Bijlage I bij plan van aanpak witwassen: Onderzoek informatie-uitwisseling

1. Inleiding

In mijn agenda financiële sector van december 2018 heb ik aangekondigd dat ik samen met de sector, DNB en AFM onderzoek doe naar de mogelijkheden voor informatie-uitwisseling om de uitvoering van het cliëntenonderzoek door Wwft-instellingen effectiever te maken. Doel is het voorkomen dat cliënten door gebruikmaking van verschillende dienstverleners misbruik van het financiële stelsel kunnen maken. Een zestal vormen van informatie-uitwisseling is onderzocht. Mede naar aanleiding van toezeggingen aan de Tweede Kamer is tevens de Autoriteit Persoonsgegevens (AP) betrokken en is ook gekeken naar andere landen. In dit document doe ik verslag van de resultaten van het onderzoek.

Dit verslag bestaat uit de volgende onderdelen. Allereerst licht ik in paragraaf 2 de gehanteerde werkwijze toe. Vervolgens geef ik in de derde paragraaf een beschrijving van het relevante wettelijke kader. Daarbij besteed ik aandacht aan drie verschillende terreinen, namelijk de anti-witwasregelgeving, de privacyregelgeving en de mededingsregelgeving. Daarna geef ik in paragraaf 4 een beschrijving van de zes vormen van informatie-uitwisseling die zijn onderzocht. In de vijfde paragraaf kijk ik naar de mogelijkheden van informatie-uitwisseling in andere landen. Ik besteed aandacht aan een aantal goede voorbeelden op dit punt. Ten slotte sluit ik af met een conclusie waarin ik een oordeel vel over de proportionaliteit en wenselijkheid van de onderzochte opties.

2. Werkwijze

In het onderzoek heb ik gekeken naar zes vormen van informatie-uitwisseling die mogelijk een bijdrage kunnen leveren aan het effectiever vervullen van de poortwachtersfunctie. Ik ben tot deze zes vormen gekomen aan de hand van suggesties vanuit de sector, van autoriteiten en uit het publieke debat. Dit betreffen:

1. verbeteren van informatiedeling t.b.v. publiek-private samenwerking (PPS);
2. delen van informatie over cliënten (KYC Utility);
3. delen van informatie over transacties (TM Utility);
4. delen van informatie over ongebruikelijke klanten;
5. gebruik van het BSN-nummer en toegang tot de Basisregistratie Personen (BRP) en
6. toegang tot de afgesloten gegevens in het UBO-register.

De centrale vraag bij de onderzochte vormen van informatie-uitwisseling is of, alle afwegingen in ogenschouwgenomen, deze proportioneel en wenselijk zijn. De rode lijn in de verschillende vormen van informatie-uitwisseling is de afweging van een effectievere vervulling van de poortwachtersrol ten opzichte van een inbreuk op de bescherming van persoonsgegevens van betrokkenen. Elke inbreuk moet getoetst worden op noodzakelijkheid, waarbij de proportionaliteit en subsidiariteit moeten worden afgewogen. Met andere woorden: verhoudt de inbreuk zich tot het te bereiken doel en is er geen minder ingrijpende manier om het doel te bereiken.

Er is met de Nederlandse Vereniging van Banken (NVB) en verschillende grote en kleinere banken. Ook zijn diverse gesprekken gevoerd met betrokken toezichthouders, opsporingsautoriteiten en de FIU-Nederland. De resultaten van het onderzoek zijn vervolgens besproken met de sector en de autoriteiten. Ook is de analyse ambtelijk besproken bij de Autoriteit Persoonsgegevens en de Autoriteit Consument en Markt.

Tot slot is ook gekeken naar informatie-uitwisseling in het kader van anti-witwasbeleid in andere landen. De focus lag daarbij op internationaal bekende goede voorbeelden hiervan.

Het onderzoek naar informatie-uitwisseling heeft zich specifiek op banken gericht, maar de uitkomsten zijn ook van belang voor de andere instellingen die onder de Wwft vallen zoals andere financiële instellingen als levensverzekeraars, en beroepsbeoefenaars als advocaten en notarissen.

3. Wettelijk kader

Het relevante wettelijke kader van dit onderzoek wordt gevormd door drie soorten regelgeving. Dat is allereerst de anti-witwasregelgeving. Dit kader bestaat uit mondiale standaarden van de Financial Action Task Force (FATF), de Europese (gewijzigde) vierde anti-witwasrichtlijn en de nationale Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). Het tweede kader is de privacyregelgeving. Dit bestaat uit de Europese Algemene Verordening Gegevensbescherming (AVG) en de nationale Uitvoeringswet Algemene Verordening Gegevensbescherming (uAVG). Naast de AVG is ook de richtlijn relevant die de gegevensbescherming door politie en justitie regelt. Deze richtlijn[1] bevat regels voor de verwerking van persoonsgegevens door bevoegde autoriteiten om strafbare feiten te voorkomen, te onderzoeken, op te sporen en te vervolgen. Deze richtlijn is geïmplementeerd in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Ten derde betreft dit de Mededingsregelgeving. Dit kader wordt gevormd door het Werkingsverdrag van de Europese Unie (TFEU) en de nationale Mededingingswet (Mw).

3.1. Anti-witwasregelgeving

Het systeem van financiële dienstverleners als poortwachters ter bescherming van het financiële stelsel volgt uit de standaarden van de FATF en de (gewijzigde) vierde anti-witwasrichtlijn, die in de Wwft zijn geïmplementeerd. Het zijn van poortwacrengt met zich mee dat onderzoek gedaan moet worden naar de cliënt en transacties gemonitord moeten worden. De vierde anti-witwasrichtlijn (hierna: de richtlijn) bepaalt dat een instelling cliëntenonderzoek moet verrichten.[2] Daarnaast bepaalt de richtlijn dat een instelling verdachte transacties moet melden bij de FIU (transactiemonitoring).[3]

Om te kunnen voldoen aan de hiervoor genoemde verplichtingen – cliëntenonderzoek en transactiemonitoring - moet een instelling persoonsgegevens verwerken. De richtlijn bepaalt dat deze verwerking overeenkomstig de Algemene Verordening Gegevensbescherming dient plaats te vinden. Persoonsgegevens mogen door instellingen alleen worden verwerkt met het oog op het voorkomen van witwassen en terrorismefinanciering, en niet verder worden verwerkt op een manier die niet verenigbaar is met dit doel. De verwerking van persoonsgegevens voor andere doeleinden, zoals commerciële doeleinden, is verboden.[4] De richtlijn kent een specifiek geheimhoudingsregime voor meldingen aan de FIU. Het is de instelling verboden om aan de cliënt of aan derden te laten weten dat een transactie als verdacht is aangemerkt en is gemeld bij de FIU. Ook mag een instelling niet laten weten dat er een (intern) onderzoek is ingesteld naar de cliënt en/of de transactie (tipping-off verbod).[5] Dit betekent dat zolang een transactie niet als verdacht is aangemerkt, de richtlijn niet verbiedt dat deze gedeeld wordt.

Bovenop bovenstaande punten is specifiek voor de Nederlandse wetgeving (Wwft) dat instellingen ongebruikelijke transacties moeten melden bij de FIU en niet enkel verdachte transacties.[6] Het tipping-off verbod geldt in Nederland voor ongebruikelijke transacties. Daarnaast staat de Wwft uitbesteding van de transactiemonitoring niet toe.[7]

---

[1] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad
[2] Art. 10 e.v. AMLD4
[3] Art. 33 AMLD4
[4] Art. 41 AMLD4
[5] Art. 39 AMLD4
[6] Art. 16 Wwft
[7] ibidem

3.2. Privacyregelgeving

Om persoonsgegevens te kunnen gebruiken is een verwerkingsgrondslag nodig. Artikel 6 AVG noemt zes limitatieve gronden voor de verwerking van persoonsgegevens. Een verwerking van persoonsgegevens kan alleen rechtmatig zijn indien de verwerking in het kader van de desbetreffende grondslag proportioneel en subsidiair is. Voor dit onderzoek zijn met name twee verwerkingsgrondslagen van belang, namelijk het geven van toestemming[8] en het bestaan van een wettelijke verplichting. Het geven van toestemming is aan een aantal voorwaarden verbonden. Zo moet het verzoek om toestemming in begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke een eenvoudige taal gepresenteerd worden. Ook moet de toestemming te allen tijde kunnen worden ingetrokken en moet de toestemming vrijelijk worden gegeven.[9] Indien de verwerking van persoonsgegevens, in het bijzonder als het een verwerking betreft waarbij nieuwe technologieën worden gebruikt, gelet op de aard, omvang, context en doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, moet vóór de verwerking een gegevensbeschermingseffectbeoordeling (GEB) worden uitgevoerd.[10] Als uit deze GEB blijkt dat de verwerking een hoog risico oplevert, moet de Autoriteit Persoonsgegevens voorafgaand aan de verwerking geraadpleegd worden.[11]

Naast ‘gewone’ persoonsgegevens kunnen ook strafrechtelijke persoonsgegevens verwerkt worden. Onder strafrechtelijke persoonsgegevens vallen niet alleen veroordelingen maar ook mogelijk gegronde verdenkingen. In het geval dat private partijen met elkaar gegevens uitwisselen over mogelijk gepleegde strafbare feiten kan er dus sprake zijn van strafrechtelijke gegevens. Bij het delen van strafrechtelijke persoonsgegevens tussen private partijen geldt in beginsel een verwerkingsverbod. Net als bij de verwerking van ‘gewone’ persoonsgegevens geldt bij de verwerking van strafrechtelijke persoonsgegevens dat de verwerking rechtmatig moet zijn: er dient sprake te zijn van een duidelijk omschreven doel en een verwerkingsgrondslag zoals genoemd in artikel 6 AVG. Daarnaast dient er in geval van de verwerking van strafrechtelijke persoonsgegevens een uitzonderingsgrond te zijn op het algemene verwerkingsverbod.[12] De uAVG bepaalt dat die uitzonderingsgrond kan worden gevonden in een daartoe door de AP verleende vergunning. Private partijen die onderling strafrechtelijke gegevens willen uitwisselen, dienen daarvoor dus gezamenlijk een vergunning aan te vragen bij de AP. De AP kan deze vergunning slechts verlenen, indien de verwerking noodzakelijk is met het oog op een zwaarwegend belang en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.[13]

Bij elke verwerking van persoonsgegevens moet een aantal beginselen in acht worden genomen.[14] Zo dient de verwerking onder andere plaats te vinden op een wijze die rechtmatig, behoorlijk en transparant is. Daarnaast mogen de persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en vervolgens niet verder worden verwerkt op een manier die met die doeleinden onverenigbaar is (doelbinding). De persoonsgegevens die worden verwerkt moeten toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (dataminimalisatie). Ook moeten de persoonsgegevens juist zijn en zo nodig worden geactualiseerd, waarbij alle redelijke maatregelen moeten worden genomen om onjuiste persoonsgegevens onverwijld te wissen of te rectificeren. De persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkene niet langer te identificeren dan noodzakelijk is (opslagbeperking). Tot slot moeten de persoonsgegevens door het

[8] Voor de verwerking van bijzondere categorieën van persoonsgegevens gelden extra waarborgen, zo is in dit geval uitdrukkelijke toestemming nodig, zie art. 9 AVG
[9] Art. 7 AVG
[10] Art. 35 AVG
[11] Art. 36 AVG
[12] Brief van 11 juni 2019, zie: *Kamerstukken II*, 2018-2019, 17050, nr. 576
[13] Art. 33 uAVG
[14] Art. 5 AVG

nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is; de persoonsgegevens moeten onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (integriteit en vertrouwelijkheid).

3.3. Mededingingsregelgeving

De mededingingswet verbiedt kartels[15] (mededingingsbeperkende afspraken), misbruik van een economische machtspositie[16] en concentraties van ondernemingen[17] zonder voorafgaande melding.[18] Indien meerdere partijen gaan samenwerken, dienen zij te opereren binnen de geldende mededingingsregels. Indien partijen een gezamenlijk onderneming oprichten kan het zijn dat er sprake is van een concentratie in de zin van de Mededingingswet.[19] In dat geval dient hiervan melding te worden gedaan bij de ACM. De ACM zal dan beoordelen of door het oprichten van de gezamenlijke onderneming de mededinging niet onnodig beperkt of verhindert en of er sprake is van het gevaar van coördinatie van het marktgedrag door de moeders. Als er geen gezamenlijke onderneming tot stand komt, kan het zijn dat de samenwerking dient te worden getoetst aan het kartelverbod[20] en/of het verbod op misbruik van een economische machtspositie.[21] Indien een groot aantal partijen gaan samenwerken, kan deze samenwerking een dergelijke positie krijgen dat het nodig is dat ook andere partijen (op termijn) kunnen toereden. De eisen voor toetreding dienen open, transparant en niet-discriminatoir te zijn. Dat wil zeggen dat andere partijen onder redelijke voorwaarden kunnen aansluiten, indien zij dit wensen. Ook is het mogelijk dat de samenwerking leidt tot inkoopmacht bij de samenwerkende partijen. In dat geval mogen de samenwerkende partijen hier geen misbruik van maken door partijen uit te sluiten of onredelijke voorwaarden te hanteren.

4. Beschrijving onderzochte vormen van informatie-uitwisseling

In deze paragraaf worden de onderzochte vormen van informatie-uitwisseling toegelicht. De zes onderzochte vormen van informatie-uitwisseling zijn:

1. verbeteren van informatiedeling t.b.v. publiek-private samenwerking (PPS);
2. delen van informatie over cliënten (KYC Utility);
3. delen van informatie over transacties (TM Utility);
4. delen van informatie over ongebruikelijke klanten;
5. gebruik van het BSN-nummer en toegang tot de Basisregistratie Personen (BRP) en
6. toegang tot de afgesloten gegevens in het UBO-register.

Per vorm wordt beschreven wat deze inhoudt en welke (persoons)gegevens worden gedeeld. Ook wordt ingegaan op de vraag in hoeverre een bepaalde optie al mogelijk is, oftewel in hoeverre die informatie-uitwisseling al plaatsvindt. Daarnaast wordt toegelicht wat er eventueel nodig is om de informatie-uitwisseling te verbeteren of mogelijk te maken. Hierbij ga ik ook in op eventuele weg te nemen wettelijke belemmeringen. Tot slot geef ik een oordeel over proportionaliteit van de informatie-uitwisseling.

4.1. Verbetering publiek-private samenwerking (PPS)

Het hebben van kennis en expertise over witwassen is van groot belang voor poortwachters om een effectief en risicogebaseerd beleid te kunnen voeren en concreet te kunnen zoeken naar vermoedens van witwassen. Bij een aantal overheidsorganisaties is specifieke kennis aanwezig over witwassen. Het

---

[15] Art. 6 Mw
[16] Art. 24 Mw
[17] Artt. 27 en 34 Mw
[18] De Nederlandse mededingingsregels zijn nagenoeg gelijkluidend als de Europese mededingingsregels in het werkingsverdrag. Daarom wordt hier alleen ingegaan op relevante bepalingen in de Mw.
[19] Zie hiervoor ook https://www.acm.nl/nl/onderwerpen/concurrentie-en-marktwerking/concentraties-van-bedrijven/fusies-overnames-en-joint-ventures
[20] Zie hiervoor ook https://www.acm.nl/nl/onderwerpen/concurrentie-en-marktwerking/concurrentie-en-afspraken-tussen-bedrijven/kartelafspraken/kartels-herkennen
[21] Zie hiervoor ook https://www.acm.nl/nl/onderwerpen/concurrentie-en-marktwerking/concurrentie-en-afspraken-tussen-bedrijven/bedrijven-met-een-machtspositie/misbruik-van-een-machtspositie-herkennen

delen van deze informatie, al dan niet wederkerig, kan zeer waardevol zijn voor het vervullen van de poortwachtersfunctie. Binnen dit onderzoek ga ik in op drie vormen van informatie-deling binnen PPS. De eerste is het op operationeel niveau delen van informatie vanuit de opsporingsinstanties met private partijen uit de sector. De tweede is het geaggregeerd delen van informatie tussen publieke en private instanties. Dit betreft geen uitwisseling van persoonsgegevens, maar van fenomenen, typologieën en witwasmethoden. De derde is informatie die de FIU-Nederland deelt naar aanleiding van gedane meldingen.

4.1.1. Operationeel delen van informatie

a) Wat houdt het in?

Het operationeel delen van informatie betekent dat namen van concrete subjecten door opsporingsinstanties worden verstrekt aan poortwachters. Deze informatiedeling vindt plaats als er vermoedens of aanwijzingen zijn dat een (rechts)persoon betrokken is bij witwassen of terrorismefinanciering en maar voordat er sprake is van een redelijk vermoeden van schuld aan een strafbaar feit (verdenking). Op basis van de verstrekte informatie kunnen financiële dienstverleners hun systemen doorzoeken op transacties van die (rechts)persoon en die vervolgens melden bij de FIU-Nederland die deze informatie vervolgens terugkoppelt naar de opsporingsinstanties.

b) Is het al mogelijk?

Het delen van subjectgerelateerde informatie in het kader van voorkomen van terrorismefinanciering is reeds mogelijk binnen de zogenaamde TF Taskforce. Op dit moment wordt onderzoek gedaan binnen het Financieel Expertise Centrum (FEC) naar (de wenselijkheid van) het oprichten van een Serious Crime Task Force (SCTF) waarbinnen concrete subjectinformatie kan worden gedeeld in het kader van het voorkomen van witwassen. Voor het delen van subjectgerelateerde informatie met banken ter voorkoming en bestrijding van witwassen is een zogenaamd ‘artikel 20 Wet politiegegevens (Wpg) besluit’ nodig. Een dergelijk besluit kan alleen worden genomen binnen de kaders van de Wpg die onder andere voorschrijft dat het verstrekken van gegevens ten behoeve van samenwerkingsverbanden, zoals een samenwerkingsverband waar zowel opsporingsinstanties als banken aan deelnemen, alleen mogelijk is als dat vanuit een zwaarwegend algemeen belang noodzakelijk is ten behoeve van het voorkomen of opsporen van witwassen.

4.1.2. Geaggregeerd delen van informatie

a) Wat houdt het in?

Het geaggregeerd delen van informatie houdt in dat er fenomenen, typologieën, kennis en expertise worden gedeeld. Dit vindt reeds op verschillende manieren en via verschillende instanties plaats. Belangrijke instanties in dit verband zijn het FEC en het AMLC.[22] Het geaggregeerd delen van informatie gebeurt zowel publiek-publiek als publiek-privaat (PPS). Daarbij worden expertise en kennis uitgewisseld en data geanalyseerd ter verbetering van elkaars taken en verantwoordelijkheden ter voorkomen en bestrijden van witwassen. Verder worden er gezamenlijk projecten uitgevoerd m.b.t. specifieke onderwerpen en geconstateerde risico’s.

b) Is het al mogelijk?

Bij het delen van deze informatie is geen sprake van de verwerking van persoonsgegevens. Wettelijk zijn er geen belemmeringen om deze informatie te delen en is alleen opportuniteit vanuit toezichts- of opsporingsbelang relevant.

[22] Voor nadere informatie wordt verwezen naar de jaarplannen en jaarverslagen van het FEC en het AMLC, te raadplegen via de websites https://www.fec-partners.nl/nl en https://www.amlc.nl/managementrapportages-amlc/

4.1.3. Informatiedeling door de FIU n.a.v. gedane meldingen

a) Wat houdt het in?

Poortwachters melden ongebruikelijke transacties bij de FIU-Nederland. Hierdoor beschikt de FIU-Nederland over specifieke informatie op het terrein van witwassen. Deze informatie en de informatie die de FIU-Nederland zelf tot haar beschikking heeft, kunnen nuttige inzichten opleveren over het meldgedrag van instellingen en witwaspatronen. Deze inzichten kunnen behulpzaam zijn bij een effectieve invulling van de poortwachtersrol omdat het instellingen kan helpen bij het bepalen van hun risicogebaseerd beleid en de inrichting van de transactiemonitoring. De FIU-Nederland heeft in dat kader ook een specifieke taak, die wettelijk is vastgelegd in de Wwft. Zo heeft de FIU-Nederland tot taak om instellingen te informeren over trends en fenomenen die naar voren komen uit ontvangen meldingen. In dat kader heeft de FIU-Nederland contact (relatiebeheer) met verschillende meldersgroepen, zoals met banken en betaalinstellingen, maar ook met trustkantoren, taxateurs en notarissen. Naast informatie over typologieën en fenomenen, stelt de FIU-Nederland ook casuïstiek en relevante jurisprudentie ter beschikking. Een andere taak van de FIU-Nederland die expliciet in de Wwft is vastgelegd, is, door tussenkomst van het OM, het informeren over de betekenis van een melding voor de vervolging van strafbare feiten. Dit betekent dat de FIU-Nederland, indien mogelijk, de instelling die een transactie heeft gemeld informeert indien de FIU die melding verdacht heeft verklaard. Daar kan lange tijd overheen gaan, omdat de gemelde transactie pas verdacht wordt op grond van informatie die op een veel later moment bij de FIU bekend wordt. In andere gevallen kan het niet in het belang van de opsporing zijn om te delen dat een transactie verdacht is verklaard, bijvoorbeeld omdat dan een lopend strafrechtelijk onderzoek wordt doorkruist.

b) Is het al mogelijk?

De taken van de FIU-Nederland zijn wettelijk vastgelegd in de Wwft. Die vormen de vereiste wettelijke grondslag. De FIU-Nederland deelt ook veel informatie die geen persoonsgegevens bevat. Er bestaan geen wettelijke belemmeringen om deze informatie te delen. Als de FIU informatie terugkoppelt over een gemelde transactie is deze terugkoppeling beperkt tot de mededeling dat de transactie als verdacht is aangemerkt. Het verstrekken van meer informatie is niet mogelijk omdat dit de belangen van een lopend strafrechtelijk onderzoek doorkruist.

4.1.4. Proportionaliteit

Zowel publieke als private partijen hebben taken en verantwoordelijkheden bij het voorkomen en bestrijden van witwassen. Het delen van informatie is noodzakelijk om tot een optimale vervulling van ieders taken en zo het systeem als geheel te komen. Op die manier dient de informatiedeling ter versterking van de gezamenlijke aanpak van witwassen. Waar het geaggregeerde informatie betreft staat buiten kijf dat dit proportioneel is en zoveel als nuttig moet gebeuren. Voor het delen van subjectinformatie vormt de strafrechtelijke wetgeving het kader, waarbinnen een afweging gemaakt moet worden tussen belangen van betrokken en het zwaarwegend algemeen belang noodzakelijk is voor het voorkomen van witwassen.

4.2. Gezamenlijke KYC Utility

a) Wat houdt het in?

Ter vervulling van het cliëntenonderzoek en het volledig maken van cliëntdossiers werken de banken aan een KYC Utility. In de KYC Utility worden per bank cliëntendossiers gemaakt en bewaard. Elke bank besteedt hiertoe diens cliëntenonderzoek uit aan de Utility. De informatie van de verschillende banken wordt door middel van Chinese Walls separaat bewaard. De informatie van elke klant is feitelijk van aard en gebaseerd op informatie door de klant zelf aangeleverd of op informatie afkomstig uit andere bronnen. Om te zorgen dat de Utility namens elke bank dezelfde soort informatie vergaart, hebben de banken afspraken gemaakt (policy alignement). Het idee is dat in geval een cliënt een zakelijke relatie met een klant wil aangaan, gekeken wordt of binnen de Utility al een dossier van deze cliënt bestaat. Vervolgens wordt aan de cliënt toestemming gevraagd om deze informatie van een

andere bank te gebruiken. Na het verkrijgen van de feitelijke informatie is het aan de betrokken bank om een risicobeoordeling te maken. Deze maakt geen onderdeel uit van de informatie in de Utility. Een KYC Utility maakt het mogelijk dat er minder (vaak) informatie hoeft te worden aangeleverd en opgevraagd. Indien een cliënt toestemming heeft gegeven, kan de benodigde informatie uit de KYC Utility worden gehaald. De gegevens hoeven dan niet opnieuw te worden opgevraagd bij de cliënt of uit andere bronnen te worden verzameld. Het bevordert daarmee ook de volledigheid van cliëntdossiers en uniforme verzameling van gegevens van cliënten.

b) Is het al mogelijk?

De KYC Utility werkt op basis van toestemming door de klant. Dit is de verwerkingsgrondslag. Het beheer van de KYC Utility zal door middel van uitbesteding aan een derde worden verricht. Bij uitbesteding blijft een bank altijd zelf verantwoordelijk voor de uitvoering van de wettelijke verplichting. Aan deze uitbesteding staat geen nationale of internationale wetgeving in de weg. De KYC Utility moet voldoen aan de privacyregelgeving. Er zal een GEB moeten worden opgesteld. Afhankelijk van de beheersing van de risico's zal de AP moeten worden geraadpleegd. Bij een KYC Utility is sprake van een grote dataconcentratie, hetgeen hoge eisen stelt aan de in te stellen waarborgen en veiligheidseisen. Relevante factoren zijn onder andere het zorgen voor een duidelijke scheiding van informatie van de verschillende banken, de manier waarop toegang en autorisatie tot de informatie wordt geregeld en borging van het beginsel van dataminimalisatie. Op dit laatste punt is het van belang dat cliëntenonderzoek mede afhankelijk is van de dienst die of het product dat gevraagd wordt. Niet alle informatie ten behoeve van een ingewikkeld product hoeft relevant te zijn bij een eenvoudige dienst of product.

Indien meerdere partijen samenwerken bij realisatie van de KYC Utility is het mededingingsrechtelijke kader zoals geschetst in paragraaf 3.3 relevant. De KYC Utility dient transparant, open en niet discriminatoir te zijn. Andere partijen op de Nederlandse markt moeten onder redelijke voorwaarden kunnen aansluiten. Bij toetreding op termijn door andere partijen mogen geen hogere drempels bestaan, zoals het in rekening brengen van onevenredige kosten voor aansluiting bij de KYC Utility. Indien de samenwerking voor de KYC Utility leidt tot inkoopmacht mag hier geen misbruik van worden gemaakt. Daarnaast is van belang dat klantgegevens concurrentiegevoelig zijn. Deze gegevens kunnen bijvoorbeeld inzicht geven in de klantenopbouw en/of samenstelling van concurrenten. Voorkomen moet worden dat partijen toegang krijgen tot elkaars concurrentiegevoelige informatie. Hier dienen voldoende waarborgen voor te worden ingebouwd.

c) Proportionaliteit

Een KYC Utility draagt bij aan het gemak van cliënten en banken aangezien er minder gegevens hoeven te worden ingevuld en opgevraagd. Het kan daarnaast zorgen voor meer uniforme en volledige beoordeling van klanten door banken. De KYC Utility kan een bijdrage leveren aan de effectiviteit van het cliëntenonderzoek en het efficiënter inzetten van middelen zodat banken zich beter kunnen inzetten op de hoge risico's. De verwerking van persoonsgegevens is alleen aan de orde bij expliciete toestemming van de cliënt en acht ik daarmee proportioneel.

4.3. Gezamenlijke TM Utility

a) Wat houdt het in?

Ter verbetering van de transactiemonitoring willen de banken overgaan op gezamenlijke transactiemonitoring. Dit zou moeten plaatsvinden binnen een Transactie Monitoring Utility. In de TM Utility worden alle transacties van de banken gemonitord op ongebruikelijkheid. Het idee is dat door alle transacties te combineren resultaten naar boven komen die bij een controle bij een individuele bank niet zichtbaar zijn doordat criminelen hun transacties zodanig over instellingen verspreiden dat de ongebruikelijkheid van die transacties niet opvalt. Vanuit de Utility kunnen rechtstreeks (namens een instelling) ongebruikelijke transacties worden gemeld aan FIU-Nederland of de Utility kan de

meldingen eerst doorgeven aan de betrokken instelling die vervolgens zelfstandig meldt. Idee is dat elke meldingsplichtige instelling die dit wil aan de Utility kan deelnemen. Bij dit initiatief is sprake van verwerking van persoonsgegevens, namelijk in de vorm van de gegevens van de transacties. Bij de Utility zijn alleen private partijen betrokken. De controle van de transacties in de TM Utility moet door middel van uitbesteding door een derde worden verricht, waarbij de individuele banken zelf verantwoordelijk blijven voor een goede uitvoering van de monitoring.

b) Is het al mogelijk?

Voor de realisatie van een TM Utility staan wettelijke belemmeringen in de weg. Op grond van de Wwft is uitbesteding van de transactiemonitoring niet toegestaan. Dit betreft een puur nationaal voorschrift, internationale regelgeving verbiedt uitbesteding niet. Daarnaast is de vraag of voor het delen van transacties tussen banken een voldoende wettelijke grondslag bestaat. Binnen de TM Utility wordt informatie van verschillende banken bij elkaar gebracht en gecombineerd en worden transacties gedeeld. Omdat hierbij persoonsgegevens worden verwerkt, is een verwerkingsgrondslag nodig. De Wwft kent een algemene plicht voor instellingen om transacties te monitoren. Omdat het delen van transacties een nieuwe verwerking van persoonsgegevens is en omdat transacties gevoelige informatie bevatten, lijkt het verstandig om de grondslag voor transactiemonitoring uit te breiden met een expliciete grondslag om deze gegevens voor het vervullen van de transactiemonitoring te delen.

Daarnaast is van belang dat de realisatie van de TM Utility geschiedt in lijn met de geldende wettelijke kaders. Zo mogen enkel de transacties worden gedeeld en niet de gedane meldingen (i.v.m. tipping-off verbod). De Utility moet er dus in voorzien dat alleen de betrokken bank van een melding op de hoogte wordt gesteld. Daarnaast moet rekening gehouden worden met het privacykader. Net als bij de KYC Utility is er bij de TM Utility sprake van een grote dataconcentratie. Dit maakt het stellen van hoge eisen aan de waarborgen en veiligheid noodzakelijk. Daarnaast geldt dat de transacties enkel voor het voorkomen van witwassen en terrorismefinanciering mogen worden verzameld en vervolgens niet verder mogen worden verwerkt op een manier die met die doeleinden onverenigbaar is (doelbinding). Verder dient het beginsel van dataminimalisatie in acht te worden genomen. Alleen die persoonsgegevens mogen worden verwerkt die noodzakelijk zijn voor het voorkomen van witwassen of terrorismefinanciering. Tot slot geldt ook bij de TM Utility dat er een GEB moet worden opgesteld. Afhankelijk van de beheersing van de risico's zal de AP moeten worden geraadpleegd.

Indien meerdere partijen samenwerken bij realisatie van de TM Utility is het mededingingsrechtelijke kader zoals geschetst in paragraaf 3.3 relevant. De TM Utility dient transparant, open en niet discriminatoir te zijn. Andere partijen op de Nederlandse markt moeten onder redelijke voorwaarden kunnen aansluiten. Indien de samenwerking voor de TM Utility leidt tot inkoopmacht mag hier geen misbruik van worden gemaakt. Daarnaast is van belang dat betaalgegevens of gegevens over transacties concurrentiegevoelig zijn. Voorkomen moet worden dat partijen toegang krijgen tot elkaars concurrentiegevoelige informatie. Hier dienen voldoende waarborgen voor te worden ingebouwd.

c) Proportionaliteit

Gezamenlijke monitoring via een TM Utility kan informatie aan het licht brengen die nu niet bij de FIU bekend wordt. Dit betekent dat de effectiviteit van de poortwachtersfunctie substantieel kan worden verhoogd. Anders dan het delen van deze transacties is er geen andere mogelijkheid om dit doel te bereiken. Zolang de transacties binnen een gesloten systeem met adequate waarborgen worden gedeeld, lijkt de inbreuk op de privacy van betrokkenen relatief beperkt ten opzichte van de huidige transactiemonitoring. Alle transacties van cliënten worden immers bij de afzonderlijke banken al gecontroleerd.

4.4. Zwarte lijst met ongebruikelijke klanten

a) Wat houdt het in?

Banken willen elkaar kunnen informeren over klanten waarmee zij vanwege onbeheersbare integriteitrisico's de zakelijke relatie hebben beëindigd of die zij als klant hebben geweigerd. Deze registratie zou bij een meldpunt kunnen plaatsvinden of via een gezamenlijke lijst. In het kader van fraude hebben de banken samen met andere instellingen reeds een dergelijke lijst (Incidentenwaarschuwingssysteem Financiële Instellingen (IFI)).[23] Het systeem voor klanten met integriteitrisico's moet banken waarschuwen voor klanten die in verband met witwassen elders zijn geëxit. Bij aanvang van een zakelijke relatie is het vaak lastig om te beoordelen of een klant dusdanige risico's met zich brengt dat geen zakelijke relatie aangegaan kan worden. Informatie over klanten met integriteitrisico's moet banken helpen over volledige informatie te beschikken bij cliëntenonderzoek en zodoende voorkomen dat criminelen door middel van shoppen tussen instellingen misbruik kunnen maken van het financiële stelsel.

Naast het delen van namen, is het ook van belang dat de inhoudelijke informatie waarop de integriteitrisico's zijn gebaseerd, tussen banken gedeeld kan worden. Het delen van deze inhoudelijke informatie kan ondersteunend werken aan het aanleggen van een register met ongebruikelijke klanten en is onmisbaar voor een instelling om af te wegen of in het concrete geval een specifieke dienst of product kan worden verstrekt. Het biedt daarbij ook een waarborg dat niet op basis van beperkte informatie een cliënt wordt geweigerd.

b) Is het al mogelijk?

Voor het aanleggen van een zwarte lijst met namen van ongebruikelijke klanten gelden de regels voor zwarte lijsten van branches. Voor het delen van strafrechtelijke persoonsgegevens tussen private partijen geldt in beginsel een verwerkingsverbod. Er dient daarom sprake te zijn van een uitzonderingsgrond. In dit geval is dat een daartoe door de AP verleende vergunning. De banken beschikken hier op dit moment niet over. De AP kan een vergunning slechts verlenen, indien de verwerking noodzakelijk is met het oog op een zwaarwegend belang van de banken en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad. Het zwaarwegende belang kan worden onderbouwd aan de hand van de wettelijke taak van de banken die zij op grond van de Europese wetgeving hebben in hun rol als poortwachter. Ook het tegengaan van financieel-economische criminaliteit kan als een zwaarwegend belang worden aangemerkt. Bij het verlenen van een vergunning laat de AP onder meer de volgende omstandigheden een rol spelen[24]:

- de mate waarin opname van een individu in het systeem waarop de gegevensuitwisseling betrekking heeft, kan betekenen dat betrokkene wordt uitgesloten van bijvoorbeeld eerste levensbehoeften of van goederen of diensten die betrekking hebben op een (klassiek of sociaal) grondrecht;
- de kwetsbaarheid van bepaalde groepen betrokkenen, zoals klanten en werknemers die minderjarig zijn of oudere werknemers;
- de reikwijdte van het systeem, in termen van zowel degenen die het systeem kunnen vullen, degenen die gegevens in het systeem kunnen raadplegen en degenen van wie persoonsgegevens in het systeem worden verwerkt. Hoe groter de reikwijdte, hoe ingrijpender de gevolgen voor opname van de betrokkene in het systeem kunnen zijn. Naarmate de reikwijdte van een systeem groter is, zullen derhalve de waarborgen voor betrokkenen zwaarder moeten wegen of zal het systeem in het geheel niet door de toetsing komen. Het beperken van de reikwijdte van het systeem (geografisch, sectoraal of anderszins) kan bijdragen aan een positieve uitkomst van de proportionaliteitsafweging.

---

[23] https://www.nvb.nl/themas/veiligheid-fraude/incidentenwaarschuwings-systeem-financi%C3%ABle-instellingen/

[24] Brief van 1 april 2019, zie *Kamerstukken II,* 2018-2019, 32761, nr. 132

Voor het verlenen van een vergunning vraagt de AP een protocol voor de inrichting en werking van de lijst. De AP heeft een handleiding voor het opstellen van een dergelijk protocol. Daarnaast is bij het opstellen van een zwarte lijst altijd een GEB verplicht. De GEB behoort opgesteld te worden voor de aanvraag van de vergunning. Als ook de GEB aan de AP voorgelegd moet worden dan kan dit tezamen met de vergunningaanvraag.

Bij het delen van de inhoudelijke informatie waarop de integriteitrisico's zijn gebaseerd, is van belang dat er, vanwege het tipping-off verbod, geen informatie kan worden gedeeld tussen Wwft-instellingen over ongebruikelijke transacties of andere informatie die met FIU-Nederland is uitgewisseld. Het delen van informatie over risico's van cliënten is een verwerking van persoonsgegevens waarvoor een grondslag is vereist. De vraag is of de algemene wettelijke verplichting om (risicogebaseerd) cliëntenonderzoek te verrichten voldoende is voor deze verwerking. Omdat het delen van de informatie waarop de integriteitrisico's zijn gebaseerd een nieuwe verwerking van persoonsgegevens is en omdat deze informatie gevoelig is aangezien het gegevens van strafrechtelijke aard kan bevatten, lijkt het noodzakelijk een specifieke wettelijke grondslag hiervoor op te nemen in de Wwft. Deze kan analoog aan de Wet toezicht trustkantoren 2018 (Wtt 2018) worden ingericht. De Wtt 2018 bevat, als onderdeel van het cliëntenonderzoek, de verplichting om onderzoek te doen of de cliënt eerder elders om diensten heeft verzocht. Indien dit het geval is geweest en bij die andere instellingen integriteitrisico's zijn gebleken, moeten deze instellingen die informatie delen.

c) Proportionaliteit

Bij zwarte lijsten bestaan er in algemene zin risico's op stigmatisering en uitsluiting van dienstverlening (in dit geval unbankables). Bij (financiële) dienstverlening kan een zwarte lijst met hoog-risicoklanten en het delen van de inhoudelijke informatie waarop de integriteitrisico's zijn gebaseerd, een belangrijke bijdrage leveren aan het voorkomen van witwassen. De vraag is met het oog op de proportionaliteit of dit doel niet te bereiken is met minder vergaande maatregelen en hoe effectief het is. Banken kunnen in algemene zin al vragen naar eerdere dienstverlening bij andere instellingen. Een klant zal deze informatie indien deze kwaadwillend is ontkennend beantwoorden. De klant is waarschijnlijk niet herkenbaar als geweigerde klant omdat het voor de hand ligt dat hij zich onder een nieuwe bedrijfsnaam aanmeldt. Een zwarte lijst en het kunnen delen van de inhoudelijke informatie waarop de integriteitrisico's zijn gebaseerd, kan derhalve bijdragen aan de effectiviteit van het cliëntenonderzoek en bemoeilijkt het (ongezien) shoppen tussen instellingen. Daarbij richt de maatregel zich enkel op de gevallen met hoge risico's waarbij meer dan een redelijk vermoeden van witwassen bestaat. Het voorkomen van misbruik van het stelsel door gebruik te maken van verschillende instellingen lijkt niet met een minder vergaand middel te bereiken.

4.5. Toegang tot BRP (NAW-gegevens) en gebruik BSN

a) Wat houdt het in?

Met gebruik van het BSN als intern ordeningsmechanisme voor hun klantadministratie kunnen banken hun klanten eenvoudiger en accurater identificeren. Het BSN is daarvoor zeer bruikbaar, omdat het een uniek nummer is. Dat levert verschillende voordelen op. Zo is het bijvoorbeeld eenvoudiger om natuurlijke personen te herkennen en hun identiteit te verifiëren en accounts van dezelfde persoon te koppelen. In relatie daarmee willen de banken graag hun klanten kunnen controleren via de Basisregistratie personen (BRP), voorheen GBA. Dit is een overheidsregister waarin gegevens zijn opgenomen over inwoners van Nederland. Dit zijn gegevens zoals naam, geslacht en adres, maar ook gegevens over nationaliteit en huwelijk of geregistreerd partnerschap. De toegang tot het BRP wordt geregeld in de Wet BRP, onder verantwoordelijkheid van het ministerie van BZK. Naast overheidsinstanties, kunnen ook derde partijen onder strenge voorwaarden toegang krijgen tot het BRP.

b) Is het al mogelijk?

Voor het gebruik van het BSN als intern ordeningsmechanisme is een wettelijke grondslag nodig.[25] Wetgeving met betrekking tot unieke overheidsnummers moet voldoen aan de AVG/uAVG. Dat betekent onder meer dat het doel van het gebruik in de wet wordt vastgelegd.[26] Het moet gaan om een doel van algemeen belang waarvoor het gebruik van BSN noodzakelijk is. De AP heeft zich tot op heden in verschillende adviezen zeer kritisch uitgelaten over 'breed' gebruik van het BSN in de bancaire sector.[27] Zij hecht aan een beperkt doel. Ook de Raad van State is zeer kritisch.[28]

Banken hebben geen toegang tot de BRP. De wet BRP bepaalt dat derden bij amvb toegang kunnen krijgen tot de BRP ten behoeve van 'werkzaamheden met een gewichtig maatschappelijk belang'. Het mag alleen gaan om 'werkzaamheden […] die samenhangen met een overheidstaak'. Uit de toelichting blijkt dat vooral moet worden gedacht aan werkzaamheden die ook door de overheid zouden kunnen worden vervuld of in het verleden daadwerkelijk tot de taak van de overheid behoorden, maar zijn verzelfstandigd of geprivatiseerd. Dit geldt niet voor de verplichtingen van banken die zij op grond van de Europese wetgeving toebedeeld hebben gekregen voor hun rol als poortwachter.

Voor zowel het gebruik van het BSN als toegang tot het BRP geldt dat moet worden voldaan aan de gebruikelijke vereisten bij nieuwe verwerkingen van persoonsgegevens zoals het opstellen van een GEB. Afhankelijk van de beheersing van de risico's zal de AP moeten worden geraadpleegd.

c) Proportionaliteit

Banken hebben er op gewezen dat het voor hen makkelijker zou zijn (efficiencywinst) en dat zij door gebruik BSN/toegang BRP hun taken beter zouden kunnen uitvoeren omdat zij hun middelen effectiever kunnen inzetten voor het voorkomen van witwassen. Gezien de unieke identificerende informatie, speelt het vraagstuk van noodzakelijkheid en subsidiariteit nadrukkelijk. Het unieke karakter maakt het gebruik van deze informatie zeer effectief, maar maakt de inbreuk op de bescherming van de persoonsgegevens ook groter. De vraag is daarbij of er andere manieren zijn om hetzelfde doel te bereiken met een minder vergaande inbreuk op de bescherming van persoonsgegevens.

4.6. Toegang UBO register

a) Wat houdt het in?

Met name banken, maar ook andere Wwft-instellingen, hebben verzocht om toegang tot de afgesloten gegevens van UBO's in het UBO-register voor vennootschappen en andere juridische entiteiten. De banken hebben te allen tijde al toegang tot de openbare gegevens: naam, geboortemaand/jaar, woonstaat, nationaliteit en aard en omvang van het belang van een UBO. De afgesloten gegevens betreffen BSN/buitenlands fiscaal nummer, geboortedag/plaats, woonadres en afschriften ID en onderbouwing aard en omvang van het gehouden economisch belang. Deze laatste gegevens zijn alleen toegankelijk voor de FIU en bevoegde autoriteiten (toezichthouders en opsporingsinstanties). Met volledige toegang kan een bank direct beschikken over alle informatie van de UBO's van een juridische entiteit. Deze informatie hoeft zij daarmee niet meer op te vragen bij de cliënt. Dit kan voordelen opleveren bij het vergaren van de informatie en het identificeren van de UBO's. Doordat dit proces waarschijnlijk sneller en efficiënter gaat, kunnen de banken hun capaciteit meer inzetten op cliënten met hogere risico's.

---

[25] Artikel 87 AVG juncto artikel 46 UAVG

[26] Artikel 6, derde lid, AVG. Dat verder bepaalt: Deze wetgeving moet beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde gerechtvaardigde doel. Artikel 46, eerste lid, UAVG stelt "Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de desbetreffende wet dan wel voor doeleinden bij de wet bepaald."

[27] Zie het advies van de AP over het gebruik van BSN voor uitvoering depositogarantiestelsel, dd 11 april 2018: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_gebruik_bsn_depositogarantiestelsel.pdf

[28] *Kamerstukken II*, 2005-2006, 30312, nr. 4

b) Is het al mogelijk?

Het wetsvoorstel voor het UBO-register is op dit moment aanhangig bij de Tweede Kamer.[29] In dit wetsvoorstel is toegang tot de afgesloten gegevens voorbehouden voor bevoegde autoriteiten. Toegang voor instellingen tot de afgesloten gegevens van UBO's vraagt dus een aanpassing van het wetsvoorstel. Het wetsvoorstel volgt de richtlijn met betrekking tot de openbaar toegankelijke gegevens van een UBO. De (gewijzigde) vierde anti-witwasrichtlijn laat de mogelijkheid open om meer gegevens van UBO's te registreren. Toegang tot deze aanvullende gegevens moet overeenkomstig de regels inzake gegevensbescherming zijn.[30] Daarnaast is wellicht een nieuw advies nodig van de AP op dit punt. Tot slot vraag dit om aanpassing van de bouw van het register, die op dit moment gerealiseerd wordt.

c) Proportionaliteit

Bij het uitvoeren van hun cliëntenonderzoek moeten meldingsplichtige instellingen de UBO van de cliënt vaststellen. Het UBO-register kan hierbij behulpzaam zijn. De richtlijn eist dat instellingen zich voor hun cliëntenonderzoek niet alleen op de informatie in het UBO-register mogen verlaten.[31] Voor een goede vervulling van de poortwachtersfunctie is immers onafhankelijk cliëntenonderzoek van cruciaal belang en de informatie in het register is juist opgegeven door de cliënt. Omdat de gegevens in het UBO-register geen authentieke gegevens zijn, is het inhoudelijk ook niet wenselijk dat meldingsplichtige instellingen zich enkel op het register baseren. Daarnaast is van belang dat voor een zo hoog mogelijke kwaliteit van het register een terugmeldmechanisme is geregeld: als een instelling in haar onderzoek discrepanties met het UBO-register ontdekt dan is zij verplicht deze te melden. Dit moet ervoor zorgen dat het register zo actueel en accuraat mogelijk is. Onafhankelijk eigen onderzoek moet daarom altijd gewaarborgd zijn.

Met betrekking tot de noodzakelijkheid van toegang tot de aanvullende gegevens is van belang dat vennootschappen en andere juridische entiteiten verplicht zijn om toereikende, accurate en actuele informatie over hun UBO's bij te houden.[32] Wwft-instellingen kunnen deze informatie in het kader van hun cliëntrelatie opvragen. Dit is relevant in verband met het vraagstuk van subsidiariteit.

5. <u>Goede voorbeelden andere landen</u>

In het kader van het onderzoek is ook gekeken naar relevante voorbeelden van informatie-uitwisseling in andere landen ten behoeve van het voorkomen van witwassen. Hierbij is gekeken naar het Verenigd Koninkrijk (VK), de Verenigde Staten (VS), Australië, Singapore, Hongkong, Canada en Mexico. In het algemeen geldt dat er grofweg twee vormen van informatie-uitwisseling plaatsvinden, namelijk het operationeel delen van informatie en geaggregeerd delen van informatie. Hierin zijn de volgende vier vormen te onderscheiden:

- Geaggregeerd delen van informatie: formuleren van typologieën en risico's;
- Operationeel delen van informatie vanuit de opsporing;
- Uitwisseling van medewerkers en real-time informatie-uitwisseling
- gezamenlijke transactiemonitoring en/of cliëntenonderzoek;
- waarschuwen van andere instellingen bij geconstateerde integriteitrisico's;

Per land wordt hieronder kort ingegaan op de verschillende vormen van informatie-uitwisseling die daar voorkomen.

[29] Kamerstukken II 2018/19, 35179
[30] Artikel 30, vijfde lid, gewijzigde vierde anti-witwasrichtlijn
[31] Artikel 30, achtste lid, gewijzigde vierde anti-witwasrichtlijn
[32] Artikel 10b Wwft dat met de Implementatiewet registratie uiteindelijke belanghebbenden van vennootschappen en andere juridische entiteiten wordt ingevoegd

5.1. Verenigd Koninkrijk: JMLIT

JMLIT is een publiek-privaat samenwerkingsverband dat bestaat uit een overkoepelend orgaan, met daaronder een operationele groep, meerdere expertwerkgroepen van deskundigen en een ‘alert service’ dat verantwoordelijk is voor de verspreiding van de door JMLIT vastgestelde typologieën. Een raad van bestuur houdt toezicht op de activiteiten van JMLIT en rapporteert aan het ‘Financial Sector Forum’ dat een dialoog tot stand brengt tussen de financiële sector, het Openbaar Ministerie en de toezichthouder op de financiële markten.

De operationele groep bestaat uit vertegenwoordigers van de sector, opsporingsautoriteiten en de financiële toezichthouder. Binnen deze groep wordt informatie op operationeel niveau gedeeld. Dit betreft informatiedeling rondom specifieke opsporingszaken. De expertgroepen bestaan uit diverse vertegenwoordigers uit de sector en onafhankelijke onderzoekers. De expertgroepen identificeren en beoordelen nieuwe en opkomende witwasbedreigingen en delen kennis over typologieën en 'red flags'. Daarnaast trachten de expertgroepen kwetsbaarheden in het anti-witwassysteem te identificeren. Tot slot kunnen de expertgroepen behulpzaam zijn bij het bepalen van de lange termijnrichting van de operationele groep.

5.2. Verenigde Staten: Contextual Briefings

De Verenigde Staten kennen twee initiatieven op het gebied van PPS. Het eerste initiatief betreft het op operationeel niveau delen van informatie. Opsporingsautoriteiten kunnen via FinCEN, dat is de Amerikaanse FIU, bij financiële instellingen een verzoek om informatie indienen. Deze verzoeken betreffen namen van relevante (rechts)personen. De financiële instellingen moeten hun data binnen twee weken doorzoeken op matches. De verzoeken om informatie vanuit de opsporing kunnen door de FinCEN worden uitgebreid met casusspecifieke contextinformatie (contextuele briefings). Voor de briefing worden instellingen uitgenodigd waarvan FinCEN verwacht dat zij relevante informatie hebben. Dit is flexibel en kan per briefing verschillen. De contextuele briefings kunnen tevens worden benut om typologieën te formuleren die kenmerkend zijn voor die zaak. Het betreft een vorm van PPS die flexibel is en wordt ingericht als reactie op specifieke opsporingszaken. Ten tweede kent de VS een vrijwillig programma waarbij financiële instellingen onderling informatie met elkaar kunnen delen om witwassen of terrorismefinanciering te detecteren. Dit programma staat nog in de kinderschoenen.

5.3. Australië: Fintel Alliance

De Fintel Alliance maakt onderdeel uit van AUSTRAC, de Australische FIU. Het betreft een publiek-privaat samenwerkingsverband tussen autoriteiten en de belangrijkste meldingsplichtige instellingen. De Fintel Alliance bestaat uit een ‘Operations Hub’ en een ‘Innovation Hub’. De Operations Hub is een samenwerkingsverband waarbij partijen uit de sector, de FIU en andere analisten van de overheid op één plek gezamenlijk werken aan opsporingsonderzoeken. De data wordt real-time uitgewisseld. De Innovation Hub heeft als doel om de sector in een veranderende omgeving in staat te stellen om innovatieve business modellen te testen en nieuwe AML/CFT controlesystemen te ontwerpen. Partners van de Fintel Alliance zijn onder andere AUSTRAC, zes banken, betaaldienstverleners en meerdere opsporingsautoriteiten. Het is ook mogelijk dat internationale opsporingsautoriteiten zich aansluiten bij de ‘Operations Hub’.

Medewerkers van de verschillende organisaties die deel uitmaken van de Fintel Alliance werken gezamenlijk, waarbij medewerkers die afkomstig zijn uit de sector officieel worden gedetacheerd bij de FIU (nadat zij zijn gescreend). Het verzenden en ontvangen van informatie door de Fintel Alliance partners geschiedt altijd via AUSTRAC. Details van de afspraken voor informatiedeling zijn vastgelegd in een protocol. Het protocol bepaalt dat informatie die wordt gedeeld met Fintel Alliance-partners niet verder mag worden verspreid zonder voorafgaande toestemming van AUSTRAC of zonder dat dit wettelijk vereist is. Privaat-private uitwisseling van informatie is in Australië wettelijk niet toegestaan.

5.4. Singapore: ACIP

De stuurgroep van de ACIP wordt gevormd door de Commercial Affaires Department (CAD, een onderdeel van de politie) en Monetary Authority of Singapore (MAS, dat is de financiële toezichthouder), acht banken en de Vereniging van Banken in Singapore. Deze stuurgroep identificeert en prioriteert de belangrijkste risico's op witwassen en terrrorismefinanciering, en besluit op welke risico's de ACIP zich moet concentreren. Werkgroepen (waar ook externe partijen aan kunnen deelnemen) bestuderen deze risico's verder. De werkgroepen bestaan uit een aantal leden van de stuurgroep en andere relevante vertegenwoordigers uit de sector. ACIP richt zich op het formuleren van typologieën en deelt geen informatie op operationeel niveau. De focus van de werkgroepen ligt op het ontwikkelen van typologieën voor speciale doelgroepen/aandachtsgebieden en op het delen van best practices.

5.5. Hongkong: FMLIT

De FMLIT lijkt zeer sterk op het JMLIT model van de UK, en valt onder verantwoordelijkheid van de Hongkongse politie en de financiële toezichthouder. Financiële analisten van banken nemen samen met opsporingsambtenaren deel aan operationele bijeenkomsten in een beveiligde omgeving. Indien die bijeenkomsten nieuwe informatie opleveren wordt die via beveiligde kanalen verzonden naar de operationele groepsleden van de FMLIT. Een ander onderdeel van de FMLIT is de 'alert service'. Dit een platform voor het ontwikkelen van 'red flags' en typologieën die voortkomen uit evidence-based onderzoek door de expertgroep. Deze red flags en typologieën worden gedeeld naar andere banken met een vergunning in Hongkong.

5.6. Canada

In Canada is het operationeel delen van informatie in PPS-samenwerkingen met meerdere partijen verboden. Initiatieven voor het delen van typologieën bestaan wel. De focus van FINTRAC (de Canadese FIU) is om ervoor te zorgen dat het AML/CFT toezicht in lijn is met en ondersteunend is bij de prioriteiten van de opsporingsautoriteiten. In dat kader hebben enkele concrete projecten plaatsgevonden. Een voorbeeld is de oprichting van een forum voor de grootste (belangrijkste) melders van verdachte transacties. Dit was samenwerking tussen FINTRAC en de vijf grootste banken. Deze partijen komen ten minste elk half jaar bijeen, waarbij publieke autoriteiten informatie delen over financiële criminaliteit en over trends die zij waarnemen. Dit is ter ondersteuning van de banken die de mogelijkheid krijgen om witwassen beter de detecteren. Daarnaast werd een specifiek samenwerkingsverband opgericht dat indicatoren en typologieën van witwasrisico's in kaart brengt. Het samenwerkingsverband ontstond uit een samenwerking van de vijf grootbanken die werd uitgebreid tot andere meldingsplichtige instellingen (zoals betaaldienstverleners) en overige publieke instanties (zoals toezichthouders en opsporingsautoriteiten). Binnen het samenwerkingsverband beslissen de private partijen welke thema's en/of risico's voorrang krijgen.

5.7. Mexico

Mexicaanse banken kunnen informatie over cliënten en hun transacties delen met andere banken. Deze informatie mag alleen worden gedeeld voor anti-witwasdoeleinden. Een centrale database, die wordt beheerd door de centrale bank, bevat alle transacties uitgevoerd door Mexicaanse banken. Banken zijn verplicht om uit de database geaggregeerde informatie te verkrijgen over hoe de door hen uitgevoerde transacties zich verhouden tot het gehele systeem. Die informatie moet vervolgens worden meegenomen bij het uitvoeren van cliëntenonderzoek en het vaststellen van het risicoprofiel van cliënten. Cliënten moeten toestemming geven voor het toevoegen aan en verkrijgen van informatie uit de database. In een later stadium zullen banken ook verplicht worden tot het toevoegen van informatie van hun cliëntendossiers (CDD-informatie) aan de database, waarbij zij ook een check moeten uitvoeren of de informatie die de database bevat, correct is.

6. Conclusie onderzoek gegevensdeling

Zoals aangegeven in paragraaf twee wordt de rode lijn van dit onderzoek gevormd door de afweging van een effectievere vervulling van de poortwachtersrol ten opzichte van een inbreuk op de bescherming van persoonsgegevens van betrokkenen. In die afweging acht ik de eerste vier onderzochte vormen van informatie-uitwisseling in ieder geval proportioneel. Zij hebben een directe meerwaarde voor de effectiviteit van de poortwachtersrol en zijn niet via een andere, minder ingrijpende weg te bereiken. Dit betreft het verbeteren van publiek-private samenwerking (PPS), het delen van informatie over cliënten (KYC Utility), het delen van informatie over transacties (TM Utility) en het delen van informatie over ongebruikelijke klanten. De laatste twee vormen van informatiedeling zijn nu nog niet mogelijk omdat er wettelijke belemmeringen bestaan. Deze wettelijke belemmeringen zal ik samen met de minister van Justitie en Veiligheid gaan wegnemen. Met betrekking tot de TM Utility betekent dit een wettelijke grondslag voor het delen van transacties voor het monitoren van die transacties en dat uitbesteding van transactiemonitoring mogelijk wordt. Met betrekking tot het delen van informatie over ongebruikelijke klanten zal – analoog aan de Wtt 2018 – de wettelijke plicht in de Wwft worden opgenomen dat instellingen onderzoek moeten doen of de cliënt eerder elders om diensten heeft verzocht. Als dit het geval is geweest en bij die andere instellingen integriteitrisico's zijn gebleken, moeten deze instellingen die informatie delen.

Voor de vier bovengenoemde vormen geldt en blijft gelden dat bij de inrichting van de informatie-uitwisseling de wettelijke kaders uit de Wwft, de privacyregelgeving en de mededingingsregelgeving in acht moeten worden genomen. De concrete uitwerking binnen PPS of bij de banken onderling zal de toetssteen zijn of hieraan voldaan wordt.

Bij het algemeen gebruik van het BSN-nummer en toegang tot de gegevens in de Basisregistratie Personen (BRP) alsmede toegang tot het afgesloten gedeelte van het UBO-register, constateer ik dit ingrijpende zaken zijn, waarbij de proportionaliteits- en subsidiariteitsafweging zorgvuldig gemaakt moet worden. Om die reden zullen wij deze vormen van informatie-uitwisseling voor een formeel advies voorleggen aan de Autoriteit Persoonsgegevens.

In paragraaf vijf is een weergave gegeven van een aantal goede voorbeelden van informatiedeling in andere landen. Die zagen vooral op samenwerking in PPS-verband en in het bijzonder op het geaggregeerd delen van informatie. Uit paragraaf 4.2.1. blijkt dat er in Nederland op veel manieren geaggregeerd informatie wordt gedeeld. Binnen PPS worden typologieën, methoden, fenomenen, kennis en expertise uitgewisseld. Ook worden er concrete projecten gedraaid op basis van geconstateerde risico's. Op dit moment loopt er bovendien met de FIU en de Volksbank een pilot waarbij medewerkers van de FIU en de Volksbank op een gezamenlijke locatie direct samen werken en (real-time) informatie uitwisselen. Op dit moment worden er initiatieven ondernomen om de pilot te verduurzamen en te verbreden door aansluiting van andere banken.. Daarnaast waren er goede voorbeelden van het operationeel delen van informatie. In Nederland vindt er ter voorkoming van terrorismefinanciering reeds operationele informatiedeling plaats. Op dit moment wordt binnen het FEC onderzocht of het operationeel delen van informatie bij witwassen mogelijk is. Andere goede voorbeelden zagen op informatiedeling tussen private instellingen, zoals gezamenlijke uitvoering van het cliëntenonderzoek of monitoren van transacties en het onderling waarschuwen bij integriteitsrisico's. Met betrekking tot private informatiedeling zijn er reeds stappen ondernomen om te komen tot gezamenlijk cliëntenonderzoek. Op basis van de hiervoor aangekondigde maatregelen wordt het straks mogelijk om informatie over transacties te delen, alsmede om namen en onderliggende inhoudelijke onderbouwing van de integriteitrisico's van ongebruikelijke klanten te delen. Op basis hiervan kan worden geconcludeerd dat vrijwel al de in paragraaf 5 beschreven goede voorbeelden in Nederland reeds mogelijk zijn of binnen afzienbare tijd worden gerealiseerd. Met alle bovengenoemde maatregelen kunnen we concluderen dat Nederland in veel opzichten internationaal

voorop loopt. Ik zal uiteraard goede voorbeelden in andere landen in de gaten houden alsook de samenwerking en informatie-uitwisseling in Nederland bij andere landen als goed voorbeeld uitdragen.