ongebruikelijke transacties (fase 3). Fase 2 wordt door medewerkers van de individuele banken uitgevoerd, zoals ook nu reeds het geval is bij door banken individueel uitgevoerde transactiemonitoring.

Rechten van betrokkenen

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) transactiemonitoring 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

Subsidiariteit

De voorgestelde maatregel laat de keuze over de wijze waarop transacties gezamenlijk gemonitord worden aan de banken en schrijft alleen voor dat dit dient te gebeuren binnen een daartoe

²⁸ Artikelen 12 tot en met 14 AVG.

²⁹ Artikel 15 AVG.

³⁰ Artikel 77 AVG.

³¹ Artikel 79 AVG.

opgezette gezamenlijke voorziening. Hierbij zijn twee alternatieven overwogen, te weten een gecentraliseerd model (gezamenlijke voorziening) en een gedecentraliseerd model van delen van transactiegegevens ten behoeve van gezamenlijke transactiemonitoring. Bij het gecentraliseerde model verzamelen banken transactiegegevens van hun cliënten en verstrekken zij deze aan een daartoe opgezette gezamenlijke voorziening ten behoeve van gezamenlijke transactiemonitoring binnen de voorziening. Bij het gedecentraliseerde model blijven de transactiegegevens in de systemen van de banken en voert een derde partij transactiemonitoring uit in de systemen van de individuele banken. Er is gekozen voor het gecentraliseerde model, 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. Daarom wordt in het wetsvoorstel voorgeschreven dat banken het gezamenlijk monitoren van transacties vormgeven middels een gezamenlijke voorziening.

Evenredigheid stelsel

Met het wetsvoorstel, en daarmee ook de voorgestelde maatregel betreffende het delen van transactiegegevens ten behoeve van gezamenlijke transactiemonitoring, wordt de aanpak van witwassen en terrorismefinanciering versterkt. Daarnaast zijn nog andere wettelijke maatregelen voor dit doel in voorbereiding. De AP heeft in haar advies op het wetsvoorstel uitgebreid stilgestaan bij de evenredigheid van het stelsel als geheel. Voor de nadere toelichting op dit onderwerp wordt daarom verwezen naar de bespreking van de adviezen in paragraaf 3.4.1.

C. Risico's en maatregelen

De risico's die spelen bij het delen van transactiegegevens en bij gezamenlijke transactiemonitoring, al dan niet door een derde partij, zien op legitimiteit, privacy en informatiebeveiliging. Bij risico's die zien op legitimiteit moet gedacht worden aan de kans dat door banken andere gegevens gedeeld worden dan de transactiegegevens die noodzakelijk zijn voor het doel, namelijk het voorkomen van witwassen en terrorismefinanciering. Bij privacygerelateerde 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. Risico's betreffende informatiebeveiliging zien bijvoorbeeld op de toegang tot gedeelde transactiegegevens door derden of onbevoegde medewerkers. Banken die gebruik willen maken van de mogelijkheid van gezamenlijke transactiemonitoring dienen vooraf via een GEB inzicht te geven in de mogelijke risico's hiervan en maatregelen te nemen om deze risico's te beperken of weg te nemen. Bij algemene maatregel van bestuur worden regels gesteld over te nemen maatregelen ter bescherming van de grondrechten en de fundamentele belangen van betrokkenen als gebruik wordt gemaakt van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard. De naleving van deze maatregelen is onderwerp van een door te betrekken instellingen uit te voeren onafhankelijke audit.

§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 terrorismefinanciering, 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. 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, worden middels een delegatiebepaling waarborgen gesteld. Hier wordt nader op ingegaan in de artikelsgewijze toelichting bij onderdeel I.

§3.4 Adviezen Autoriteit Persoonsgegevens

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

§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 verstreckende 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 paragraaf 3.1 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.

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.³² 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 surveillance-karakter van de dataretentierichtlijn voor de voorgestelde maatregel niet opgaat.

³² Advies conceptvoorstel Implementatiewet wijziging vierde anti-witwasrichtlijn.

§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 gegevens in het UBO-register. Op 16 december 2019 heeft de AP advies uitgebracht.³³

Naar aanleiding van het advies is besloten om met dit wetsvoorstel te voorzien in 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 zal aan de hand van het advies voor banken en notarissen toegang worden gegeven tot de gegevens in de BRP. Deze twee poortwachters spelen een belangrijke rol bij het voorkomen van witwassen en financieren van terrorisme en hebben beiden ervaring met de verwerking van gevoelige persoonsgegevens. Deze toegang vereist een wijziging van het Besluit basisregistratie personen. 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.

§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 terrorismefinanciering. 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 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

³³ Zie bijlage 3 bij kamerstukken II 2019/20, 31477, nr. 50.

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 het effect dat het verbod op contante betalingen vanaf € 3.000 zal hebben op de taakuitoefening van de Financial Intelligence Unit.

§4.1 Bureau Toezicht Wwft

BTWwft heeft naar aanleiding van dit wetsvoorstel een uitvoeringstoets uitgevoerd voor het verbod op contante betalingen vanaf € 3.000 euro voor handelaren. Uit de uitvoeringstoets volgt dat het verbod uitvoerbaar is.

In de uitvoeringstoets wordt vastgesteld dat in zijn algemeenheid het verbod een barrière opwerpt tegen witwassen en financieren van terrorisme. Wel geeft BTWwft aan dat 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, bijvoorbeeld door uit te wijken naar het buitenland of transacties op te knippen. Het karakter van witwassen zou ertoe kunnen leiden dat illegale geldstromen bewust aan het zicht worden onttrokken van autoriteiten. 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. 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. 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 terrorismefinanciering', 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 een hoger risico op witwassen of terrorismefinanciering. Hiermee wordt een meer risico gebaseerde 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 De Nederlandsche Bank t.a.v. aanvullende maatregelen trustdienstverlening

DNB heeft in haar uitvoeringstoets aangegeven dat het vanuit het perspectief van handhaafbaarheid, de voorkeur heeft dat trustdienst c uit de huidige wet (het ten behoeve van de cliënt gebruik maken van een doorstroomvennootschap) blijft bestaan en vergunningplichtig blijft. Dit zou dan gecombineerd kunnen worden met een verbod op het gebruik maken door trustkantoren van een doorstroomvennootschap. Een dergelijke invulling zou naar het oordeel van DNB beter aansluiten bij de systematiek van de Wtt 2018.

Deze constructie is in de consultatie ook geopperd door een andere partij. Vanuit wettechnisch oogpunt is het echter onwenselijk om een vergunningplicht voor een bepaalde activiteit in te regelen in een wet, om deze activiteit in dezelfde wet vervolgens te verbieden. Er wordt dan een vergunningprocedure in het leven geroepen op basis waarvan vervolgens niet gehandeld kan worden. Dit zorgt niet alleen voor onduidelijkheid, maar ook voor mogelijke onnodige lasten bij zowel instellingen als de toezichthouder. In dit wetsvoorstel is met de definiëring van doorstroomvennootschap wel getracht zoveel mogelijk te blijven bij de definitie van doorstroomvennootschap in de huidige wet.

Ten aanzien van partijen die mogelijk beroeps- of bedrijfsmatig doorstroomvennootschappen

aanbieden of ter beschikking stellen en hiermee tegen het verbod in handelen, geeft DNB aan het voor haar lastig zal zijn hier alleen handhavend op te treden. In haar argumentatie wordt als uitgangspunt genomen de definitie van doorstroomvennootschap uit de wettekst voor consultatie. Aangezien de definitie van doorstroomvennootschap na de consultatie is aangepast, zullen veel van de praktische problemen die DNB noemt zich niet meer voordoen. Zo zal DNB niet meer hoeven vast te stellen of sprake is van (i) een 'economische activiteit', en (ii) gebruik dat niet tot doel heeft om te voldoen aan enige wettelijke verplichting.

DNB geeft ten aanzien van het verbod van artikel 23a aan dat zij verwacht een eenmalige en een doorlopende inspanning voor de handhaving van dit voorschrift te moeten uitvoeren. Zo zal er bijvoorbeeld eenmalig een controle onder trustkantoren moeten worden uitgevoerd om te bezien in hoeverre trustkantoren die cliënten in portefeuille hebben die onder deze bepaling vallen, dienstverlening aan deze cliënten beëindigen. DNB zal onder andere haar jaarlijkse uitvraag hiervoor gebruiken.

Tot slot geeft DNB aan dat het wenselijk is om een overgangstermijn in te regelen voor zowel artikel 3a als artikel 23a. Hier is gevolg aan gegeven.

§4.4 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.

§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 drie nieuwe verplichtingen voor instellingen, namelijk (1) het verbod op contante betalingen vanaf € 3.000 voor beroeps- of bedrijfsmatige handelaren van goederen, (2) de verplichting voor instellingen om in het kader van het cliëntenonderzoek navraag te doen naar gebleken risico's op witwassen en terrorismefinanciering bij eerdere dienstverlening en (3) aanvullende maatregelen voor de trustdienstverlening.

§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 verzwaaard indien de instelling een hoger risico op witwassen of terrorismefinanciering vaststelt bij een cliënt. Er wordt namelijk van instellingen verlangd dat zij in een dergelijk geval nagaan of de cliënt de afgelopen vijf jaar gebruik heeft gemaakt van dienstverlening van een andere instelling behorend tot dezelfde categorie. In 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 terrorismefinanciering, 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 terrorismefinanciering bij de instelling waar de cliënt voorheen diensten heeft afgenomen. 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 terrorismefinanciering neer op € 69,75. Omdat het op voorhand onduidelijk is bij hoeveel transacties of zakelijke relaties instellingen zullen vaststellen dat er sprake is van een indicatie op een hoger risico op witwassen of financieren van terrorisme zijn de totale kosten van de verplichting niet kwantificeerbaar. Dit is in hoge mate 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.

§5.1.3 Aanvullende maatregelen trustdienstverlening

De structurele regeldruk voor trustkantoren zal afnemen door invoering van de voorgestelde maatregelen, nu diensten die op dit moment nog worden aangeboden en waarvoor verplichtingen gelden, in zijn geheel worden verboden. Op dit moment zullen trustkantoren veelal verscherpt cliëntenonderzoek verrichten in geval van het aanbieden van doorstroomvennootschappen of in geval van dienstverlening waarbij partijen betrokken zijn uit derde hoog risicolanden of landen die op de lijst staan van non-coöperatieve landen op belastinggebied. Deze verscherpte controle houdt in dat trustkantoren extra onderzoeksmaatregelen moeten treffen, naast het gebruikelijke cliëntenonderzoek. Door de invoering van de voorgestelde maatregelen zal dit niet meer het geval zijn, nu de betreffende diensten verboden worden. Naast het cliëntenonderzoek gelden voor deze diensten ook de andere verplichtingen op grond van de Wtt 2018 niet meer, zoals het monitoren van transacties. Wel zullen trustkantoren binnen hun huidige portefeuille moeten bekijken welke cliënten onder het verbod vallen. Naar verwachting zal dit niet veel extra werk opleveren nu deze gegevens vastgelegd zullen zijn in de cliëntendossiers.

Zoals eerder gesteld zal de structurele regeldruk voor trustkantoren met de invoer van de nieuwe verboden afnemen. Trustkantoren zullen met ingang van de aangepaste wet, echter wel de huidige dossiers eenmalig moeten doorlichten om na te gaan of ze aan de nieuwe wet voldoen. Voor wat betreft dit onderzoek (doorlichten van cliëntendossiers) geldt dat het informatie betreft die al beschikbaar zou moeten zijn in de cliëntendossiers. Dit omdat trustkantoren veelal lijsten en overzichten bijhouden van hun cliëntendossiers, waarin ook gegevens in opgenomen staan over UBO's, hoog risicolanden etc. Voor het doorlichten van dossiers wordt gemiddeld gerekend op maximaal twee weken (fulltime) werk, wat neerkomt op $2 \times 40 \text{ uur} = 80 \text{ uur}$. Het uurtarief van de compliance functie is gemiddeld genomen 54 euro per uur. De eenmalige kosten voor het doorlichten van cliëntendossiers wordt hiermee geschat op (eenmalig) 4320 euro, per trustkantoor. Hier staat echter tegenover dat de lopende compliance werkzaamheden en monitoring (zoals bijvoorbeeld transactiemonitoring) voor deze dossiers gestopt kunnen worden wat tot gevolg heeft dat de netto-kosten veel lager zullen uitvallen dan de schatting van € 4320 per trustkantoor.

Daarbij zal elke keer als een land op de landenlijst geplaatst wordt een opschoning moeten plaatsvinden. Echter na inwerkingtreding van deze wet zullen naar alle waarschijnlijkheid veel trustkantoren de specifieke informatie in het kader van artikel 23a gaan bijhouden waardoor doorlichten van de dossiers snel kan plaatsvinden. En ook hierbij geldt dat de kosten voor het opschonen van de cliëntenlijsten en het beëindigen van de cliëntrelaties in de plaats zullen komen van de lopende compliance kosten.

Momenteel zijn er 140 trustkantoren actief, waarmee het totaal aan eenmalige kosten in verband met de nieuwe maatregelen uitkomt op € 604.800. Hier staat echter tegenover dat, de lopende compliance werkzaamheden, zoals verscherpte controles en transactiemonitoring, kunnen stoppen. Kortom, de nieuwe maatregelen leiden tot eenmalige doorlichtingskosten en structureel tot verminderende (lopende) compliance-kosten.

§5.2 Adviescollege Toetsing en Regeldruk

Het Adviescollege Toetsing en Regeldruk heeft in haar advies aandacht gevraagd voor de eerste drie 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 eerdere dienstverlener aanreikt dienen als een niet-bindende aanvulling en de instelling dus niet van de verplichting ontslaan tot het maken van een eigen individuele risicoafweging. De verwachting is zodoende niet dat deze maatregel zal leiden tot een verhoging van het aantal cliënten dat ten onrechte wordt uitgesloten van dienstverlening. Overigens kunnen consumenten en kleine 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.

Het college heeft afzonderlijk geadviseerd ten aanzien over de aanvullende maatregelen voor trustdienstverlening. Het college heeft geadviseerd de regeldrukeffecten tevens kwantitatief uit te werken. Daarbij is aangegeven dat er ook een totaalbeeld van de kosten dient te worden gegeven. Beide punten zijn opgevolgd en verwerkt in de voorgaande paragraaf.

§6. Openbare consultatie

De eerste drie onderdelen van dit wetsvoorstel en de aanvullende maatregelen bij trustdienstverlening zijn apart geconsulteerd.³⁴ Hieronder zal eerst op de consultatie ten aanzien van de eerste drie onderdelen ingegaan worden. Daarna zal ingegaan worden op de consultatie van de aanvullende maatregelen bij trustdienstverlening.

§6.1 Eerste drie onderdelen wetsvoorstel

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 Nederlandse Vereniging van Banken, de Nederlandse Vereniging voor Rechtspraak en Netwerk Notarissen. Ook individuele instellingen hebben gebruik gemaakt van de gelegenheid om een reactie in te sturen, waaronder advocatenkantoren, 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.

§6.1.1 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.

§6.1.2 Verbod op contante betalingen vanaf € 3.000

³⁴ De internetconsultatie voor de eerste drie onderdelen is terug te vinden op: <https://www.internetconsultatie.nl/wetplanvanaanpakwitwassen>
De internetconsultatie voor de maatregelen bij trustdienstverlening is terug te vinden op: <https://www.internetconsultatie.nl/wijzigingwtt2018>

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.³⁵ 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 - 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

³⁵ National Risk Assessment, *Wetenschappelijk Onderzoek- en documentatiecentrum*, Cahier 2020-11, p. 52.

ongebruikelijke transacties meer gemeld te worden bij de FIU-Nederland. Bij de evaluatie van de maatregel zal ook aan deze punten aandacht worden besteed.

§6.1.3 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. 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 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 goed 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 terrorismefinanciering 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.

§6.1.4 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.

§6.1.5 Gegevensbescherming

§6.1.5.1 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.

§6.1.5.2 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.

§6.2 Aanvullende maatregelen trustdienstverlening

In de periode van 9 april 2020 tot en met 7 mei 2020 is een concept van dit onderdeel van het wetsvoorstel publiek geconsulteerd. Naar aanleiding van de publieke consultatie zijn acht reacties ontvangen, die allemaal openbaar zijn. De openbare reacties zijn afkomstig van Pellicaan Advocaten, Portunus Services en Develop Your Controls (DYC) B.V., Van Campen Liem, NVVTK, Holland Quaestor en drie particulieren.

Naar aanleiding van de consultatiereacties zijn de wettekst en de memorie van toelichting op een aantal punten aangepast. In het navolgende zullen de ontvangen reacties, voor zover relevant voor dit wetsvoorstel, per thema worden beschreven.

§6.2.1 Doorstroomvennootschappen

De nieuwe definitie van doorstroomvennootschap heeft tot veel vragen geleid en is daarom aangepast. Vooropgesteld dient te worden dat dit wetsvoorstel trustdienst c, wat nu een vergunningplichtige activiteit is, verbiedt aan eenieder. De huidige definitie van doorstroomvennootschap dient als basis van het nieuwe verbod. Er is voor gekozen om de elementen "economische activiteit" en "wettelijke verplichting" uit de definitie te halen omdat deze elementen voor verwarring leken te zorgen. Het is immers niet bedoeling meer of andere dienstverlening te verbieden dan op dit moment vergunningplichtig is. Wel is in artikel 5 van de Wtt 2018 toegevoegd dat het mogelijk is bij ministeriële regeling vrijstelling te regelen van het verbod.

Eén van de voorstellen die is gedaan in de consultatiereacties is om doorstroomvennootschap als vergunningplichtige activiteit te laten staan, en deze activiteit vervolgens te verbieden in de wet. Dit is praktisch gezien misschien een goede oplossing, maar juridisch gezien niet. Het is namelijk niet juridisch correct als er eerst een vergunningplicht in het leven wordt geroepen voor een activiteit om dezelfde activiteit vervolgens te verbieden. In dit wetsvoorstel is met de definiëring van doorstroomvennootschap wel getracht zoveel mogelijk te blijven bij de definitie van doorstroomvennootschap in de huidige wet.

Uit de laatste statistieken van DNB blijkt dat er in de trustsector nog maar tien doorstroomvennootschappen gebruikt worden. Dit vanwege de hoge integriteitsrisico's die trustkantoren zelf aan deze dienstverlening toekennen. Een veel gehoord bezwaar tegen het verbod van artikel 3a is dat het gebruikmaken van doorstroomvennootschappen de illegaliteit in zal verdwijnen. Bij het reguleren van activiteiten of diensten bestaat er altijd een kans dat er iets verdwijnt in de illegaliteit. De kans dat er echter een hele illegale markt tot stand komt voor het gebruik van doorstroomvennootschappen lijkt onwaarschijnlijk gezien de laatste statistieken van DNB.

Verschillende partijen hebben tot slot opgemerkt dat een overgangstermijn wenselijk is, dit verzoek is opgevolgd en ingeregeld in artikel V van dit wetsvoorstel.

§6.2.2 Dienstverlening waarbij landen betrokken zijn die op de lijst van derde-hoog risicolanden en/of de lijst van non-coöperatieve landen op belastinggebied staan

Voor de invoering van deze verboden is gekozen omdat blijkt dat de sector de integriteitsrisico's die gepaard gaan met haar dienstverlening onvoldoende beheerst. Op basis van de huidige wet dienen trustkantoren verscherpt cliëntenonderzoek te verrichten indien een zakelijke relatie of trustdienst naar zijn aard een hoger risico op witwassen of financieren van terrorisme met zich brengt. Deze maatregelen hebben echter niet tot het gewenste effect geleid en daarom wordt dienstverlening aan cliënten, doelvennootschappen, uiteindelijk belanghebbenden van cliënten en uiteindelijk belanghebbenden van doelvennootschappen woonachtig of gevestigd in derde-hoog risicolanden en non-coöperatieve landen op belastinggebied, nu verboden. Dit is een stap verder dan hetgeen geldt op basis van de huidige wet; eerst was de dienstverlening onder strikte voorwaarde mogelijk, met dit wetsvoorstel wordt het verboden. Hiervoor is dus gekozen omdat de sector nog steeds niet op het integriteitsniveau is dat verantwoord is.

Nederland dient op basis van de Europese anti-witwasrichtlijn maatregelen te treffen om integriteitsrisico's op een passende wijze te beheersen en te beperken. Deze richtlijn is geïmplementeerd onder minimumharmonisatie, Nederland mag dus verder gaan dan de maatregelen zoals opgenomen in de richtlijn. Kortom, Nederland kan dienstverlening aan cliënten, doelvennootschappen, uiteindelijk belanghebbenden van cliënten en uiteindelijk belanghebbenden van doelvennootschappen woonachtig of gevestigd in derde-hoog risicolanden en non-coöperatieve landen op belastinggebied verbieden. In de consultatiereacties werd deze vraag expliciet gesteld.

In één van de reacties vraagt men zich af of er niet wordt gehandeld in strijd met het lex certa beginsel door de verboden te verbinden aan dynamische landen lijsten. Het lex certa beginsel is

gebaseerd op het legaliteitsbeginsel. Dit beginsel komt er in de kern op neer dat de overheid slechts een sanctie kan opleggen indien hier een wettelijke basis voor is. Indien partijen het verbod van artikel 23a niet naleven kan er bestuursrechtelijk worden opgetreden. Dit is helder neergelegd in de wet en daarom is er geen strijdigheid met het *lex certa* beginsel. Indien een trustkantoor vooraf communiceert over het verbod van artikel 23a, bijvoorbeeld door dit op te nemen in haar algemene voorwaarden, dan zal tevens geen sprake zijn van rechtsonzekerheid in de contractuele relatie nu partijen weten dat de zakelijke relatie elk moment opgezegd kan worden indien bepaalde landen op de betreffende lijsten worden geplaatst.

Ook bij artikel 23a is door een aantal partijen opgemerkt dat de dienstverlening nu de illegaliteit in zal verdwijnen. Zoals eerder gesteld blijft dit altijd een risico. Dit zal echter goed gemonitord worden en indien er signalen zijn dat deze dienstverlening massaal in de illegaliteit wordt voortgezet dan zullen de nodige maatregelen worden getroffen.

Het argument dat deze dienstverlening juist bij trustkantoren belegd moet worden vanwege de integriteitsrisico's, gaat helaas niet meer op. Het vertrouwen dat de sector kennis heeft van de integriteitsrisico's en deze afdoende mitigeert is er niet volledig. Omdat de sector het lastig vindt om integriteitsrisico's te identificeren en te mitigeren is ervoor gekozen om bepaalde risico's helemaal buiten spel te plaatsen, door bepaalde dienstenverlening te verbieden.

Verschillende partijen hebben opgemerkt dat een overgangstermijn wenselijk is, dit verzoek is opgevolgd en ingeregeld in artikel V van dit wetsvoorstel.

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. 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 in een handeling of door middel van meer 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. Dit is om te voorkomen dat het verbod wordt omzeild. Dit blijft gehandhaafd.

Het verbod geldt voor betalingen in contanten die in of vanuit Nederland worden verricht. Hierbij is het territorialiteitsbeginsel leidend. Dit betekent dat contante betalingen die in het buitenland worden verricht, niet onder de Nederlandse regelgeving vallen. Indien een Nederlandse handelaar in het buitenland goederen koopt of verkoopt en daarbij contant betaalt of contant geld accepteert, vallen deze transacties niet onder de reikwijdte van de Wwft. Dit geldt ongeacht of de Nederlandse handelaar die contante transacties op een later moment in de eigen administratie opneemt.

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 eerder 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 terrorismefinanciering 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 Wtt 2018.

De verplichting opgenomen in het eerste lid bestaat uit verschillende componenten, deze worden hieronder toegelicht. Een instelling dient voorafgaand aan het aangaan van de zakelijke relatie of transactie een inschatting te maken van de risico's op witwassen of terrorismefinanciering die dit met zich brengt. De onderzoeksplicht is een 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 terrorismefinanciering met zich meebrengt. 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 ontstaan van betrokkenheid bij witwassen of financieren van terrorisme. 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 cliënt 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. Voor een uitgebreide toelichting op dit onderzoek wordt verwezen naar

paragraaf 2.2.1 van het algemene deel van de toelichting.

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 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 terrorismefinanciering onverwijld te verstrekken. 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 Algemene verordening gegevensbescherming. Voorts geldt de bewaartermijn van vijf jaar, opgenomen in artikel 33, derde lid, van de Wwft onverkort. 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 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 vierde lid. Ook reeds bestaande cliënten dienen hierover geïnformeerd te worden. 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 terrorismefinanciering die na inwerkingtreding van dit wetsvoorstel zijn gebleken.

In het vijfde 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 terrorismefinanciering 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 terrorismefinanciering 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 h, waar zowel makelaars 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 terrorismefinanciering geconstateerd bij een cliënt door een instelling uit een categorie relevant zijn voor de risicoafweging voor een instelling uit een andere

categorie.

In het zesde 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 terrorismefinanciering 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.

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 1a, tweede lid, om een gezamenlijke voorziening voor het monitoren van transacties op te zetten. Hiertoe wordt in het nieuwe tweede lid banken de bevoegdheid gegeven om het cliëntenonderzoek, waaronder transactiemonitoring, opgenomen in artikel 3, tweede lid, onderdeel d, alsmede het melden van ongebruikelijke transacties, opgenomen in artikel 16, eerste lid, uit te besteden aan een derde. Het uitgangspunt dat de instelling zelf verantwoordelijk is, blijft ongewijzigd. Dit geldt voor alle onder d genoemde onderdelen van de voortdurende controle op de zakelijke relatie. Het blijft immers de verantwoordelijkheid van de banken om aan de hand van de resultaten van de uitbestede activiteiten te beoordelen of en zo ja welke maatregelen genomen moeten worden. Zo blijft de bank zelf verantwoordelijk voor het al dan niet melden van een ongebruikelijke transactie op grond van artikel 16 Wwft of het nemen van andere maatregelen ten aanzien van de cliëntrelatie (paragraaf 1.2 van de Wwft). Op die manier blijven instellingen volledig zicht houden op de resultaten van de uitbestede activiteiten en zal dit niet ten kosten gaan van de mogelijkheid van instellingen voor risicobeoordeling.

Indien een instelling verplichtingen waarbij persoonsgegevens worden verwerkt uitbesteedt, 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 overige voorschriften in 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 gaat het om voorwaarden om te voorkomen dat het toezicht op de naleving van de verplichting niet wordt bemoeilijkt door uitbesteding. 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 en 3b 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 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 paragraaf 3.1 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 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 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 en het melden van ongebruikelijke transacties. Op grond van het eerste lid kunnen banken een gezamenlijke voorziening opzetten om te voldoen aan de verplichtingen uit artikel 3, tweede lid, onderdeel d, om transacties voortdurend te controleren en artikel 16 van de Wwft om ongebruikelijke transacties te melden aan de FIU-Nederland. Het opzetten van een dergelijke voorziening is een gezamenlijke vorm van uitbesteding op grond van artikel 10, tweede lid. In het tweede lid is opgenomen dat banken alleen binnen deze gezamenlijke voorziening gegevens betreffende transacties kunnen delen. Uit de twee eerste leden volgt dat de gegevens alleen voor het uitvoeren van transactiemonitoring en ten behoeve van het melden van ongebruikelijke transacties 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.

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 een eigen verantwoordelijkheid van de instellingen.

In het algemeen deel van de toelichting is reeds opgemerkt dat het delen van transacties tussen meerdere banken risico's voor de bescherming van persoonsgegevens met zich brengt, onder andere omdat het kan gaan om grote hoeveelheden data die tussen meerdere partijen worden gedeeld. 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 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 vierde lid is opgenomen dat de onderlinge verstrekking van de gegevens, bedoeld in het eerste lid, dient te worden beëindigd als die verstrekking niet langer noodzakelijk is voor het melden van ongebruikelijke transacties als bedoeld in artikel 16 van de Wwft. De gegevens dienen op dat moment vanzelfsprekend te worden verwijderd.

In het vijfde lid 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. In dat kader dient het verslag ook in te gaan in hoeverre de voorziening bijdraagt aan het filteren van zogenaamde *false positives* (transacties waarvan achteraf blijkt dat deze onterecht als risico zijn aangemerkt). 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 twee jaar na ingebruikname van de voorziening. Daarna dient deze elke vijf jaar plaats te vinden. Het jaarverslag en de resultaten van de onafhankelijke audit dienen openbaar te worden gepubliceerd.

Artikel II (*Wijziging Wet toezicht trustkantoren 2018*)

Onderdeel A (*wijziging artikel 1*)

Het begrip doorstroomvennootschap vervalt, omdat er een algeheel verbod wordt ingevoerd voor het beroeps- en bedrijfsmatig aanbieden van doorstroomvennootschappen. In het verlengde hiervan wordt de trustdienst als bedoeld in onderdeel c, van de begripsomschrijving van trustdienst in artikel 1, eerste lid, van de Wtt 2018, geschrapt en worden de onderdelen d tot en met f geletterd c tot en met e.

Onderdeel B (*nieuw artikel 3a*)

Met artikel 3a wordt het beroeps- of bedrijfsmatig gebruik maken van

doorstroomvennootschappen ten behoeve van een cliënt verboden. Met dit verbod wordt de dienst die op dit moment nog vergunningplichtig is en beschreven is in artikel 1, eerste lid, onderdeel c van de begripsomschrijving van trustdienst, verboden. Voor een inhoudelijke toelichting wordt verwezen naar paragraaf 2.4.1 van het algemeen deel van deze toelichting.

Onderdeel C (*wijziging artikel 5*)

In artikel 5, eerste lid, wordt het nieuwe artikel 3a toegevoegd, zodat het mogelijk wordt om, net als voor de andere verboden in de Wtt 2018, vrijstelling te verlenen van het verbod om beroeps- of bedrijfsmatig gebruik te maken van doorstroomvennootschappen ten behoeve van een cliënt.

Onderdeel D (*wijziging artikel 19*)

Het eerste lid van artikel 19 vervalt omdat de trustdienst als bedoeld in onderdeel c, van de begripsomschrijving van trustdienst in artikel 1 van de Wtt 2018, (doorstroomvennootschap) wordt geschrapt.

Onderdeel E (*nieuw artikel 23a*)

Artikel 23a wordt ingevoegd om dienstverlening, waarbij landen betrokken zijn die op de lijst van derde-hoogrisicolanden staan of op de lijst van non-coöperatieve landen op belastinggebied, te verbieden. Zoals in paragrafen 2.4.2 en 2.4.3 van het algemeen deel van deze toelichting is aangegeven, gaat het om gevallen waarbij de cliënt, de doelvennootschap of de uiteindelijk belanghebbende van de cliënt of doelvennootschap woonachtig of gevestigd is of zijn zetel heeft in één van die landen.

Er is sprake van een dynamische verwijzing naar de genoemde lijsten omdat die lijsten van tijd tot tijd geactualiseerd worden aan de hand van de meest recente inzichten. Dit betekent dat trustkantoren wijzigingen van deze lijsten in de gaten moeten houden. Voor de lijst van derde-hoogrisicolanden gold dit al omdat bij betrokkenheid van landen op die lijst op grond van de huidige wet al verscherpt cliëntenonderzoek verricht moet worden.

Het tweede lid van artikel 23a bevat een overgangstermijn. Op het moment dat een land wordt toegevoegd aan de betreffende lijsten, zal een trustkantoor dienen na te gaan of er diensten worden verleend die vanaf dat moment onder het verbod vallen. Trustkantoren hebben op grond van dit lid drie maanden de tijd om de betreffende dienstverlening te staken.

Onderdeel F (*verval artikel 28*)

Artikel 28 komt te vervallen omdat de trustdienst als bedoeld in onderdeel c, van de begripsomschrijving van trustdienst in artikel 1 van de Wtt 2018, wordt geschrapt.

Onderdeel G, H, I en J (*wijziging artikelen 28, 29 en 30 (nieuw)*)

De artikelen 29 tot en met 30a worden vernummerd tot 28 tot en met 30, zodat de nummering van de artikelen rond het cliëntenonderzoek doorloopt.

In verband met het schrappen van de trustdienst doorstroomvennootschap en het wijzigen van de lettering van de trustdiensten in artikel 1, worden enkele technische wijzigingen aangebracht in de vernummerde artikelen 28, 29 en 30.

Onderdeel K (*wijziging artikel 33*)

Onderdeel b van artikel 33, eerste lid, komt te vervallen nu deze dienstverlening onder de verbodsbepaling van artikel 23a komt te vallen. Daarmee bestaat het eerste lid niet meer uit

verschillende onderdelen.

Onderdeel L (*verval artikel 36*)

In verband met de invoering van het verbod van artikel 23a lid 1 sub a, komt artikel 36 te vervallen. Dit omdat het treffen van bijzondere maatregelen bij dienstverlening met betrokkenheid van derde-hoogrisicolanden niet aan de orde zal zijn nu er een algeheel verbod voor dienstverlening geldt.

Onderdeel M (*wijziging artikel 55*)

Dit betreft een herstelbepaling. Het toe te voegen derde lid was abusievelijk komen te vervallen bij de totstandkoming van de Wtt 2018. Het derde lid brengt met zich mee dat dat DNB ook aangifte mag doen en in dat kader informatie mag delen met het OM. Eenzelfde bepaling is opgenomen in de Wwft (art. 22, lid 3).

ARTIKEL III (*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 terrorismefinanciering 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.

Daarnaast worden de nieuwe bepalingen in de artikelen 3a en 23a van de Wtt 2018 strafbaar gesteld. Het betreft het verbod om beroeps- of bedrijfsmatig gebruik maken van doorstroomvennootschappen ten behoeve van een cliënt. Daarnaast gaat het om het verbod van dienstverlening, waarbij landen betrokken zijn die op de lijst van derde-hoogrisicolanden staan of op de lijst van non-coöperatieve landen op belastinggebied. Aangezien de artikelen 28 en 36 van de Wtt 2018 vervallen, vervallen deze ook als strafbaar gestelde artikelen.

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

ARTIKEL V (*overgangstermijn artikelen 3a en 23a Wtt 2018*)

Dit artikel regelt een overgangstermijn voor de nieuwe verboden in artikel 3a en 23a van de Wtt 2018. Op het moment dat deze onderdelen van de wet in werking treden, zullen trustkantoren activiteiten die voortaan onder deze verboden vallen, dienen te staken. Daarvoor zal onder meer een doorlichting van de bestaande dossiers dienen plaats te vinden. De betreffende partijen waar het om gaat hebben trustkantoren al goed in beeld, vanwege de verscherpte maatregelen die ze op basis van de huidige nemen. Trustkantoren krijgen zes maanden de tijd om de zakelijke relatie te beëindigen. Een termijn van zes maanden wordt redelijk geacht omdat dit partijen afdoende tijd geeft om de werkzaamheden af te ronden.

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

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 gezien.

ARTIKEL VII *(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,