Krachten gebundeld

Naar een effectievere en efficiëntere invulling van de poortwachtersrol in Nederland

KPMG Advisory N.V.

Amstelveen, 23 augustus 2023

143 pagina's

Inhoudsopgave (1)

Inhoudsopgave (2)

Management-samenvatting

Achtergrond

Het Nederlandse financiële stelsel kan door criminelen worden misbruikt om illegaal verkregen vermogen wit te wassen of om terrorisme te financieren. Om dit te voorkomen zijn in de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) maatregelen opgelegd aan financiële instellingen en professionele dienstverleners – de zogenaamde poortwachters. Poortwachters hebben daarnaast te maken met verplichtingen volgend uit de Sanctiewet 1977 (Sw) en vaak ook met specifieke wet- en regelgeving, of beroepsstandaarden. Sommige financiële instellingen, zoals schadeverzekeraars, vallen niet onder de Wwft maar worden wel geacht de Sw na te leven.

Met dit onderzoek is een verkenning verricht naar de kansen en mogelijkheden om door samenwerking van de verschillende groepen poortwachters, dan wel door het toepassen van creatieve andere werkwijzen, een verbetering van de efficiëntie en effectiviteit van de anti-witwasketen en de naleving van de Sw te realiseren.

Dit onderzoek is verricht in de periode van medio maart tot eind juni 2023 door KPMG Advisory N.V. (KPMG) op verzoek van de Nederlandse Vereniging van Banken (NVB), het Verbond van Verzekeraars, de Nederlandse Coöperatieve Vereniging van Makelaars en Taxateurs in onroerende goederen NVM U.A. (NVM), de Vereniging VBO – Vereniging van Makelaars & Taxateurs (VBO), de Koninklijke Notariële Beroepsorganisatie (KNB), Holland Quaestor (branchevereniging van trustkantoren), de Vereniging VNO-NCW (VNO-NCW) en de Koninklijke Vereniging MKB-Nederland (MKB-Nederland).

Poortwachters: een heterogene groep

Hoewel de doelstelling en verplichtingen op grond van de Wwft gelijk zijn voor alle poortwachters, betreft het een heterogene groep en zijn accentverschillen in ieders rol en verantwoordelijkheden te ontwaren. Instellingen en beroepsbeoefenaars zijn om verschillende redenen onder de reikwijdte van de Wwft gebracht. Zo zijn banken en trustkantoren aangemerkt als poortwachter vanwege het verlenen van toegang tot het betalingsverkeer en de Nederlandse economie, en is dat vanwege de specifieke juridische dienstverlening bijvoorbeeld het geval voor notarissen. Ook kunnen instellingen en beroepsbeoefenaars als poortwachter zijn aangemerkt vanwege het risico op misbruik voor witwasdoeleinden – te denken valt aan vastgoed of cash – of omdat zij op basis van de aard van hun dienstverlening in de gelegenheid zijn om indicaties van fraude en andere vormen van financieel-economische criminaliteit te signaleren. De relatie van poortwachters met hun klanten verschilt ook. Voor sommige poortwachters geldt dat zij lange, duurzame relaties hebben met hun klanten. Andere poortwachters – zoals makelaars – hebben daarentegen juist eenmalig of op ad-hoc basis contact met klanten.

Knelpunten in de uitvoering van de Wwft en de Sw

In de uitvoering van hun poortwachtersrol lopen poortwachters tegen verschillende knelpunten aan bij de naleving van de Wwft en de Sw. Sommige van deze knelpunten zijn te herleiden tot de fundamenten van het anti-witwasbeleid. In de eerste plaats bestaan er spanningen tussen de commerciële bestaansredenen van de poortwachters en de invulling van hun poortwachtersrol, soms nog aangevuld met maatschappelijke verwachtingen bij breed gedragen maatschappelijke ambities op het gebied van onder meer duurzaamheid, klimaat, milieu, gezondheid, mensenrechten en governance.

Voorts voelen poortwachters zich daarnaast op verschillende vlakken onvoldoende gesteund door de overheid, onder meer vanwege een gebrek aan duidelijke sturing en prioritering door de overheid, conflicterende wet- en regelgeving, een gebrek aan bevoegdheden in het licht van de uitdijende onderzoeksplicht, onzekerheid over de interpretatie van de risicogebaseerde benadering en de beperkte mogelijkheid om te leren door het gebrek aan een effectieve feedbackloop. Vooral het spanningsveld tussen de bescherming van privacy enerzijds en het effectief voorkomen van witwassen en terrorismefinanciering anderzijds, wordt als een grote beperkende factor ervaren. Dit spanningsveld heeft zich recentelijk op meerdere gebieden geuit: bij de toegang tot het UBO-register, bij de (on)mogelijkheden voor informatiedeling tussen poortwachters en publieke partijen en tussen poortwachters onderling, alsook bij verschillende wetgevingstrajecten zoals het Plan van aanpak witwassen en gegevensverwerking door samenwerkingsverbanden. Het ervaren gebrek aan ondersteuning kan frustratie opleveren bij poortwachters en is schadelijk voor hun motivatie scherp de poort te bewaken.

Tegelijkertijd lopen poortwachters het risico om zelf hard aangepakt te worden wanneer zij, naar de mening van diezelfde overheid, hun poortwachtersrol niet of niet voldoende vervullen. Dit betreft zowel bestuurs- of tuchtrechtelijke handhaving door de toezichthouders als de strafrechtelijke handhaving door het Openbaar Ministerie. Deze aanpak van poortwachters resulteert in een situatie dat poortwachters verkrampen en zich gedwongen voelen om meer te doen dan nodig, wat ook wel wordt aangemerkt wordt als het ‘rule-based’ invullen van risicogebaseerde normen of een ‘compliancegerichte’ naleving, om maar aan te kunnen tonen te hebben voldaan aan alle vereisten.

Klanten ervaren deze verkramping in toenemende mate in de vorm van verminderde toegang tot het financiële stelsel. Zo kunnen particulieren en bedrijven met hogere integriteitsrisico’s – bijvoorbeeld politiek prominente personen (PEP’s), verenigingen of stichtingen – te maken krijgen met een weigering of beperking van dienstverlening. Ook lopen klanten aan tegen langere doorlooptijden bij aanvang of uitbreiding van de dienstverlening en krijgen zij te maken met hogere kosten en met herhaalde (onnodige) uitvragen.

Een verkenning naar samenwerking en andere alternatieve werkwijzen

Desondanks zijn poortwachters steeds meer doordrongen van het belang van de poortwachtersrol en willen zij deze rol effectiever en efficiënter inrichten: voor zichzelf en voor hun klanten. Initiatieven in binnen- en buitenland laten zien dat bovengenoemde knelpunten (deels) op te lossen zijn door in te zetten op samenwerking en het gebruik van (nieuwe) technologieën. Ook centrale sturing door de overheid, waardoor de overheid meer met één stem spreekt, duidelijke keuzes maakt en prioriteert, kan bijdragen aan het verhogen van de effectiviteit en efficiëntie.

Onderlinge samenwerking poortwachters

Wat betreft samenwerking vallen de ontwikkeling van gezamenlijke voorzieningen door poortwachters, alsook de inzet op het gebied van publiek-private samenwerking op. Informatiedeling wordt gezien als een belangrijke hoeksteen voor een effectief anti-witwasbeleid.

Wereldwijd wordt met wisselend succes geëxperimenteerd met gezamenlijke voorzieningen op het gebied van transactiemonitoring, sanctiescreening en (aspecten van) het CDD-proces. De verschillende initiatieven betrokken in dit onderzoek laten zien dat gezamenlijke voorzieningen kunnen helpen bij het verkorten van de cliëntenonderzoeken en dat daarmee ook de kosten dalen. Beschikbare data wordt als het ware hergebruikt, geactualiseerd en verrijkt en dat betekent dat herhaalde uitvragen naar klanten niet meer nodig zijn. Met betrekking tot transactiemonitoring wordt wel gewezen op het feit dat met netwerkanalyses meer kan worden gezien – en dus gerichter ongebruikelijk en verdacht gedrag kan worden geïdentificeerd – dan een individuele poortwachter dit zou kunnen. Daarnaast wordt gewezen op de mogelijke verhoogde efficiëntie van het transactiemonitoringproces, de verlaging van kosten door het gezamenlijk ontwikkelen en onderhouden van utiliteiten, en verbeterd risicomanagement.

Uit dit onderzoek blijkt dat het opzetten en operationeel krijgen van een gezamenlijke voorziening geen sinecure is en dat daarbij verschillende aspecten goed moeten worden doordacht. Daarbij gaat het onder meer om de technologie, de deelnemers en governance, het type informatie en actualisatie, het type klanten, de functies van de voorziening (bijvoorbeeld dataverzameling en/of validatie van data), datastandaardisatie, privacy en overige zaken zoals intellectueel eigendom, mededinging en cybersecurity. Deze aspecten spelen een belangrijke rol en zijn ook (deels) van invloed op de mate van succes van initiatieven die in binnen- en buitenland ontplooid worden.

Bij private samenwerking kan het ook gaan om het gebruik van waarschuwingssystemen om de cliëntenonderzoeken van poortwachters effectiever te maken en het financiële systeem ‘schoon’ te houden. Een voorbeeld betreft het Incidentenwaarschuwingssysteem Financiële Instellingen. Dit systeem voor banken en verzekeraars toont aan dat informatie-uitwisseling tussen verschillende (afgebakende) private partijen met als doel het effectiever voorkomen en bestrijden van misbruik van het financieel stelsel – in dit geval fraude en misleiding – mogelijk is. Vanuit het oogpunt van privacy moet de informatie-uitwisseling proportioneel en subsidiair zijn en de opzet van het systeem voldoende waarborgen kennen.

Publiek-private samenwerking

In aanvulling op voorgaande is ook de publiek-private samenwerking (PPS) een belangrijk middel om de preventie van witwassen, terrorismefinanciering en de naleving van sanctieregelgeving effectiever te maken. De gedachte daarbij is dat financieel-economische criminaliteit beter kan worden voorkomen door samen te werken, en kennis en 'intelligence' te delen. In potentie kan PPS poortwachters helpen om hun interne processen zoals de transactiemonitoring te verbeteren en hun KYC/CDD-processen gerichter uit te voeren. Binnen de EU zijn PPS-verbanden in opmars hoewel de structuur, doelstellingen, deelnemers en het type informatie dat wordt uitgewisseld, verschillen. Publiek-private samenwerking vindt in Nederland zowel plaats op fenomeenbasis – zoals het delen van typologieën en trends – als op operationeel niveau ten aanzien van transacties, meldingen en/of (rechts)personen. Voorbeelden van PPS-initiatieven in Nederland zijn Fintell Alliance NL, de publiek-private samenwerking binnen het Financieel Expertise Centrum (FEC), het Anti-Money Laundering Centre (AMLC) en de PPS binnen het Landelijk Informatie- en Expertise Centrum (LIEC) en de Regionale Informatie- en Expertise Centra (RIEC's). Dit onderzoek toont dat publiek-private samenwerking op operationeel niveau vooral plaatsvindt met banken.

Uit dit onderzoek blijkt dat het creëren van een gelijkwaardige relatie tussen de publieke en private partners belangrijk is. Wederzijds vertrouwen, ervaren veiligheid, commitment, begrip en voldoende transparantie vormen een belangrijke basis voor een effectieve PPS. Dit geldt ook voor een evenredige inzet van mensen en middelen, een heldere (niet-complexe) governance en duidelijke vastlegging van doelen, partijen, en wederzijdse rollen en verantwoordelijkheden.

Digitale identiteit

Wat betreft het gebruik van technologie wordt in de context van KYC/CDD gewezen op de ontwikkeling en het gebruik van de digitale identiteit, ook wel e-ID genoemd. Dit is een digitale verantwoording waarmee de identiteit van een persoon kan worden gecontroleerd. Digitale identiteiten zijn op zichzelf geen nieuw fenomeen en worden al langer gebruikt, in het bijzonder door overheden.

Daarom zijn veel digitale identiteiten tot op heden ontwikkeld door en voor overheden zelf.

De identificatie en verificatie van de identiteit van klanten is een belangrijk onderdeel van het cliëntenonderzoek, waarbij digitale identiteiten en toepassingen een steeds grotere rol spelen. Het aangaan van zakelijke relaties op afstand, ook wel 'non-face-to-face' of 'remote onboarding' genoemd, vindt steeds vaker plaats en het gebruik van voldoende betrouwbare identificatiemiddelen in plaats van reguliere identificatiedocumenten, zoals paspoorten of rijbewijzen, is daarbij toegestaan. Steeds meer innovatieve technologieën worden ontwikkeld om het aangaan van zakelijke relaties op afstand te faciliteren. Daarbij kan gedacht worden aan het identificeren en verifiëren van de identiteit van klanten via videobellen, het digitaal ondertekenen van documenten of het gebruik van biometrische technologie.

De ontwikkeling van de Europese digitale identiteit met een portemonnee (wallet) voor zowel natuurlijke personen als rechtspersonen biedt kansen voor poortwachters om het cliëntenonderzoek en de voortdurende controle op de zakelijke relatie efficiënter te maken. Uit dit onderzoek komt naar voren dat zowel private als publieke partijen een belangrijke rol kunnen spelen bij de ontwikkeling en het gebruik van digitale identiteiten. Echter, om hierin te slagen is een ondersteunende overheid nodig, die de ontwikkeling van de digitale identiteit, en het gebruik daarvan, in het kader van de Wwft en Sw zowel technologisch als juridisch mogelijk maakt.

Centrale sturing

Voor een centrale sturing is het hebben van een strategie gebaseerd op een nationale risicobeoordeling belangrijk. Een goede strategie stelt kaders, geeft richting en stelt in staat om prioriteiten aan te brengen. Hoewel daar in Nederland voorzichtig stappen in zijn gezet met het Plan van aanpak witwassen uit 2019 en de Beleidsagenda aanpak witwassen uit 2022, blijkt uit dit onderzoek dat een duidelijke behoefte bestaat bij poortwachters aan een overheid die (meer) centraal aanstuurt, meer met één stem spreekt, duidelijke keuzes maakt en prioriteert. De Nederlandse national risk assessments (NRA's) witwassen en terrorismefinanciering kunnen versterkt worden met elementen uit NRA's uit het buitenland.

Voorts kan de Nederlandse overheid leren van de nationale strategieën zoals ontwikkeld in Canada, de Verenigde Staten (VS) en – in het bijzonder – het Verenigd Koninkrijk (VK). De strategieën van Canada en de VS zijn specifiek gericht op anti-witwasregelgeving, terwijl de strategie van het VK een holistische, integrale aanpak van economische criminaliteit bevat waarbij de bestrijding van witwassen een van de prioriteiten is. De strategie in het VK is veruit het meest gedetailleerd en kent de grootste betrokkenheid vanuit de private sector. Deze bevat concrete acties gericht op resultaten, alsook een duidelijke governance, planning en deadlines. Tot slot blijkt ook uit dit onderzoek dat Italië een voor Nederland interessant land is; daar kent men een sterk gecoördineerde sturing via een nationaal comité waar een grote en diverse groep overheidsorganisaties bij betrokken is. Hier wordt het belang getoond van een gezamenlijke taakstelling teneinde informatie met elkaar te kunnen delen.

Oplossingsrichtingen voor meer effectiviteit en efficiëntie

Uit dit onderzoek volgt dat er voor poortwachters verschillende manieren zijn om door samenwerking verbeteringen in effectiviteit en efficiëntie van de naleving van de Wwft en Sw te realiseren. De verkenning toont echter ook aan dat om de effectiviteit van het anti-witwasbeleid in zijn geheel te verhogen, de rol van de overheid cruciaal is. Dit ziet vooral op het ondersteunen van poortwachters, bijvoorbeeld via het wegnemen van (juridische) belemmeringen voor poortwachters en het inzetten op meer structurele samenwerking tussen poortwachters en publieke partijen, waardoor poortwachters beter hun rol kunnen pakken. Dit draagt naar verwachting ook bij aan de motivatie van poortwachters. Verder ziet dit voor de overheid op het pakken van de regie waarmee de overheid op hoofdlijnen centraal stuurt en prioriteert, waarmee een (nog) sterker fundament wordt gelegd voor een helder en gedragen beleid dat poortwachters in staat stelt om misbruik van het financiële stelsel door criminelen op effectieve en efficiënte wijze te bestrijden door witwassen en het financieren van terrorisme te voorkomen.

Uit dit onderzoek volgt een aantal geselecteerde oplossingsrichtingen die op kortere en langere termijn gerealiseerd kunnen worden om de naleving van de Wwft en Sw effectiever en efficiënter in te richten en die bijdragen aan het realiseren van een effectievere en efficiëntere anti-witwasaanpak. De complexiteit en impact van de oplossingsrichtingen verschillen. De oplossingsrichtingen zijn onderverdeeld in drie clusters:

1. Oplossingsrichtingen waarbij poortwachters primair aan zet zijn.
2. Oplossingsrichtingen waarbij poortwachters en overheid in gezamenlijkheid moeten optreden.
3. Oplossingsrichtingen waarbij de overheid aan zet is.

De volgende figuur zet de oplossingsrichtingen uiteen. Deze worden vervolgens nader toegelicht.

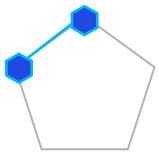
Poortwachters	Poortwachters en overheid	Overheid
• KYC-taxonomie • Waarschuwingssystemen • Gezamenlijke voorzieningen	• Versterking publiek-private samenwerking • Gebruik digitale identiteit (e-ID) in de context van het cliëntenonderzoek	• Ondersteunende overheid richting poortwachters: – Betrouwbare, publieke registers en een adequate ontsluiting naar poortwachters – Waardevolle feedbackloop – Regulering makelaarsberoep en een Wwft-registratieplicht voor niet-gereguleerde beroepen en instellingen – Bescherming poortwachters in het geval van angst voor represailles – Publieke voorlichting over de rol en verantwoordelijkheden van poortwachters • Pakken van eigenaarschap en sterkere centrale sturing: – Nationale coördinator – Versterking, verdieping en uitbreiding van de NRA – Prioriteren en vaststellen van een risk appetite voor Nederland

Tabel MS1: Overzicht oplossingsrichtingen

Poortwachters

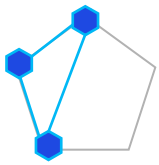
Uit dit onderzoek komen enkele kansen en mogelijkheden naar voren voor poortwachters om door samenwerking zelf al stappen te zetten om de efficiëntie en effectiviteit van de anti-witwasketen en de naleving van de Sw te verbeteren. In de basis is hier wederzijds vertrouwen en kennis over en weer voor nodig. Het is daarom belangrijk dat poortwachters zich (blijven) inzetten voor een (gedeeld) begrip van ieders specifieke rol en verantwoordelijkheden in de uitoefening van de gezamenlijke poortwachtersfunctie en kennis over de (aard van de) werkzaamheden van de verschillende poortwachters. Ook is het belangrijk om elkaar structureel op te zoeken om ontwikkelingen, trends en fenomenen te delen. Bovendien is het van belang dat poortwachters elkaar opzoeken en ondersteunen bij hulpvragen, gegeven de nuances in rollen, verantwoordelijkheden alsook de uiteenlopende expertise van de verschillende poortwachters.

KYC-taxonomie

Complexiteit	Impact
	

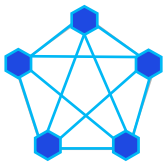
Een eerste oplossingsrichting voor poortwachters betreft het ontwikkelen van een gemeenschappelijke standaard op het gebied van KYC. De KYC-taxonomie betreft een gezamenlijke interpretatie van wettelijke vereisten, bijbehorende datapunten en onderliggende documentatie. Een gedeelde KYC-taxonomie zorgt ervoor dat poortwachters dezelfde informatie op een uniforme, dan wel geharmoniseerde, manier verzamelen. Zodoende biedt het poortwachters een opstap naar de mogelijkheid om bij te dragen aan een effectievere en efficiëntere informatiedeling, doordat zij hetzelfde begrip hebben van de informatie en zodoende 'dezelfde taal' spreken. Vanuit het perspectief van klanten biedt een gedeelde KYC-taxonomie duidelijkheid en voorspelbaarheid en kunnen herhaalde (onnodige) verzoeken voorkomen worden.

Waarschuwingssysteem

Complexiteit	Impact
	

Een tweede oplossingsrichting voor poortwachters betreft het opzetten van waarschuwingssystemen, voor zover niet reeds aanwezig zoals voor banken, verzekeraars en trustkantoren. Een waarschuwingssysteem is een systeem waarin gegevens zijn opgenomen van natuurlijke personen en/of rechtspersonen die een mogelijk risico vormen voor individuele poortwachters of voor de integriteit van het financiële stelsel, bijvoorbeeld in het geval van zware verdenkingen of bewezenverklaring van fraude of ander crimineel gedrag. Deze informatie wordt (onder bepaalde strikte voorwaarden) verstrekt en gebruikt door poortwachters. Meerdere partijen weten en zien meer dan één: informatiedeling stelt poortwachters in staat om risico's beter en sneller te onderkennen, te beperken en om de juiste mitigerende maatregelen te nemen.

Gezamenlijke voorzieningen

Complexiteit	Impact
	

Een derde oplossingsrichting voor poortwachters betreft het toewerken naar gezamenlijke voorzieningen. In aanvulling op de stappen die reeds door banken zijn gezet op het gebied van gezamenlijke transactiemonitoring en waar momenteel vooral actie aan de zijde van de overheid gewenst is met het verder brengen van het wetsvoorstel Wet plan van aanpak witwassen, kan het toewerken naar een gezamenlijke voorziening van verschillende categorieën poortwachters ten aanzien van (aspecten van) het CDD-proces een positieve bijdrage leveren aan de efficiënte en effectieve naleving van de Wwft/Sw.

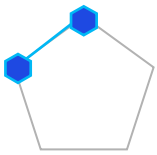
Initiatieven uit het buitenland laten zien welke aspecten poortwachters daarbij zouden moeten meenemen. Daarbij gaat het onder andere om de groep deelnemers, het type klanten, de gewenste functies van de utiliteit, het type informatie en actualisatie, de gewenste technologie voor het platform, de governance rondom de utiliteit en aspecten zoals privacy, mededinging en cybersecurity.

Op basis van inzichten verkregen in dit onderzoek, is het aan te raden om (een) gezamenlijke voorziening(en) klein te laten starten. Dat kan door de kring van deelnemers en de functies van de voorziening te beperken, bijvoorbeeld door deze te beperken tot het verzamelen van data en/of het valideren van deze data. Het verdient aanbeveling om de gezamenlijke voorziening juridisch zo simpel mogelijk te houden en deze in eerste instantie voor nationaal gebruik op te zetten.

Poortwachters en overheid

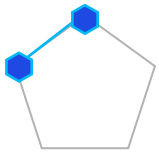
Uit dit onderzoek komen ook enkele andere kansen en mogelijkheden om de efficiëntie en effectiviteit van de anti-witwasketen en de naleving van de Sw te verbeteren, waarbij poortwachters en publieke partijen – weliswaar op basis van de eigen rollen en verantwoordelijkheden – gezamenlijk stappen moeten zetten.

Publiek-private samenwerking

Complexiteit	Impact
	

In de eerste plaats betreft dit het bestendigen en uitbreiden van een structurele publiek-private samenwerking. Gezien de overwegend positieve ervaringen van de operationele samenwerking tussen publieke partners en banken, verdient het aanbeveling om deze PPS te bestendigen en uit te breiden naar andere categorieën poortwachters. Poortwachters en overheid dienen hier gezamenlijk stappen in te zetten. Daarbij dient ervoor te worden gewaakt dat niet te veel verschillende vormen van PPS opgezet worden en dat concrete acties ondergeschikt raken aan overleg en besluitvorming. Voorts is het aan te raden om deze nieuwe PPS in eerste instantie via korte en concrete pilots op te starten en deze te evalueren om vervolgens tot een duurzame vorm van samenwerking te komen. Ook kan overwogen worden om andere categorieën poortwachters dan banken bij bestaande PPS-initiatieven aan te laten sluiten, zoals bij de Serious Crime Task Force (SCTF) binnen het FEC. Het creëren van een gelijkwaardige relatie tussen publieke en private partners is daarbij een belangrijk aandachtspunt, evenals een evenredige inzet van mensen en middelen en een heldere (niet-complexe) governance en duidelijke vastlegging. Om écht effectief samen te kunnen werken en impact te kunnen maken, is het van essentieel belang dat de overheid het (gericht) delen van informatie – zowel tussen de publieke partners onderling, tussen de private partners onderling, als tussen de publieke en private partners – juridisch mogelijk maakt.

Digitale identiteit

Complexiteit	Impact
	

In de tweede plaats betreft dit (het toewerken naar) het gebruik van digitale identiteiten in de context van het cliëntenonderzoek. Het gebruik van digitale identiteiten en authenticatiemiddelen biedt zowel poortwachters als klanten verschillende operationele efficiënties bij cliëntenonderzoeken. Poortwachters kunnen anticiperend op het digitale paspoort al gebruik (gaan) maken van digitale authenticatiemiddelen binnen de huidige juridische kaders van de Wwft/Sw. Poortwachters kunnen ook aan de hand van de ontwikkeling van de KYC-taxonomie bepalen voor welke datapunten en brondocumenten het wenselijk is om te koppelen aan de digitale identiteiten, en deze wensen delen met de overheid. Tot slot kunnen poortwachters de mogelijkheden voor aansluiting bij, of de ontwikkeling van, een centraal afsprakenstelsel ten behoeve van de naleving van de Wwft/Sw verkennen. De overheid dient de poortwachters op korte termijn te ondersteunen bij het verduidelijken van welke (aanbieders van) identificatiemiddelen voldoen aan het niveau ‘substantieel’ of ‘hoog’.

Vooralsnog wordt dit aan de individuele poortwachters zelf gelaten. Dit brengt de nodige onduidelijkheid en een aanzienlijke inspanning voor poortwachters met zich en het belemmert (in het bijzonder kleine) poortwachters om van dergelijke middelen gebruik te maken. Ook is het belangrijk dat de overheid werk maakt van een spoedige realisatie van het Europese digitaal paspoort en bijbehorende attributen, waarbij zij de wensen van de poortwachters meeneemt.

Overheid

Het moment lijkt aangebroken te zijn dat de overheid meer dan voorheen de poortwachters gaat motiveren om hun rol zo goed mogelijk te vervullen door hen duidelijkheid en ondersteuning 'aan de voorkant' te bieden. Terug naar de kern van het anti-witwasbeleid gaat het erom dat de overheid een duidelijke regierol pakt, waarmee zij (op hoofdlijnen) centraal stuurt en daarbij prioriteert op basis van de NRA.

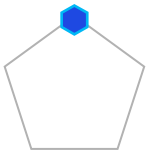
Ondersteunende overheid

Ondanks dat bestrijding van de criminaliteit een kerntaak is van de overheid, heeft de overheid binnen het anti-witwasbeleid een belangrijke rol aan poortwachters toebedeeld. Om tot een optimale invulling van de poortwachtersrol te komen, is het belangrijk dat poortwachters daartoe in staat worden gesteld, onder andere door hen het juiste instrumentarium en de benodigde duidelijkheid te bieden. Daartoe volgen uit dit onderzoek vijf aanbevelingen:

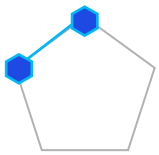
1 Maak werk van betrouwbare, publieke registers en zorg voor een adequate ontsluiting naar poortwachters

Als startpunt van relevante informatie en gegevens voor het cliëntenonderzoek is het belangrijk dat data uit publieke registers (zo) betrouwbaar (mogelijk) is. Om extra werk voor poortwachters te voorkomen, zouden zij in beginsel moeten kunnen vertrouwen op deze informatie. Hieronder vallen de volgende concrete acties:

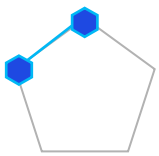
- Behoud de toegang tot het UBO-register voor poortwachters en alle instellingen die onder de RtSw 1977 vallen en geef aan hen ook toegang tot het afgesloten gedeelte van het UBO-register.

Complexiteit	Impact
	

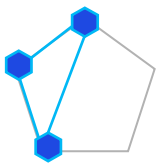
- Geef poortwachters toegang tot de BRP voor de uitvoering van hun cliëntenonderzoek.

Complexiteit	Impact
	

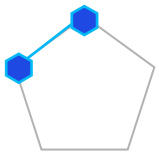
- Maak werk van lopende wetgevingsinitiatieven die poortwachters kunnen helpen effectiever en efficiënter aan hun Wwft-verplichtingen te voldoen, specifiek met betrekking tot het centraal aandeelhoudersregister en het mogelijk maken van het 'zoeken op naam' van personen in het Handelsregister.

Complexiteit	Impact
	

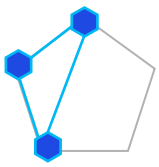
- Overweeg poortwachters verder te ondersteunen door registers te creëren waarvoor poortwachters momenteel veelal gebruik moeten maken van commerciële aanbieders, bijvoorbeeld ten aanzien van het creëren van een publiek PEP-register en het bijhouden van actuele sanctielijsten.

Complexiteit	Impact
	

- Overweeg sanctiechecks tegen publieke registers van overheidswege te verrichten en de onderzoeksinspanning voor bedrijven enigszins te verlichten, bijvoorbeeld door de Kamer van Koophandel de taak te geven sanctiechecks te verrichten op de informatie opgenomen in het UBO-register of Handelsregister.

Complexiteit	Impact
	

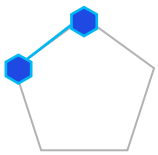
2 Creëer een waardevolle feedbackloop

Complexiteit	Impact
	

De roep om een effectieve feedbackloop vanuit de poortwachters bestaat mogelijk al zo lang als de meldplicht zelf bestaat. Geaggregeerde feedback wordt al gedeeld met poortwachters. Wat nog ontbreekt is een individuele terugkoppeling op het niveau van de meldende organisatie of de transactie waarop de melding betrekking heeft. Poortwachters kunnen hiervan leren en dit kan een positief effect hebben op de meldingsbereidheid en kwaliteit van meldingen.

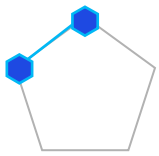
Een start voor het creëren van een waardevolle feedbackloop kan worden gemaakt door het op sectorniveau terugkoppelen van uitkomsten van gedane meldingen vanuit die sector over een bepaalde periode door FIU-NL, eventueel samen met de opsporing, binnen de huidige wettelijke kaders. Daarnaast zou toegewerkt moeten worden naar een terugkoppeling op individuele meldingen. Met betrekking tot verdacht verklaarde transacties is het waardevol voor poortwachters om (meer) inzicht te krijgen in het gebruik van de door hen gemelde verdachte transacties in het strafrechtelijke opsporingsproces. Opsporingsdiensten en het OM zouden daarom ten minste op een geaggregeerd niveau een terugkoppeling moeten (kunnen) geven, bijvoorbeeld in de vorm van statistieken en het delen van casuïstiek.

3 Reguleer het makelaarsberoep en overweeg een Wwft-registratieplicht in te voeren voor niet-gereguleerde beroepen en instellingen

Complexiteit	Impact
	

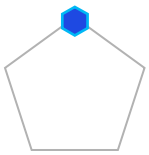
De vastgoedsector is kwetsbaar voor witwassen en dat het makelaarsberoep niet gereguleerd is, maakt de sector in potentie nog kwetsbaarder: er worden geen minimumkwaliteitseisen gesteld noch wordt er een verplichte aansluiting bij beroepsorganisaties vereist. Het is daardoor nagenoeg onmogelijk te achterhalen hoeveel makelaars daadwerkelijk actief zijn in Nederland, omdat niet alle makelaars aangesloten zijn bij een van de drie brancheverengingen (NVM, VBO en VastgoedPro). Dit gebrek aan afbakening heeft mogelijk ook impact op het toekennen van bevoegdheden. Gegeven het belang van de poortwachtersrol en daarbij een goede balans tussen taken en bevoegdheden, is het zinvol om regulering van het makelaarsberoep opnieuw te introduceren. Het is belangrijk om de lessen uit het verleden te betrekken bij de vormgeving van de regulering van het beroep. Regulering van het makelaarsberoep kan samengaan met het invoeren van een Wwft-registratieplicht voor niet-gereguleerde beroepen en instellingen. Ook kan regulering van het makelaarsberoep gepaard gaan met een heroverweging van de huidige Wwft-vereisten en -praktijk ten aanzien het cliëntenonderzoek op de wederpartij door makelaars.

4 Bescherm poortwachters in het geval van angst voor represailles bij het doen van meldingen van ongebruikelijke transacties

Complexiteit	Impact
	

Een knelpunt ervaren door poortwachters betreft de angst voor represailles bij het doen van meldingen van ongebruikelijke transacties bij FIU-NL. De nodige stappen zijn gezet en verschillende oplossingen worden verkend om (het gevoel van) veiligheid van melders te versterken, maar meer bescherming van poortwachters is noodzakelijk. Waar de poortwachters een door de overheid opgelegde plicht hebben om te melden, heeft de overheid de plicht om de melder te beschermen.

5 Geef publieke voorlichting over de rol en verantwoordelijkheden van poortwachters

Complexiteit	Impact
	

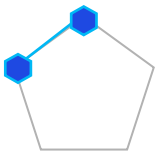
Om poortwachters in staat te stellen hun beperkte middelen daadwerkelijk in te zetten voor de vervulling van hun poortwachtersrol, zou de overheid meer publieke voorlichting moeten geven. Gedacht kan worden aan het bieden van een (digitale) plek waar voorlichting is te vinden voor klanten over de rollen en verplichtingen van poortwachters bij de naleving van de Wwft en de Sw, het opzetten van een campagne, en het inrichten van een vragen- en/of klachtenloket.

Centrale sturing

Het anti-witwasbeleid in Nederland laat zich kenmerken door een hoge mate van fragmentatie. Het is een op zichzelf staand beleidsterrein, maar valt binnen de bredere aanpak van georganiseerde criminaliteit. Dit maakt dat er veel verschillende overheidspartijen betrokken zijn, variërend van departementen, toezichthouders, gemeenten, FIU, overheidsdiensten en uitvoeringsorganisaties, opsporingsinstanties tot het OM. Een gebrek aan een centrale sturing, inclusief een duidelijke prioritering en belangenafweging, kan ertoe leiden dat de overheid geen duidelijke keuzes maakt en daardoor gaat dralen en verzanden in algemene toezeggingen. Met een eenduidige visie van de overheid waarbij de verschillende belangen van betrokken overheidspartijen al op voorhand afgewogen zijn en keuzes zijn gemaakt, kan dergelijke 'verlamming' worden voorkomen en tot actie worden overgegaan. Duidelijkheid draagt bij aan de motivatie van poortwachters, die met de gegeven sturing (nog) gericht(er) aan de slag kunnen gaan.

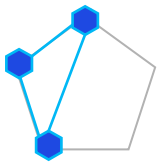
Concreet leidt dit tot drie aanbevelingen:

1 Wijs een nationale coördinator namens de overheid aan die de regie pakt in de nationale anti-witwasaanpak

Complexiteit	Impact
	

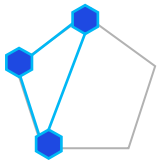
De coördinator acteert idealiter op de hoofdlijnen en treedt op als verbinder tussen de betrokken publieke partijen en hun belangen, als aanjager van een effectief en efficiënt anti-witwasbeleid, en is namens de overheid richting de private sector het gezicht of boegbeeld van deze nationale aanpak.

2 Versterk, verdiep en breid de nationale risk assessment uit

Complexiteit	Impact
	

Nationale risicobeoordelingen (National Risk Assessments, NRA's) zijn het fundament voor een nationale anti-witwasstrategie en de risicogebaseerde benadering in het anti-witwasbeleid. De Nederlandse overheid kan daarbij leren van NRA's uit het buitenland. Daarbij gaat het om de gebruikte analysemethoden en het betrekken van sectorale en geografische risico's in, of in aanvulling op, de NRA.

3 Prioriteer en stel een risk appetite voor Nederland vast

Complexiteit	Impact
	

Het is niet realistisch te stellen dat met een effectieve toepassing van het anti-witwasbeleid het witwassen compleet voorkomen kan worden. Het is evenmin realistisch om van poortwachters te verwachten dat zij hun poorten zodanig bewaken dat er helemaal geen crimineel geld het financiële systeem binnenkomt. Met prioriteitstelling in een nationale anti-witwasstrategie kan de inzet van poortwachters zich vooral richten op de belangrijkste nationale prioriteiten. Omdat niet alles een prioriteit kan zijn of kan blijven, betekent dit uiteraard ook dat de inzet op andere vlakken minder zal zijn. Het is daarom aan te raden dat de Nederlandse overheid met de NRA en bij de vaststelling van haar prioriteiten ook een nationale risk appetite vaststelt die samen met de gestelde prioriteiten als bandbreedte kan dienen voor de risicogebaseerde toepassing van het anti-witwasbeleid, en dus voor de poortwachters bij de uitoefening van hun rol.

Van oplossingsrichtingen naar actie

De mate waarin de oplossingsrichtingen gerealiseerd gaan worden en hun volle potentieel benut wordt, zal afhangen van de inzet en de commitment van poortwachters en de overheid. Voor de poortwachters is het zaak dat zij de concrete stappen binnen de mogelijkheden die zij daartoe hebben ook (durven) gaan zetten.

Voor de overheid is het belangrijk dat zij de poortwachters daartoe in staat stelt. Daarbij gaat het om het geven van bevoegdheden en het wegnemen van (juridische) onduidelijkheden of conflicten. In het licht van de verwachte impact is het toewerken naar sterke centrale sturing van wezenlijk belang. Centrale sturing vereist een heldere nationale anti-witwasaanpak neergelegd in een strategie die is gebaseerd op de daadwerkelijke risico's voor Nederland, en waarin duidelijke keuzes worden gemaakt ten aanzien van de prioriteiten bij de bestrijding van witwassen en terrorismefinanciering.

Veel oplossingsrichtingen worden geraakt door de huidige discussie rondom privacy. Daarom moet de hoogste prioriteit liggen bij het afwegen van het belang van privacy enerzijds, en het voorkomen van witwassen en terrorismefinanciering (en in het verlengde daarvan de bestrijding van criminaliteit) anderzijds.

Kortom, het is tijd om goede intenties om te zetten in concrete acties. Dit onderzoek heeft laten zien dat dat vooral kan door in te zetten op samenwerking en het gebruik van technologie. Dat kunnen poortwachters niet alleen. Dat kan de overheid niet alleen. Dat kan alleen met elkaar. Op basis van vertrouwen.

Inleiding

1.1 Aanleiding en relevantie

Het Nederlandse financiële stelsel kan door criminelen worden misbruikt om illegaal verkregen vermogen wit te wassen of om terrorisme te financieren. Om dit te voorkomen zijn in de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) maatregelen opgelegd aan financiële instellingen en professionele dienstverleners – de zogenaamde poortwachters. Deze poortwachters zijn verantwoordelijk voor het voorkomen dat hun dienstverlening wordt misbruikt door criminelen. Dit doen zij onder andere door het verrichten van een cliëntenonderzoek, het monitoren van de zakelijke relatie en het melden van ongebruikelijke transacties. Op grond van de Sanctiewet 1977 (Sanctiewet of Sw) is het natuurlijke en rechtspersonen verboden om aan gesanctioneerde personen of entiteiten geld of andere financiële middelen beschikbaar te stellen en, waar van toepassing, bepaalde (financiële) diensten aan te bieden. Hoewel de Sanctiewet een bredere reikwijdte heeft, hebben poortwachters ook hier een belangrijke maatschappelijke rol. Daarnaast zijn op verschillende poortwachters nog specifieke wetgeving en/of beroepsstandaarden van toepassing met aanvullende verplichtingen toegespitst op hun dienstverlening, zoals onder meer bij trustkantoren en het notariaat het geval is.

De diverse groepen poortwachters hebben hetzelfde doel, maar acteren op verschillende momenten in tijd en hebben soms ook te maken met verschillen in wet- en regelgeving. Poortwachters ervaren (mede) daarom verschillende knelpunten die een effectieve en efficiënte naleving van de Wwft en de Sw in de weg staan. Sommige van deze knelpunten zijn te herleiden tot de fundamenten van het anti-witwasbeleid. Met de toenemende maatschappelijke aandacht voor privacy wordt momenteel veel gesproken over de bescherming van de privacy in relatie tot de (groeiende) verplichtingen voor poortwachters bij het voorkomen van witwassen en terrorismefinanciering.

Het spanningsveld heeft zich recentelijk in meerdere vormen geuit: bij de toegang tot het UBO-register, bij mogelijkheden voor informatiedeling tussen poortwachters en publieke partijen en tussen poortwachters onderling, en bij verschillende wetgevingstrajecten zoals het Plan van aanpak witwassen en gegevensverwerking door samenwerkingsverbanden. Andere knelpunten zijn mogelijk op te lossen door samenwerking of door het toepassen van creatieve andere werkwijzen. In dit onderzoek wordt verkend welke mogelijkheden daartoe bestaan met een blik 'over de sectoren' heen. Hoewel het onderzoek zich richt op de situatie in Nederland, worden met de verkenning ook relevante initiatieven uit het buitenland betrokken. De gepresenteerde oplossingsrichtingen zijn voor een bredere groep poortwachters en voor de overheid relevant.

Dit onderzoek is door KPMG Advisory N.V. (KPMG) verricht op verzoek van een groep van acht branche- en beroepsorganisaties in de periode van medio maart tot eind juni 2023.(1)

Betrokken groepen poortwachters zijn banken, levens- en schadeverzekeraars, makelaars, notarissen en trustkantoren. Het onderzoek is vanuit de opdrachtgevers gecoördineerd door MKB-Nederland en VNO-NCW.

1.2 Onderzoeksvragen

Dit onderzoek heeft tot doel een verkenning te verrichten naar kansen en mogelijkheden om door samenwerking van de verschillende groepen poortwachters, dan wel door het toepassen van creatieve andere werkwijzen, een verbetering van de efficiëntie en effectiviteit van de anti-witwasketen en de naleving van de Sanctiewet te realiseren.

(1) De betrokken organisaties zijn: Nederlandse Vereniging van Banken (NVB), Verbond van Verzekeraars, Nederlandse Coöperatieve Vereniging van Makelaars en Taxateurs in onroerende goederen NVM U.A. (NVM), Vereniging VBO - Vereniging van Makelaars & Taxateurs (VBO), Koninklijke Notariële Beroepsorganisatie (KNB), Holland Quaestor, Vereniging VNO-NCW (VNO-NCW) en Koninklijke Vereniging MKB-Nederland (MKB-Nederland). Het onderzoek is inhoudelijk op 27 juni 2023 afgesloten.

Het onderzoeksdoel wordt beantwoord aan de hand van de volgende deelvragen:

1. Wat zijn de rollen en verantwoordelijkheden van iedere individuele poortwachter?
2. Welke knelpunten zijn er om taken vanuit die rollen en verantwoordelijkheden uit te voeren?
3. Kan samenwerking met andere poortwachters dan wel een alternatief werkproces die knelpunten wegnemen?
    - Dragen samenwerking en de alternatieve werkwijzen bij aan het effectief en efficiënt voldoen aan de Wwft-verplichtingen?
    - Dragen samenwerking en de alternatieve werkwijzen bij aan het effectief en efficiënt naleven van de Sanctiewet?
    - Wat belet die samenwerking(en)?
4. Zijn er internationale alternatieven die leiden tot efficiëntere en/of effectievere werkprocessen?
5. Welke stappen kunnen worden gezet om verbeteringen te realiseren?

Leeswijzer

Dit rapport is als volgt opgebouwd.

Hoofdstuk 2 geeft inzicht in de rollen en verantwoordelijkheden van verschillende poortwachters.

Hoofdstuk 3 gaat over de uitvoeringspraktijk en knelpunten die daarbij worden ervaren.

Hoofdstuk 4 bevat relevante (internationale) voorbeelden op het gebied van samenwerking en alternatieve werkwijzen van poortwachters die van belang (kunnen) zijn voor de Nederlandse praktijk en het vraagstuk van effectieve en efficiënte naleving van de Wwft en Sw.

Hoofdstuk 5 beschrijft de oplossingsrichtingen en concrete stappen die daarbij kunnen worden gezet om via samenwerking en alternatieve werkwijzen een effectievere en efficiëntere naleving van de Wwft en Sw te realiseren.

1.3 Doel en beperking verspreidingskring rapportage

Dit document is uitsluitend bestemd voor het aan opdrachtgevers kenbaar maken van de, in het kader van de aan KPMG verstrekte opdracht, tot nu toe verrichte werkzaamheden, daaruit voortvloeiende inzichten en het afstemmen van deze inzichten ten behoeve van de verdere uitwerking van het onderzoek.

Zonder onze uitdrukkelijke en voorafgaande schriftelijke toestemming is het niet toegestaan deze rapportage dan wel delen daarvan, te gebruiken voor andere doeleinden, daaraan te refereren, openbaar te maken en/of aan derden te verstrekken.

1.4 Afbakening onderzoek

Voor dit onderzoek worden de concepten van effectiviteit en efficiëntie toegelicht, alsook de reikwijdte van het onderzoek.

Effectiviteit en efficiëntie

In de onderzoeksvraag wordt een onderscheid gemaakt tussen effectiviteit en efficiëntie van de naleving van de Wwft en Sw.

- Effectieve naleving gaat over het *doel dat de wet- en regelgeving beoogt te bereiken*. Met andere woorden: is de betreffende wetgeving doeltreffend in het voorkomen van witwassen, terrorismefinanciering en het voorkomen van schendingen van sanctiemaatregelen? Dit betreft de effectiviteit op het metaniveau, omdat het gaat over het grotere vraagstuk of het anti-witwassysteem zoals we dat momenteel kennen op basis van de Wwft en Sw daadwerkelijk bijdraagt aan – kortweg – minder financieel-economische criminaliteit.
    - Effectieve naleving gaat ook gerichter over de vraag of binnen dit beleid of systeem aan de *wettelijke vereisten wordt voldaan*; in dit onderzoek de normen op grond van de Wwft en Sw die op poortwachters van toepassing zijn.

- **Efficiënte** naleving gaat over de *doelmatigheid van het voldoen aan de huidige wettelijke verplichtingen*. Daarbij gaat het om de vraag of er manieren zijn om met minder middelen en inspanningen aan de wettelijke vereisten te voldoen.

Focus op Nederland

Het anti-witwasbeleid en de sanctieregelgeving betreffen (vooralsnog) nationale wet- en regelgeving.(2) In dit onderzoek worden buitenlandse initiatieven betrokken en geanalyseerd.

In het licht van de onderzoeksvraag en deelvragen beperken de oplossingsrichtingen zich tot Nederland.

1.5 Onderzoeksmethodiek

Dit onderzoek is tot stand gekomen door een combinatie van verschillende onderzoeksmethoden.

Een literatuurstudie vormt de basis voor de analyse van knelpunten en kansen, en mogelijkheden voor een effectievere en efficiëntere naleving van de relevante wetgeving. De literatuurstudie leidt tot een eerste inventarisatie van knelpunten die poortwachters en klanten ervaren, factoren die deze knelpunten weg kunnen nemen en mogelijke overige oplossingsrichtingen om verbeteringen in effectiviteit en efficiëntie te realiseren.

Met de vertegenwoordigers van de bij dit onderzoek betrokken branche- en beroepsorganisaties, enkele Wwft-toezichthouders, Financial Intelligence Unit Nederland (FIU-NL), het Openbaar Ministerie (OM), alsook enkele experts uit de wetenschap en praktijk zijn kwalitatieve, semigestructureerde interviews gehouden om inzichten uit het literatuuronderzoek te verifiëren en om aanvullende inzichten te verkrijgen. (3) Zie bijlage C voor het totaaloverzicht met geïnterviewde partijen.

Voorts zijn via het internationale KPMG-netwerk en een netwerk van experts uit de wetenschap en praktijk relevante binnen- en buitenlandse initiatieven in kaart gebracht die als voorbeeld of inspiratie kunnen dienen voor oplossingsrichtingen in Nederland. Deze verkenning is verricht op basis van verkregen inzichten uit de literatuurstudie en verrichte interviews.

(2) Zie paragraaf 3.2.1 voor Europese ontwikkelingen op het gebied van de anti-witwasregelgeving.

(3) Semigestructureerde interviews zijn interviews waarbij enkele standaardvragen vooraf zijn vastgesteld en waar ruimte bestaat om tijdens het gesprek door te vragen op antwoorden of aanvullende vragen gesteld kunnen worden.

De rollen en verantwoordelijkheden van poortwachters

2

2.1 Inleiding

Dit hoofdstuk gaat in op de rollen en verantwoordelijkheden van de poortwachters[4] in het voorkomen van witwassen en financieren van terrorisme. Met poortwachters worden instellingen uit de private sector bedoeld die door de overheid zijn aangewezen als belangrijke schakel in het voorkomen van witwassen en het financieren van terrorisme. De rol van poortwachter vereist dat een grote groep financiële instellingen en professionele dienstverleners – waaronder banken, (levens)verzekeraars, trustkantoren, makelaars en notarissen – hun klanten en de risico's die zij met zich meebrengen kennen en deze risico's zo veel mogelijk mitigeren. Waar nodig en als uiterste stap, dienen zij de verlening van hun diensten te weigeren of stop te zetten als zij de risico's niet of onvoldoende kunnen mitigeren.[5]

Poortwachters acteren in een breder ecosysteem dat onder de anti-witwasregelgeving is opgetuigd. Dit wordt ook wel de meldketen of de anti-witwasketen genoemd. Poortwachters hebben daarin te maken met publieke partijen, zoals toezichthouders, FIU-NL, het OM en strafrechtelijke opsporingsinstanties zoals de politie en de Fiscale inlichtingen- en opsporingsdienst (FIOD).[6] In de volgende figuur is de verdeling tussen private en publieke partijen op gesimplificeerde wijze weergegeven:

Figuur 1: Rolverdeling publieke en private partijen binnen het anti-witwasbeleid

(4) Met poortwachters worden in dit onderzoek alle instellingen die onder de Wwft vallen bedoeld. Ook schadeverzekeraars vallen binnen de reikwijdte van dit onderzoek, hoewel zij uitsluitend onder de Sanctieregelgeving vallen. De Sanctiewet is van toepassing op iedereen in Nederland en kent in tegenstelling tot de Wwft geen poortwachtersfunctie. Zie ook paragrafen 2.2, 2.4 en 3.2.2. Om verwarring te voorkomen, scharen wij schadeverzekeraars in het kader van dit onderzoek wel onder de term 'poortwachter' wanneer naar poortwachters wordt verwezen.

(5) Van Wingerde en Hofman 2022, p. 10.

(6) De termen 'overheidspartijen', 'publieke partijen', 'publieke partners' en 'overheid' hebben in dit onderzoek dezelfde betekenis.

Om de rollen en met name de verantwoordelijkheden van poortwachters verder te kunnen duiden, volgen hierna eerst beschrijvingen van de doelstellingen voortvloeiend uit de Sanctiewet en Wwft (paragrafen 2.2 en 2.3). In paragraaf 2.4 wordt ingegaan op de specifieke rollen en verantwoordelijkheden van alle poortwachters.

2.2 Doelstelling en verplichtingen vanuit de Sanctiewet

Sancties zijn dwingende maatregelen en kunnen worden opgelegd tegen landen, bedrijven, organisaties of personen wanneer zij een dreiging vormen voor de internationale vrede en of veiligheid. Het doel van sancties is om ongewenst gedrag te doen veranderen of dit moeilijker te maken, en daarmee een afschrikkende werking te hebben richting derden. Er bestaan verschillende soorten sancties waaronder financiële sancties, handelsbeperkingen, wapenembargo's en reis- en visumbeperkingen voor bepaalde personen.(7) De verschillende soorten sancties sluiten elkaar niet uit.

De Sanctiewet (Sw) is opgesteld in 1977 en geeft de bevoegdheid aan de minister van Buitenlandse Zaken om uitvoering te geven aan internationale sanctiemaatregelen (artikel 2). Onder de Sw vallen internationale sanctiemaatregelen vanuit bijvoorbeeld de Europese Unie en de Verenigde Naties.(8) In tegenstelling tot de Wwft, is de Sw op eenieder die zich in Nederland bevindt van toepassing.(9) In het geval van financiële sancties geldt dat, afhankelijk van het betreffende sanctieregime, van gesanctioneerde personen of organisaties de bezittingen worden bevroren. Het is in de regel verboden om aan hen geld of andere financiële middelen beschikbaar te stellen, en waar van toepassing, bepaalde (financiële) diensten aan te bieden. De gedetailleerde verplichtingen hangen af van de betreffende sanctieregimes. Niet-naleving van de Sw betreft een economisch delict waar partijen strafrechtelijk voor kunnen worden vervolgd door het Openbaar Ministerie.

Voor banken, pensioenfondsen, verzekeraars, andere financiële instellingen, gereguleerde aanbieders van cryptodiensten(10) en trustkantoren gelden meer specifieke sanctieverplichtingen die zijn neergelegd in de Regeling toezicht Sanctiewet 1977 (RtSw 1977). Tevens is uitsluitend voor deze instellingen een toezichtregime opgetuigd (artikel 10 Sw). Op grond van de Aanwijzing rechtspersonen Sanctiewet 1977 zijn de Autoriteit Financiële Markten (AFM) en De Nederlandsche Bank (DNB) aangewezen als de verantwoordelijke toezichthouders. In het geval van niet-naleving door de instellingen van de specifieke vereisten uit de RtSw 1977 kunnen de toezichthouders bestuursrechtelijke maatregelen en sancties opleggen.(11)

In de Regeling toezicht Sanctiewet 1977 staan drie kernverplichtingen, die hierna kort worden toegelicht:

1. Plicht tot een adequate controle

Instellingen dienen maatregelen met betrekking tot de administratieve organisatie en interne controle (AO/IC-maatregelen) te nemen. Daaronder valt ten minste dat er een adequate controle plaatsvindt waarmee kan worden nagegaan of de identiteit van een relatie overeenkomt met een gesanctioneerde partij, en waarmee tegoeden kunnen worden bevroren indien nodig (artikel 2). Voor de AO/IC-vereisten kunnen instellingen aansluiten bij vereisten rondom de organisatie en governance zoals opgenomen in de Wet financieel toezicht (Wft), Wtt 2018 of Wwft. Hierbij dient te worden opgemerkt dat een relatie in de Sw gedefinieerd wordt als 'eenieder die betrokken is bij een financiële dienst of transactie'. Het begrip relatie is daarmee breder dan het begrip zakelijke relatie in de Wwft.(12)

(7) Ministerie van Financiën, *Leidraad Financiële Sanctieregelgeving*, 12 augustus 2020, beschikbaar via deze link, p. 4.
(8) Ministerie van Financiën, *Leidraad Financiële Sanctieregelgeving*, 12 augustus 2020, beschikbaar via deze link, p. 5-6.
(9) Volgens de Leidraad Financiële Sanctieregelgeving van het ministerie van Financiën, p. 4 gaat het om *"iedereen die zich in Nederland bevindt, op alle Nederlandse (rechts)personen en alle Nederlanders buiten Nederland"*.
(10) Dit zijn aanbieders van bewaarportemonnees voor virtuele valuta en aanbieders van diensten voor het wisselen van virtuele valuta en fiduciaire valuta.
(11) Artikel 10f Sw juncto Aanwijzing rechtspersonen Sanctiewet 1977 en artikelen 10ba, 10c en 10d Sw.
(12) DNB, *Leidraad Wwft/Sw*, september 2022, beschikbaar via deze link, p. 71.

2. Meldplicht

Wanneer een instelling vaststelt dat een relatie ingevolge de Sw gesanctioneerd is ('hit'), dient zij hier een melding van te maken (artikel 3). In tegenstelling tot meldingen van ongebruikelijke transacties op grond van de Wwft dienen deze meldingen niet bij FIU-NL gedaan te worden, maar bij de verantwoordelijke toezichthouder. Bij een dergelijke hit-melding dient de identiteit van de gesanctioneerde partij bekend te worden gemaakt. De ene meldplicht sluit de andere meldplicht echter niet uit; een sanctiehit kan ook leiden tot de veronderstelling dat mogelijk sprake is van een ongebruikelijke transactie in de zin van de Wwft. In dat geval dienen instellingen aan zowel FIU-NL als de verantwoordelijke toezichthouder een melding te doen.(13) Een instelling mag de relatie met de gesanctioneerde partij in de regel niet beëindigen.(14)

3. Bewaarplicht

Op grond van artikel 4 moeten instellingen de gegevens inzake meldingen en de daarbij relevante rekeningen en transacties bewaren voor een periode van vijf jaar nadat de sanctieregeling niet meer van toepassing is op de betreffende relatie.

De Sanctiewet kent een resultaatverplichting: instellingen zijn verplicht alle sanctieregelingen na te leven en zodoende te voldoen aan hun verplichtingen, waaronder het screenen van relaties.(15) In de wijze van naleving van de sanctieregelingen lijkt voor de bedrijfsvoering met betrekking tot de AO/IC een beperkte risicogebaseerde benadering wel toegestaan.(16) DNB geeft aan dat alle relaties moeten worden gescreend, maar dat aan de wijze van screening wel een risicogebaseerde invulling gegeven mag worden, bijvoorbeeld door een lagere frequentie of minder indringende controle.(17)

2.3 Doelstelling en verplichtingen vanuit de Wwft

De Wwft is in 2008 in werking getreden door samenvoeging van de Wet identificatie bij dienstverlening (WID) en de Wet melding ongebruikelijke transacties (Wet MOT) en biedt preventieve maatregelen in het beleid tegen witwassen en het financieren van terrorisme.(18) De Wwft behelst de omzetting van verschillende Europese anti-witwasrichtlijnen in het Nederlands recht (zie verder paragraaf 3.2.1).

Het doel van de wet is het tegengaan van witwassen van illegaal verkregen vermogen en het financieren van terrorisme en – uiteindelijk – het handhaven van de integriteit en het bewaken van de stabiliteit en reputatie van het financiële stelsel.(19) Om dit doel te bereiken hebben financiële instellingen en professionele dienstverleners op grond van de Wwft een poortwachtersfunctie toebedeeld gekregen. Met de poortwachtersfunctie wordt bedoeld dat deze instellingen en dienstverleners een belangrijke rol hebben in het beschermen van, of geven van toegang tot, het rechtsbestel en het financiële stelsel. Voor bijvoorbeeld accountants en notarissen is voor hun poortwachtersrol bij de introductie van de Wwft aangegeven dat zij rechtskracht geven aan transacties en dat ze daarmee als het ware 'de toegang tot de bovenwereld' bewaken.(20) Met de gedachte dat de bestrijding van witwassen via de private sector effectiever en efficiënter is, is steeds meer nadruk op de rol en verantwoordelijkheid van poortwachters in het voorkomen van witwassen en terrorismefinanciering komen te liggen.

In de systematiek van de Wwft ligt besloten dat toezichthouders toezien op de naleving van de normen uit de Wwft door poortwachters. In het geval van niet-naleving kan worden overgegaan tot bestuursrechtelijke handhaving, en mogelijk ook het instellen van een tuchtprocedure voor bepaalde beroepsbeoefenaars. Niet-naleving van de Wwft door poortwachters leidt ook steeds vaker tot strafrechtelijke vervolging voor organisaties en hun bestuurders.(21)

(13) DNB, *Leidraad Wwft/Sw,* september 2022, beschikbaar via deze link, p. 74.
(14) DNB, *Leidraad Wwft/Sw,* september 2022, beschikbaar via deze link, p. 70.
(15) Ministerie van Financiën, *Leidraad Financiële Sanctieregelgeving*, 12 augustus 2020, beschikbaar via deze link, p. 11.
(16) Bökkerink en Ligthart 2014, p. 214; Kodrzycki en Geertsma 2019, p. 234.
(17) Bökkerink en Ligthart 2014, p. 214; DNB, *Sanctiescreening*, 16 september 2022, beschikbaar via deze link.
(18) Kamerstukken II, 2007/2008, 31 238, nr. 3, p.1.
(19) Kamerstukken II, 2007/2008, 31 238, nr. 3, p. 1, Kamerstukken II, 2017/2018, 34 808, nr. 3, p. 2.
(20) Kamerstukken II, 2007/2008, 31 237 en 31 238, nr. 6, p. 3.
(21) Van Wingerde en Hofman 2022, p. 13.

Om de integriteit van het financiële stelsel te handhaven, zijn in de Wwft verplichtingen opgenomen waaraan poortwachters moeten voldoen.[22] Samengevat gaat het momenteel om de volgende vijf kernverplichtingen:

1. Risicomanagement

Instellingen moeten weten aan welke risico's op witwassen en terrorismefinanciering zij worden blootgesteld en dienen hun beleid, procedures en maatregelen daarop af te stemmen (artikelen 2b en 2c). Instellingen zijn verplicht maatregelen te nemen om de risico's op witwassen en financieren van terrorisme vast te stellen en te beoordelen, waarbij de maatregelen in verhouding staan tot de aard en de omvang van de instelling.[23]

Daarbij wordt ten minste rekening gehouden met risico's gerelateerd aan cliënten, landen, producten en diensten, en transacties en leveringskanalen. De risicobeoordeling moet worden gedocumenteerd, actueel worden gehouden en desgevraagd kunnen worden gedeeld met de toezichthouder.

Ook kent de Wwft enkele verplichtingen rondom de governance van poortwachters, zoals het aanwijzen van een bestuurder met eindverantwoordelijkheid voor de naleving van de Wwft door de instelling en het beschikken over een onafhankelijke en effectieve compliancefunctie en auditfunctie (artikel 23).

2. Cliëntenonderzoek

Instellingen zijn verplicht om op risicogebaseerde wijze een cliëntenonderzoek te verrichten voordat zij een zakelijke relatie aangaan (artikelen 3 en 4).[24] Het cliëntenonderzoek behelst onder meer de identificatie en verificatie van de klant, en waar van toepassing diens juridisch vertegenwoordigers. Instellingen moeten vaststellen of een klant voor zichzelf optreedt dan wel ten behoeve van een derde. Ook dienen instellingen bij rechtspersonen de identiteit van uiteindelijk belanghebbenden vast te stellen en redelijke maatregelen te nemen om deze identiteit te verifiëren, alsook om inzicht te verwerven in de eigendoms- en zeggenschapsstructuur van de rechtspersoon. De instelling dient het doel en de beoogde aard van de zakelijke relatie vast te leggen en een voortdurende controle uit te voeren (artikel 3). De Wwft benoemt tevens een aantal situaties voor vereenvoudigd en verscherpt cliëntenonderzoek (artikelen 6 t/m 9).

3. Meldplicht

Wanneer instellingen een (verrichte of voorgenomen) ongebruikelijke transactie identificeren, dienen zij deze onverwijld te melden aan FIU-NL (artikel 16).[25] De ongebruikelijke aard van transacties dient te worden vastgesteld aan de hand van subjectieve en objectieve indicatoren.[26]

- Als een transactie voldoet aan een *objectieve indicator*, zijn instellingen altijd verplicht een melding te maken bij FIU-NL. Een voorbeeld voor banken betreft een betaling met creditcard of prepaid card voor een bedrag van EUR 15.000 of meer.
- Bij *subjectieve indicatoren* gaat het om situaties waarbij de instelling aanleiding heeft om te veronderstellen dat deze verband kunnen houden met witwassen of financieren van terrorisme, en dit hangt veelal af van de omstandigheden van het geval.

Ook situaties waar het cliëntenonderzoek niet kan worden afgerond of een zakelijke relatie wordt beëindigd vanwege indicaties dat de klant betrokken is bij witwassen of het financieren van terrorisme, vallen onder de meldplicht.

Instellingen mogen medewerkers niet benadelen op basis van een op goeder trouw gemaakte melding bij FIU-NL, bijvoorbeeld door een demotie, negatieve beoordeling of uitsluiting.[27] Instellingen en hun werknemers mogen in de regel niemand laten weten dat zij een melding bij FIU-NL hebben gemaakt. Dit heet ook wel het 'tipping-off' verbod.[28]

(22) Op trustkantoren zijn in het verlengde van de Wwft tevens strengere verplichtingen uit de Wet toezicht trustkantoren 2018 van toepassing. Dit wordt nader toegelicht in paragraaf 3.2.3.
(23) Voor bepaalde financiële instellingen genoemd in artikelen 3:10, 3:17 Wft, en artikel 10 Bpr, artikel 19 Besluit financieel toetsingskader pensioenfondsen en artikel 14 Besluit uitvoering Pensioenwet, is de systematische risicoanalyse breder en omvat alle integriteitsrisico's. Hetzelfde geldt voor trustkantoren op grond van artikel 10 Besluit toezicht trustkantoren 2018. Dit staat ook wel bekend als de SIRA.
(24) Hierop bestaan enkele beperkte uitzonderingen, zie artikel 4, derde t/m zesde lid, Wwft.
(25) Bij transacties gaat het om een handeling of samenstel van handelingen ten behoeve van een cliënt waarvan de instelling ten behoeve van haar dienstverlening aan die cliënt heeft kennisgenomen. Het kan dus ook gaan om deelbetalingen of transacties waartussen een verband bestaat.
(26) Deze indicatoren zijn opgenomen in bijlage 1 van het Uitvoeringsbesluit Wwft 2018.
(27) Artikel 20b Wwft.
(28) Artikel 23 Wwft. Uitsluitend instellingen die binnen eenzelfde groep opereren, mogen deze informatie binnen de groep delen. Zie artikel 23a Wwft.

4. Bewaarplicht

Op grond van artikel 33 Wwft zijn instellingen verplicht om relevante informatie van cliënten op toegankelijke wijze vast te leggen en deze te bewaren voor vijf jaar na het einde van de zakelijke relatie of de uitvoering van de transactie.

5. Opleidingsplicht

Instellingen dienen op grond van artikel 35 Wwft ervoor te zorgen dat werknemers periodiek opleidingen volgen zodat zij in staat zijn om witwasrisco's te identificeren, het cliëntenonderzoek goed en volledig uit te voeren en ongebruikelijke transacties te herkennen. Ook het bestuur en, waar van toepassing, het toezichthoudend orgaan dienen trainingen te volgen om hun verantwoordelijkheden te kunnen dragen. Opleidingen dienen actueel gehouden te worden en dus regelmatig te worden geëvalueerd en herzien. De inhoud, diepgang en frequentie van opleidingen dienen te worden afgestemd op functies van werknemers binnen de instelling.(29)

Zowel op Europees als nationaal niveau zijn belangrijke wijzigingen inzake anti-witwasregelgeving aanstaande. Zie hiervoor verder paragraaf 3.2.1.

2.4 Verschillen in de rollen en verantwoordelijkheden van poortwachters

Op grond van de Wwft zijn verschillende groepen financiële en niet-financiële instellingen, en beroepsbeoefenaars als poortwachter aangewezen. Deze rol hebben zij toegewezen gekregen vanwege de rol die zij als professionele dienstverlener vervullen. Omdat deze rol per instelling en dienstverlener verschilt, hun blootstelling aan risico's op witwassen en het financieren van terrorisme anders is, en ook de sanctievereisten tussen poortwachters verschillen, zijn er accentverschillen te identificeren tussen verschillende poortwachters.

Hierna volgt een uiteenzetting van de rollen van de verschillende (groepen) poortwachters genoemd in de Wwft. Het feit dat sommige instellingen (tevens) aan aanvullende vereisten vanuit de Sw moeten voldoen is in paragraaf 2.2 reeds toegelicht. Daarnaast gelden voor bepaalde instellingen en beroepsbeoefenaars nog aanvullende sectorale wetgeving en/of (beroeps)regels die mogelijk een versterkende of beperkende werking hebben op de naleving van hun Wwft- en Sw-verplichtingen.(30) Dit komt verder aan de orde in paragraaf 3.3.2.

Hierna wordt eerst ingegaan op de groepen poortwachters betrokken bij dit onderzoek, gevolgd door de overige poortwachters.

2.4.1 Banken, verzekeraars, trustkantoren, notarissen en makelaars

Banken

Banken vervullen binnen de maatschappij een sleutelrol in het verlenen van toegang tot het betalingsverkeer en zijn daarom een belangrijke partij bij het waarborgen van de integriteit en stabiliteit van het financiële stelsel. Deze sleutelrol – gecombineerd met de toegenomen aandacht voor de bestrijding van witwassen en financieren van terrorisme vanuit de toezichthouder, het OM, de maatschappij en media – heeft ertoe geleid dat de discussie over de invulling van de poortwachtersrol zich heeft toegespitst op banken.(31) In de recente evaluatie van de Financial Action Task Force (FATF) concludeert de FATF dat binnen de groep niet-financiële instellingen bij veel instellingen het gevoel leeft dat het cliëntenonderzoek voornamelijk een rol voor de banken is.(32) In de afgelopen jaren hebben banken zich steeds vaker geconfronteerd gezien met hun rol als poortwachter: toezichthouder DNB heeft verschillende handhavingsmaatregelen genomen voor niet-naleving van de Wwft en ook zijn banken en hun bestuurders strafrechtelijk vervolgd.(33) Banken hebben naast de Wwft bredere integriteitsverplichtingen op grond van de Wet op het financieel toezicht (Wft) en onderliggende regelgeving.

(29) DNB, *Leidraad Wwft/Sw,* september 2022, beschikbaar via deze link, p. 10.
(30) Zo geldt voor banken, verzekeraars en andere financiële instellingen onder meer de Wet op het financieel toezicht (Wft), voor trustkantoren de Wet toezicht trustkantoren 2018 (Wtt 2018), voor notarissen de Wet op het notarisambt (Wna), voor advocaten de Advocatenwet en voor accountants de Wet toezicht accountantsorganisaties (Wta).
(31) Stichting Maatschappij en Veiligheid 2022, p. 14 en NVB 2022a, p. 13.
(32) FATF 2022b, p. 122.
(33) Stichting Maatschappij en Veiligheid 2022, p. 5.

Een voorbeeld betreft de uitgebreide vereisten rondom risicomanagement en governance.

Verzekeraars

De verzekeringssector kent vier verschillende soorten verzekeraars: levensverzekeraars, schadeverzekeraars, natura-uitvaartverzekeraars en herverzekeraars. Uitsluitend levensverzekeraars zijn als poortwachter op grond van de Wwft aangemerkt. De reden hiervoor volgt uit het risico dat de middelen die gebruikt worden om de verzekering te financieren, mogelijk illegaal verkregen middelen betreffen. Bovendien bestaat er een (beperkt) risico dat de polisuitkeringen worden gebruikt voor het financieren van terrorisme. Vanwege deze risico's zijn financiële dienstverleners die bemiddelen in levensverzekeringen ook aangemerkt als poortwachter onder de Wwft.(34) De andere soorten verzekeraars vallen niet onder de reikwijdte van de Wwft. Deze verzekeraars dienen wel te voldoen aan de aanvullende verplichtingen van de Sw.(35)

Verzekeraars hebben net als banken te maken met bredere integriteitsverplichtingen op grond van de Wet op het financieel toezicht (Wft) en onderliggende regelgeving.

Trustkantoren

Gegeven de aard van hun dienstverlening, spelen trustkantoren een belangrijke rol bij het verlenen van toegang tot het Nederlandse economisch klimaat aan buitenlandse rechtspersonen. In de literatuur wordt gesteld dat trustdiensten kunnen worden misbruikt om eigendomsstructuren te verhullen.(36) Ook kunnen klanten financiële constructies nastreven die bepaalde fiscale integriteitsrisico's met zich meebrengen.(37) Om deze redenen dienen trustkantoren een rol te spelen in de bewaking van de integriteit van het financiële stelsel en zijn zij aangemerkt als poortwachter onder zowel de Wwft als de Wtt 2018. Deze laatste wet bevat aanvullende, meer gedetailleerde en strengere verplichtingen rondom het cliëntenonderzoek en legt ook enkele verboden op aan trustkantoren, zoals verder wordt uitgewerkt in paragraaf 3.2.3. Recentelijk is er vooral aandacht geweest voor de risico's op witwassen via illegale trustdienstverlening.(38)

Notarissen

Notarissen zijn onafhankelijke juridisch adviseurs die gemaakte afspraken en verklaringen rechtsgeldig vastleggen in een notariële akte. Vanwege hun specifieke juridische kennis en rol in het Nederlandse rechtsstelsel zijn zij aangemerkt als poortwachter.(39) Niet alle diensten die door notarissen worden verleend vallen onder de reikwijdte van de Wwft: kort gezegd gaat het om diensten gerelateerd aan het ondernemingsrecht en vastgoed.(40) Daarbij gaat het bijvoorbeeld om het oprichten van vennootschappen, de aan- of verkoop van aandelen, of het faciliteren van vastgoedtransacties. Ook geldt een procesvrijstelling: de Wwft is niet van toepassing op werkzaamheden rondom de juridische verdediging van klanten.(41) De aard van de dienstverlening van notarissen in combinatie met de geheimhoudingsplicht van de notaris op grond van de Wet op het notarisambt (Wna), maakt dat zij in de literatuur worden aangemerkt als een aantrekkelijke beroepsgroep voor criminelen, wat het belang van hun rol als poortwachter aantoont.(42)

Makelaars en taxateurs

De vastgoedsector is vatbaar voor witwassen en andere vormen van financieel-economische criminaliteit. Vastgoed is een populaire keuze voor investeerders door de relatief stabiele – en doorgaans stijgende – prijzen. Ook is vastgoed functioneel: het kan worden bewoond of worden verhuurd.(43) Dit trekt echter ook criminelen aan.

Factoren die bijdragen aan de vatbaarheid van de vastgoedsector voor criminelen zijn onder meer de beperkte duur van de relatie met klanten waardoor het voor een makelaar lastig is om verdachte omstandigheden of patronen te identificeren, de mogelijkheid voor het verplaatsen van grote geldstromen bij de aan- of verkoop van vastgoed, een gebrek aan transparantie bij de waarde- en prijsvorming van vastgoed en mogelijkheden voor hoge rendementen.(44)

(34) FATF 2018, p. 9.
(35) Artikel 10 Sw 1977 en Artikel 1 RtSw 1977.
(36) FATF 2019, p. 9.
(37) DNB 2019, p. 5.
(38) Zie hierover paragraaf 3.2.3.
(39) Van Wingerde & Hofman 2022, p. 10.
(40) Artikel 1a, vierde lid, onder d Wwft. Zie ook: Snijder-Kuipers 2020, p. 36-37.
(41) Artikel 1a, vijfde lid, Wwft.
(42) Zie over de geheimhoudingsplicht: Van Wingerde & Hofman 2022, p. 43.
(43) Europees Parlement 2019, p. 2.
(44) Europees Parlement 2019, p. 1-2; FATF 2022a, p. 16-17.

Gezien hun dienstverlening en expertise worden makelaars geacht om indicaties van financieel-economische criminaliteit te herkennen. Tegen deze achtergrond worden makelaars aangemerkt als poortwachters. In tegenstelling tot veel andere categorieën poortwachters is de makelaardij in Nederland een niet-gereguleerd beroep en is de titel makelaar niet wettelijk beschermd, wat de sector nog kwetsbaarder kan maken.(45) Er wordt in de literatuur gewezen op het feit dat het ontbreken van regulering ervoor kan zorgen dat *"zich eerder malafide makelaars op de markt kunnen begeven en dat deze tevens niet uit het beroep van makelaar kunnen worden gezet"*.(46) Tegen deze achtergrond worden makelaars aangemerkt als poortwachters. Dit geldt zowel bij de aan- en verkoop van onroerende zaken als de bemiddeling bij en het sluiten van huurcontracten waarbij de maandelijkse huurprijs een bedrag van EUR 10.000 of meer bedraagt.(47)

Taxateurs onroerend goed bepalen de waarde van vastgoed, en vallen daarom ook onder de reikwijdte van de Wwft. Het gaat om alle soorten taxaties met betrekking tot onroerende zaken, bijvoorbeeld in verband met een aankoop of een herfinanciering.

2.4.2 Overige poortwachters

Financiële instellingen niet-zijnde banken en verzekeraars

Naast de hiervoor genoemde banken en verzekeraars zijn er nog verschillende andere financiële instellingen die onder de Wwft als poortwachter zijn aangemerkt. Dit betreffen onder meer (beheerders van) beleggingsinstellingen en instellingen voor collectieve beleggingen in effecten (icbe's), beleggingsondernemingen, betaaldienstverleners en -agenten, elektronisch geldinstellingen en wisselinstellingen. Deze instellingen zijn als poortwachter aangemerkt vanwege het risico dat zij worden misbruikt om de criminele oorsprong van gelden te verhullen via grote volumes van financiële transacties (ook wel 'layering' genoemd).

Accountants, advocaten, belastingadviseurs

Evenals notarissen worden accountants, advocaten en belastingadviseurs vanwege hun specifieke juridische, fiscale of financiële expertise als poortwachter aangemerkt.(48) Criminelen kunnen misbruik maken van deze expertise, bijvoorbeeld om via complexe juridische eigendomsstructuren eigenaarschap te verhullen, of om de criminele oorsprong van middelen te verhullen.(49) Ook geldt dat accountants, advocaten en belastingadviseurs gezien de aard van hun dienstverlening juist kunnen stuiten op vermoedens van financieel-economische criminaliteit. Denk bijvoorbeeld aan indicaties voor fraude bij de controle van de jaarrekening door accountants.

Voor advocaten geldt net als voor notarissen dat zij niet voor alle diensten onder de reikwijdte van de Wwft vallen.(50) De procesvrijstelling zoals beschreven bij notarissen is eveneens van toepassing op advocaten, belastingadviseurs en beroepsbeoefenaars die werkzaamheden vergelijkbaar aan die van advocaten of notarissen verrichten.

Aanbieders cryptodiensten

De markt voor virtuele valuta is de afgelopen jaren sterk in populariteit gegroeid. Virtuele valuta hebben bepaalde kenmerken die witwassen aantrekkelijk maken, waaronder de anonimiteit, de snelheid van transacties en het gemak van grensoverschrijdende transacties.(51) Vanuit dit perspectief zijn aanbieders van bewaarportemonnees en bedrijven die diensten aanbieden voor het wisselen tussen virtueel en fiduciair geld met de komst van de vijfde Europese anti-witwasrichtlijn en omzetting in de Wwft aangemerkt als poortwachter.(52)

(45) FATF 2022a, p. 16; Hoogenboom 2021, p. 171 merkt op dat een aanzienlijk deel van de makelaars niet aangesloten is bij brancheverenigingen en dat de laatste juist een belangrijke rol vervullen bij het creëren en versterken van de poortwachtersfunctie van makelaars. Hij pleit voor het opnieuw invoeren van de beschermde titel voor 'makelaar onroerend goed' met een verplicht lidmaatschap bij de te consolideren brancheorganisatie.
(46) Van Wingerde et al. 2023, p. 49.
(47) Artikel 1a, vierde lid, onder h, Wwft.
(48) Van Wingerde & Hofman 2022, p. 10
(49) FATF 2019a, p. 12-16.
(50) Artikel 1a, vierde lid, onder c, Wwft.
(51) FATF 2021b, p. 16.
(52) Richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU, *PbEU* L-156, p. 43-74.

Met de aanstaande Europese verordening Markten in Cryptoactiva (MiCAR) wordt de gehele cryptosector aan integriteitseisen onderworpen.[53] Het huidige registratieregime wordt vervangen door een zwaarder vergunningenregime, wat gepaard gaat met meer gedetailleerde normen wat betreft hun governance, waar meer soorten aanbieders van cryptodiensten onder zullen vallen.

Kansspelaanbieders

Met de invoering van de Wet Kansspelen op afstand in 2021 zijn naast Holland Casino ook aanbieders van online kansspelen als poortwachter onder de Wwft opgenomen. Online gokken kent namelijk vele witwasrisico's, waaronder de mogelijkheid tot anonimiteit, het hebben van een relatie op afstand ('non-face-to-face'), en complexe en omvangrijke transactiepatronen.[54]

Handelaren in luxegoederen, professionele handelaren in goederen en pandhuizen

Handelaren in luxegoederen, zowel kopers als verkopers, vallen onder de Wwft. Bij luxegoederen gaat het om voertuigen, schepen, kunstvoorwerpen, antiquiteiten, edelstenen, edele metalen, sieraden en juwelen. Ook handelaren in kunstvoorwerpen (kunst en culturele goederen) worden als poortwachter aangewezen, voor zover betaling voor de kunst plaatsvindt voor een bedrag van EUR 10.000 of meer.

Voor kunst en culturele goederen geldt dat de waarde lastig is in te schatten en daarmee aantrekkelijk is voor witwassen. Ook kunnen criminelen ervoor kiezen om kunst te bewaren, wordt kunst veel met cash of via schijnconstructies aangeschaft, en wordt ogenschijnlijke legitimiteit gegeven aan middelen die betrokken zijn geweest bij fictieve verkopen en nepveilingen.[55]

Professionele handelaren, zowel kopers als verkopers, vallen onder de reikwijdte van de Wwft voor zover zij betalingen verrichten in contanten van EUR 10.000 of meer voor goederen anders dan voornoemde luxegoederen. Het is algemeen bekend dat cash een geschikt middel is om wit te wassen vanwege de anonimiteit rondom herkomst, bezit en gebruik.

Domicilieverleners

Aanbieders van (post)adressen kunnen mogelijk worden misbruikt door criminelen. Het enkel beroeps- of bedrijfsmatig een (post)adres ter beschikking stellen (domicilieverlening) zonder aanvullende werkzaamheden is geen trustdienst onder de Wtt 2018. Daarom zijn ook deze domicilieverleners aangemerkt als poortwachter onder de Wwft.

2.5 Conclusies over de rollen en verantwoordelijkheden van poortwachters

Uit het voorgaande wordt duidelijk dat hoewel de doelstelling en verplichtingen op grond van de Wwft gelijk zijn voor alle poortwachters, dit een grote heterogene groep betreft waarin accentverschillen in ieders rol en verantwoordelijkheden te identificeren zijn.

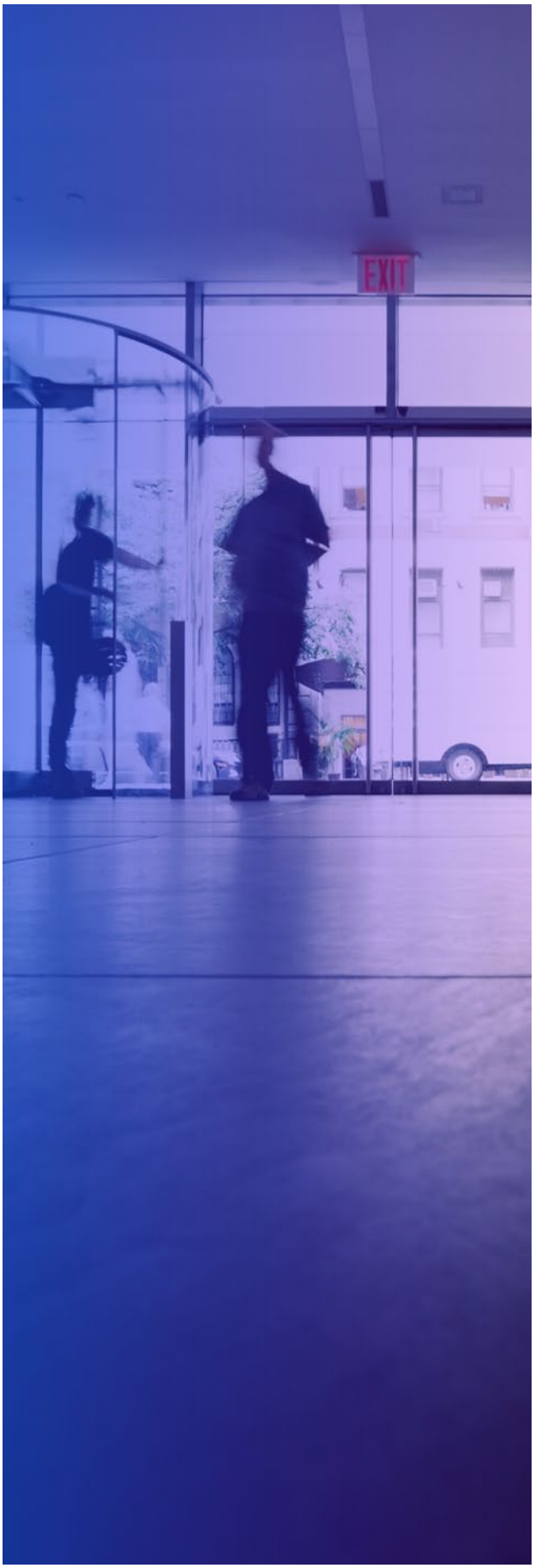
Instellingen en beroepsbeoefenaars worden om verschillende redenen als poortwachter aangemerkt. Op basis van de dienstverlening bieden zij bijvoorbeeld toegang tot het betalingsverkeer of de Nederlandse economie (banken en trustkantoren) of verlenen zij specifieke juridische, fiscale of financiële diensten (bijvoorbeeld notarissen, advocaten en belastingadviseurs). Ook kunnen instellingen en beroepsbeoefenaars als poortwachter worden aangemerkt vanwege het risico op misbruik voor witwasdoeleinden – te denken valt aan vastgoed of cash – of omdat zij op basis van de aard van hun dienstverlening in de gelegenheid zijn om indicaties van fraude en andere vormen van financieel-economische criminaliteit te signaleren. Dit laatste is bijvoorbeeld het geval bij accountants. In relatie tot de poortwachtersrol valt ook op dat de duur van de relatie met klanten verschillend is voor poortwachters. Soms hebben zij lange, duurzame relaties met klanten zoals het geval bij banken, trustkantoren of controlerend accountants het geval is.

(53) DNB, 'MiCAR belangrijke stap in regulering van crypto-markten', nieuwsbericht 6 oktober 2022. In mei 2023 is de verordening aangenomen: Raad van de EU, 'Digitaal geld: Raad neemt nieuwe regels aan over markten in cryptoactiva (MiCA)', persbericht 16 mei 2023. De verordening treedt in werking op de 20e dag na bekendmaking in het Publicatieblad van de Europese Unie en is 18 maanden later van toepassing.
(54) Europese Commissie 2022, p. 23; N. Boere, 'Online gokken als witwasmethodiek', nieuwsbericht AMLC 28 november 2022.
(55) FATF 2023, p. 21-22.

Andere poortwachters hebben juist eenmalig of op ad-hoc basis contact met klanten (bijvoorbeeld handelaren in (luxe)goederen, taxateurs of makelaars).

De Sw en de daarmee gepaarde verplichtingen zijn op alle poortwachters van toepassing. Echter, banken, verzekeraars, andere financiële instellingen, trustkantoren en aanbieders van cryptodiensten hebben in vergelijking met andere poortwachters te maken met meer gedetailleerde verplichtingen en staan onder toezicht van de AFM en/of DNB. Noemenswaardig is ook dat schadeverzekeraars niet onder de Wwft, maar wel onder de Sw vallen en formeel geen poortwachtersfunctie hebben.

Tot slot wordt opgemerkt dat verschillende poortwachters ook moeten voldoen aan sectorale wetgeving en/of (beroeps)regelgeving die van invloed kan zijn op (de uitvoering van) hun poortwachtersrol op grond van de Wwft. Dit kwam in dit hoofdstuk al naar voren voor onder meer banken, verzekeraars en trustkantoren en notarissen en zal ook, waar relevant, verder aan de orde komen in hoofdstuk 3.



De uitvoering van de Wwft en Sanctiewet

3

3.1 Inleiding

Om een verkenning te kunnen verrichten naar kansen en mogelijkheden om een verbetering van de efficiëntie en effectiviteit van de anti-witwasketen en de naleving van de Sanctiewet te realiseren, is het belangrijk om te weten hoe het met de uitvoering van de Wwft en Sw staat. Daarbij is het nuttig te kijken naar de ontwikkelingen in recente jaren en de verwachte ontwikkelingen op korte en middellange termijn (paragraaf 3.2) en knelpunten die door verschillende groepen betrokkenen worden ervaren of geconstateerd (paragraaf 3.3).

3.2 Relevante ontwikkelingen voor de uitvoering

Deze paragraaf gaat in op de ontwikkelingen van de Wwft en Sanctiewet. Tevens wordt ingegaan op de ontwikkelingen in de Wet toezicht trustkantoren, omdat de Wtt 2018 gedeeltelijk een verlengde vormt van de normen uit de Wwft met normen die strikter van aard zijn. Ook wordt ingegaan op relevante technologische ontwikkelingen die een impact (kunnen) hebben op de uitvoering van de Wwft en Sw. Gegeven het spanningsveld tussen de uitvoering van de Wwft en Sw, die enerzijds als doel heeft het beschermen van de integriteit van de financiële sector, en de privacyregelgeving met als doel de bescherming van privacy van burgers en bedrijven anderzijds, wordt tot slot ook nog ingegaan op relevante ontwikkelingen op het gebied van privacy.

3.2.1 De ontwikkelingen van de Wwft in vogelvlucht

In hoofdstuk 2 is reeds opgemerkt dat de Wwft in augustus 2008 tot stand is gekomen.[56] De Wwft is het resultaat van de omzetting van meerdere Europese anti-witwasrichtlijnen, welke op hun beurt weer voortvloeien uit de aanbevelingen van de FATF. De FATF is een internationale organisatie op het gebied van de bestrijding van witwassen, financiering van terrorisme en de financiering van massavernietigingswapens.[57] De FATF publiceert internationale standaarden ter bestrijding van witwassen die wereldwijd de basis vormen voor wetgevende en toezichthoudende instanties in de ontwikkeling van wet- en regelgeving. In de afgelopen jaren is de Wwft als gevolg van wijzigingen aan de FATF-standaarden, en vervolgens de Europese richtlijnen, meerdere keren gewijzigd.

De ontwikkelingen van het anti-witwasbeleid op Europees niveau nemen een grote vlucht. Wijzigingen volgen elkaar in steeds rapper tempo op, waardoor de Wwft ook steeds vaker is aangepast. Waar tussen de derde (AMLD3[58]) en vierde anti-witwasrichtlijn (AMLD4[59]) bijvoorbeeld tien jaar zat, zit tussen de vierde en vijfde Europese anti-witwasrichtlijn (AMLD5[60]) slechts drie jaar. Daarbovenop wordt sinds 2019 al gesproken over nieuwe Europese regelgeving; en wordt sinds juli 2021 daadwerkelijk toegewerkt naar nieuwe Europese anti-witwasregelgeving (zie verderop in deze paragraaf).

Met de opeenvolgende regelgeving is ook steeds de groep poortwachters uitgebreid. Meer en meer private partijen zijn de afgelopen jaren onder de reikwijdte van de anti-witwasregelgeving komen te vallen en fungeren zodoende als poortwachter. De AMLD3 introduceerde bijvoorbeeld aanbieders van trust- en bedrijfsdiensten als nieuwe groep poortwachters. De AMLD4 bracht aanbieders van kansspelen en een uitbreiding van de groep handelaren in goederen onder de reikwijdte, en met AMLD5 werd de reikwijdte nog verder uitgebreid met aanbieders van cryptodiensten (bewaarportemonnees en wisseldiensten).

(56) Kamerstukken II, 2007/2008, 31 238, nr. 3, p. 3.
(57) Bökkerink 2022, p. 196.
(58) Richtlijn 2005/60/EG van het Europees Parlement en de Raad van 26 oktober 2005 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme, *PbEU* L-309, p. 15-36.
(59) Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie, *PbEU* L-141, p. 73-117.
(60) Richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU, *PbEU* L-156, p. 43-74.

Tot slot is ook de materiële normstelling enorm uitgebreid de afgelopen jaren en wordt steeds meer van poortwachters verwacht in de uitvoering van de Wwft. Er zijn nieuwe normen geïntroduceerd, en ook zijn bestaande verplichtingen gedetailleerder geworden. Te denken valt aan toegenomen nadruk op de risicogebaseerde benadering en bronnen waar instellingen rekening mee moeten houden(61), de uitbreiding van verscherpte onderzoeksmaatregelen bij binnenlandse politiek prominente personen (PEP's), de specifieke verscherpte onderzoeksmaatregelen in het geval van hoogrisicolanden aangewezen door de Europese Commissie, de introductie van het register van uiteindelijk belanghebbenden (UBO-register) en de terugmeldplicht, en vereisten met betrekking tot de governance van instellingen zoals de compliance- en interne auditfuncties.

Blik op de toekomst

Bovengenoemde ontwikkelingen lijken zich door te zetten op Europees niveau. Vanwege meerdere witwasschandalen waarbij Europese banken betrokken waren alsook de publicaties van de Panama en Paradise Papers waarin onthullingen gerelateerd aan belastingontduiking en ontwijking van sancties werden gedaan, heeft de Europese Commissie in 2019 eerste stappen gezet om te komen tot een sterker Europees regelgevend kader.(62) In juli 2021 presenteerde zij het zogenaamde EU AML Package.(63) Dit pakket bestaat uit vier wetgevingsvoorstellen:

- een nieuwe anti-witwasrichtlijn ('AMLD6');
- een anti-witwasverordening ('AMLR');
- een verordening tot oprichting van een nieuwe Europese anti-witwasautoriteit (Anti-Money Laundering Authority, 'AMLA'); en
- een herziening van de verordening betreffende bij geldovermakingen te voegen informatie.

De kern van het EU AML package is de introductie van een uniform normenkader voor alle instellingen en beroepsbeoefenaars die onder de reikwijdte van het Europese anti-witwasbeleid vallen en de introductie van Europees toezicht.(64) Door het overhevelen van een groot deel van de materiële normstelling naar een Europese verordening die rechtstreeks van toepassing is, wordt de voorgestelde richtlijn in vergelijking met de AMLD5 beperkter. AMLD6 zal normen bevatten over nationale registers, zoals het UBO-register en vastgoedregister, alsook taken en verantwoordelijkheden van nationale FIU's en toezichthouders.

Medio 2023 bevinden de voorstellen voor de AMLD6, AMLR en AMLA-R zich in de triloogfase tussen de Europese Commissie, de Raad en het Europees Parlement. De herziening van de verordening betreffende bij geldovermakingen te voegen informatie is ondergebracht bij het eerdergenoemde MiCAR en in mei 2023 definitief aangenomen.(65)

Ook op nationaal niveau worden belangrijke wetswijzigingen verwacht. In oktober 2022 is na jaren van voorbereiding het wetsvoorstel Wet plan van aanpak witwassen ingediend bij de Tweede Kamer.(66) Dit wetsvoorstel introduceert wijzigingen op de Wwft die toezien op het door banken gezamenlijk monitoren van transacties en het delen van gegevens tussen Wwft-instellingen van dezelfde categorie over klanten met een hoger risicoprofiel.(67) Het wetsvoorstel volgt uit een breder Plan van aanpak uit 2019 en heeft tot doel de aanpak van witwassen in Nederland effectiever te maken.(68) Meer informatie over dit wetsvoorstel en de relatie tot privacyregelgeving is opgenomen in paragraaf 3.2.5.

(61) Bijvoorbeeld de richtsnoeren van de EBA en de door de Europese Commissie gepubliceerde Supranational Risk Assessment (SNRA) en de national risk assessments witwassen en terrorismefinanciering voor Nederland.
(62) Groen en Van den Broek 2023, p. 13-15.
(63) Europese Commissie, 'Anti-money laundering and countering the financing of terrorism legislative package', persbericht 20 juli 2021.
(64) Groen en Van den Broek 2023, p. 14.
(65) Zie paragraaf 2.4.2 over MiCAR. Zie ook Raad van de EU, 'Witwassen: Raad neemt regels aan die overmakingen van cryptoactiva traceerbaar maken', persbericht 16 mei 2023.
(66) Het Plan van aanpak witwassen dateert van juni 2019: Kamerstukken II, 2018/2019, 31 477, nr. 41, bijlage Plan van aanpak witwassen.
(67) Wetsvoorstel Wet plan van aanpak witwassen, Kamerstukken II, 2022/2023, 36 228, nr. 2.
(68) Kamerstukken II, 2018/2019, 31 477, nr. 41.

3.2.2 De ontwikkelingen van de Sanctiewet in vogelvlucht

Op basis van de Sanctiewet 1977 geeft Nederland uitvoering aan de (inter)nationale sanctiemaatregelen. In de jaren negentig waren VN-sancties een veelgebruikt instrument, maar het vetorecht voor permanente leden in de VN Veiligheidsraad maakt dat met de geopolitieke veranderingen het voor de VN steeds moeilijker geworden is om tot sanctiebesluiten te komen.(69) Unilaterale sancties worden steeds vaker door de Europese Unie, maar ook door landen als de Verenigde Staten en het Verenigd Koninkrijk opgelegd.

De Russische inval in Oekraïne heeft ertoe geleid dat het sanctielandschap zich razendsnel heeft ontwikkeld; in ruim een jaar tijd heeft de EU elf sanctiepakketten aangenomen.(70) Vanwege problemen met de implementatie van sancties en het toezicht daarop, mede door de grote hoeveelheid betrokken publieke partijen, is in 2022 de Nationaal Coördinator Sanctienaleving en Handhaving aangewezen. Deze Nationaal Coördinator kreeg als taak om de naleving van sancties tussen ministeries en uitvoeringsorganisaties af te stemmen en om verbeterpunten te identificeren. Het rapport met bevindingen van de Nationaal Coördinator is in mei 2022 gepubliceerd en toont verschillende knelpunten.(71) Voorbeelden betreffen de structuur van de Nederlandse economie, een versnipperd toezichtlandschap met beperkingen in gegevensuitwisseling, en uitdagingen bij de identificatie van UBO's. Ook wordt in het rapport aangestipt dat instellingen die onder de RtSw 1977 vallen – waaronder banken, verzekeraars en trustkantoren – de sanctieregels liever te streng dan te los toepassen, waardoor sprake lijkt te zijn van 'overcompliance'.(72) Aanbevelingen volgend uit dit rapport richten zich onder andere op intensievere samenwerking tussen alle betrokken partijen, uitbreiding van toezicht en de meldplicht naar het notariaat, de advocatuur en accountancy en een sterkere rechtsgrondslag voor het uitwisselen van gegevens. Het kabinet heeft aangekondigd te werken aan volledige herziening van het Nederlandse sanctiestelsel als antwoord op de aanbevelingen uit het rapport.(73)

Blik op de toekomst

Hoe de Nederlandse herziening van het sanctiestelsel eruit gaat zien, is ten tijde van dit onderzoek nog niet bekend. Ook is het nog niet duidelijk hoe deze wijzigingen zich zullen verhouden tot de ontwikkelingen op Europees niveau. Met het eerdergenoemde EU AML package zullen namelijk ook verschuivingen in Europese regelgeving plaats gaan vinden: het ontwijken van gerichte financiële sancties wordt expliciet onder de reikwijdte van de AMLR gebracht. Ook wordt in de laatst beschikbare Europese voorstellen van de AMLD6 voorzien in een volledig systeem van toezicht op de naleving van gerichte financiële sancties door alle betrokken poortwachters.

3.2.3 De ontwikkelingen van de Wtt in vogelvlucht

De trustsector is sinds 2004 gereguleerd: trustkantoren zijn sinds die tijd vergunningplichtig en dienen te voldoen aan het wettelijk kader zoals neergelegd in de Wet toezicht trustkantoren. Onthullingen zoals de Panama Papers, onderzoeken door toezichthouder DNB en uitkomsten van het onderzoek van de Parlementaire ondervragingscommissie Fiscale constructies gaven aanleiding tot een grootschalige herziening van de op trustkantoren van toepassing zijnde wet- en regelgeving.(74) De Wet toezicht trustkantoren 2018 (Wtt 2018) vormt sinds 1 januari 2019 het regelgevend kader voor trustkantoren. De belangrijkste wijzigingen ten opzichte van de oude Wet toezicht trustkantoren betroffen de vereisten rondom de professionaliteit en integriteit van trustkantoren en het cliëntenonderzoek.

(69) Van den Herik 2022, p. 111-112.
(70) In juni 2023 is het elfde sanctiepakket aangenomen: Raad van de EU, 'Russia's war of aggression against Ukraine: EU adopts 11th package of economic and individual sanctions', persbericht 23 juni 2023.
(71) Nationaal coördinator sanctienaleving en handhaving 2022.
(72) Nationaal coördinator sanctienaleving en handhaving 2022, p. 13.
(73) Kamerstukken II, 2022/2023, 36 200 V, nr. 56, p. 5-9.
(74) Kamerstukken II, 2017/2018, 34 910, nr. 3, p. 4; Riekerk 2016, p. 433.

Voor de trustsector is het goed te vermelden dat de Wtt 2018 enkele specifieke en striktere eisen bevat in vergelijking met de Wwft. Enkele voorbeelden betreffen:

1. Bij trustkantoren strekt het cliëntenonderzoek zich bijvoorbeeld niet alleen uit tot de klant, maar via artikelen 27-30a Wtt 2018 ook tot overige bij de trustdienstverlening betrokken partijen, zoals doelvennootschappen, trusts of partijen betrokken bij de verkoop van een rechtspersoon.(75)
2. De Wtt 2018 vereist voor elementen uit het cliëntenonderzoek, specifiek voor situaties waar hogere integriteitsrisico's zijn, een resultaatverplichting. Hoewel dit past binnen de risicogebaseerde systematiek van de Wwft, betekent dit voor trustkantoren een zwaardere onderzoekslast.(76)
3. Trustkantoren zijn meer beperkt in de mogelijkheden voor het introducerend cliëntenonderzoek wanneer dit is verricht door een andere Wwft-instelling. Op grond van de Wtt 2018 moet het onderzoek door het trustkantoor zelf worden uitgevoerd, of door een zogeheten introducerende instelling binnen de groep van het trustkantoor.(77)
4. Trustkantoren zijn verplicht om te onderzoeken of een ander trustkantoor diensten verleent of heeft verleend aan de cliënt of de doelvennootschap, en of een cliënt of de doelvennootschap op voorhand bij een ander trustkantoor is geweigerd.(78)

Hoewel de Wtt 2018 relatief recente wetgeving betreft, is deze toch al een aantal keer ingrijpend gewijzigd. De meest recente wijzigingen dateren uit 2022 en de eerste helft van 2023. Een eerste belangrijke wijziging betreft het verbod om trustdiensten te verlenen aan cliënten uit bepaalde landen. Dit verbod is in eerste aanleg voor Rusland en Belarus via een spoedmaatregel ingesteld na de inval van Rusland in Oekraïne in februari 2022.(79)

Dit verbod trad op 16 juli 2022 in werking. Via het wetsvoorstel Wet integriteitsmaatregelen trustkantoren (Wit), dat op 6 december 2022 door de Eerste Kamer is aangenomen, wordt dit verbod uitgebreid naar hoogrisicolanden die door de Europese Commissie zijn aangewezen als staten met een hoger risico op witwassen of financieren van terrorisme of landen die als niet-coöperatief worden aangemerkt op belastinggebied. Een tweede wijziging die via de Wit is doorgevoerd, betreft het verbod om beroeps- of bedrijfsmatig gebruik te maken van doorstroomvennootschappen ten behoeve van een cliënt. Achtergrond van dit verbod ligt in de aanpak van belastingontduiking en -ontwijking in Nederland. In de Memorie van toelichting wordt gesteld dat *"het ter beschikking stellen van een doorstroomvennootschap [...] voornamelijk fiscale doeleinden [dient] en leidt tot een gebrek aan transparantie".*(80)

Mede als gevolg van de uitbreidingen van verboden in de trustwetgeving is ook wel gewezen op het risico van illegale trustdienstverlening. Op basis van onderzoek is geschat dat *"in termen van aantal doelvennootschappen [...] het marktaandeel van illegale trust dus ca. 15 procent [is]".*(81) Het probleem hierbij is dat deze illegalen zich onttrekken aan het oog van de toezichthouder, waardoor er juist nog minder grip op is op deze groep.(82) Het probleem van illegaliteit is recentelijk duidelijk geworden naar aanleiding van onderzoek van het Financieele Dagblad (FD) en Company.Info naar de impact van de spoedwet met het verbod voor trustkantoren om diensten te verlenen aan Russische klanten.(83) Het FD stelt dat Russische klanten sinds het verbod *"in de luwte"* opereren, er minder zicht is op deze groep en dat het verhuizen van Russische klanten naar andere partijen dan gereguleerde trustkantoren niet betekent dat *"witwas- en integriteitsrisico's vanzelf verdwijnen".*(84)

(75) Kamerstukken II, 2017/2018, 34 910, nr. 3, p. 4.
(76) Kamerstukken II, 2017/2018, 34 910, nr. 3, p. 9.
(77) Artikel 23 Wtt 2018.
(78) Zie artikel 68 Wtt 2018 in samenhang met Kamerstukken II, 2022/2023, 32 545, nr. 180, p. 6. Wat betreft het punt van 'op voorhand geweigerd' geeft minister Kaag zelf aan dat de wet hierover nu niet duidelijk is en dat dit bij een eerste geschikte mogelijkheid zal worden gewijzigd.
(79) Wijziging van de Wet toezicht trustkantoren 2018 in verband met een spoedmaatregel om trustdienstverlening aan cliënten in de Russische Federatie of de Republiek Belarus te verbieden, *Stb.* 2022, 303.
(80) Kamerstukken II, 2021/2022, 36 102, nr. 3, p. 2.
(81) SEO 2021, p. iv.
(82) Zie bijvoorbeeld 'Nederland kent strengste trustwetgeving in EU', *Holland Quaestor* 27 februari 2023.
(83) S. Motké, G. de Groot en J. Leupen, 'Hoe een 'zwart gat' in Amsterdam zich vult met Russen', *FD* 24 maart 2023; G. de Groot, J. Leupen en S. Motké, 'Russische klanten gaan ondergronds na Nederlands trustverbod', *FD* 24 maart 2023.
(84) FD Redactioneel Commentaar, 'Nederland heeft blinde vlek in trusttoezicht', *FD* 28 maart 2023.

Blik op de toekomst

Andere ontwikkelingen zijn alweer aanstaande. Op 31 juli 2022 is het rapport 'De toekomst van de trustsector' gepubliceerd.(85) In opdracht van de minister van Financiën is onderzocht of bij trustdienstverlening de integriteit voldoende te waarborgen is. Onderzoekers concluderen dat inherente integriteitsrisico's voornamelijk worden ingegeven door de *"internationale aard en de complexiteit van transacties en eigendomsstructuren"*, en dat de *"risico's niet volledig worden weggenomen zolang transacties die door Nederland lopen, de eigendomsstructuren die in Nederland gevestigd zijn en de legitimiteit van de herkomst van vermogen niet volledig navolgbaar zijn"*, maar dat deze risico's deels kunnen worden beheerst door de poortwachtersfunctie van trustkantoren.(86) In reactie op het onderzoek informeerde de minister van Financiën de Tweede Kamer over de vervolgstappen en noemde daarbij enkele relevante voorstellen.(87) Zo bevat de consultatieversie van het wetsvoorstel Wijzigingswet Financiële Markten 2024 enkele aanscherpingen op de Wtt 2018: wijziging van de definities 'optreden als bestuurder', het vervallen van de eis van voorafgaande toestemming van DNB bij bepaalde wijzigingen van de zeggenschapsstructuur door vergunninghoudende trustkantoren, en een aanscherping in relatie tot het uitvoering geven aan belastingadvies door trustkantoren in verband met het verbod voor trustkantoren om aan dezelfde klant zowel belastingadvies te geven als trustdiensten te verlenen.(88) Ook gaf de minister aan enkele aanvullende maatregelen te overwegen, waaronder i) een verduidelijking van de wettelijke bepaling inzake de verplichte informatiedeling tussen trustkantoren dat óók moet worden nagegaan of klanten op voorhand bij een ander trustkantoor zijn geweigerd (om het zogenaamde trustshoppen te voorkomen), en ii) het vergroten van de transparantie van trustkantoren (via een rapportageverplichting in de jaarrekening).(89)

3.2.4 Relevante technologische ontwikkelingen voor de uitvoering van de Wwft en de Sanctiewet

Ook technologische ontwikkelingen hebben een impact op de uitvoering van de Wwft en Sw. Deze ontwikkelingen kunnen in potentie bijdragen aan een effectievere en efficiëntere naleving van de wetgeving en zodoende financieel-economische criminaliteit beter bestrijden.(90) Hierna volgen drie ontwikkelingen:

1. Digitale identiteit en portemonnee ('wallet')

Zoals in hoofdstuk 2 is geschetst, is het cliëntenonderzoek een kernverplichting in de Wwft. Een belangrijk onderdeel van het cliëntenonderzoek is het identificeren van de klant (en waar relevant gerelateerde partijen zoals de UBO of juridisch vertegenwoordiger) en het verifiëren van diens identiteit. De ontwikkeling richting een digitale identiteit voor burgers en ondernemingen kan de onderzoekslast voor poortwachters verlagen, omdat poortwachters niet meer op individuele basis informatie bij klanten hoeven op te vragen, maar toegang kunnen krijgen tot de digitale identiteit wanneer klanten daar toestemming voor geven.(91)

De verordening betreffende elektronische identificatie en vertrouwensdiensten (eIDAS-verordening) is in 2014 ingevoerd om elektronische identificatie in Europa mogelijk te maken en grensoverschrijdende belemmeringen tussen nationale systemen weg te nemen.(92) In de verordening zijn onder andere afspraken neergelegd over het gebruik van de onderlinge digitale infrastructuur en betrouwbaarheidsniveaus. Momenteel wordt de eIDAS-verordening herzien. De Europese Commissie heeft voorgesteld om elke lidstaat te verplichten om een elektronische identiteit (e-ID) en minstens één digitale portemonnee ('wallet') te ontwikkelen die in de hele Europese Unie gebruikt moet kunnen worden.

(85) SEO 2022.
(86) SEO 2022, p. 26-27.
(87) Kamerstukken II, 2022/2023, 32 545, nr. 180.
(88) Consultatie voor de Wijzigingswet financiële markten 2024, 29 april 2022, beschikbaar via deze link.
(89) Kamerstukken II, 2022/2023, 32 545, nr. 180, p. 6.
(90) DNB 2022, p. 28.
(91) DNB 2022, p. 28.
(92) Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, *PbEU* L-257, p. 73-114.

De digitale portemonnee zou naast identiteitsgegevens ook andere informatie kunnen bevatten, zoals diploma's, adresgegevens en machtigingen voor vertegenwoordigers van rechtspersonen.[93] Via de digitale portemonnee kunnen personen zich identificeren en kunnen zij kiezen welke gegevens zij via de portemonnee willen delen. Een e-ID kan dus meer informatie dan uitsluitend de identiteitsgegevens bevatten. De informatie die wordt gedeeld kan worden afgestemd op de informatienoodzaak van de ontvangende instelling.

In paragraaf 4.3 en bijlage B wordt verder ingegaan op ontwikkelingen en initiatieven ten aanzien van digitale identiteiten binnen en buiten de Europese Unie.

2. Kunstmatige intelligentie

Kunstmatige intelligentie ('KI') is een koepelterm voor verschillende technieken waarbij machines vaardigheden zoals redeneren, plannen en leren kunnen inzetten (zoals bijvoorbeeld ook Machine Learning).

Waar sommige van deze technieken geschikt zijn om afwijkingen ten opzichte van een groep te vinden, kunnen andere technieken worden ingezet om te leren van eerder door een persoon gemaakte keuzes en bij toekomstige, gelijke situaties een inschatting te maken van welke keuze een persoon zou hebben gemaakt. Het potentiële voordeel van KI is dat het systeem een afwijking van een groep kan constateren – juist zonder de kennis te hebben over hoe personen hiertoe zouden komen – en zodoende dus nieuwe risico's kan detecteren. Tegelijkertijd kleeft aan dit potentiële voordeel ook een potentieel risico wanneer KI niet goed wordt uitgevoerd of gebaseerd is op kwalitatief slechte data, wat er bijvoorbeeld toe leidt dat het systeem (ongewenst) profileert en discrimineert.[94]

Hoewel uit een survey van KPMG uit 2023 blijkt dat de meeste mensen huiverig zijn om kunstmatige intelligentie te vertrouwen en KI een relatief lage mate van acceptatie heeft, wordt de potentie ervan voor de preventie van financieel-economische criminaliteit wel onderkend.[95] Hiermee zouden maatregelen sneller, goedkoper en effectiever kunnen worden.[96] Kunstmatige intelligentie wordt door de private sector in beperkte mate al gebruikt in het anti-witwasdomein, bijvoorbeeld op het gebied van klantrisicoanalyses of transactiemonitoring.[97] De FATF wijst onder andere op de mogelijkheid om risico's beter te identificeren.[98] De EBA wijst op het versnellen van cliëntenonderzoeken, alsook het verwerken van documenten.[99] De Wolfsberg Group onderkent dat instellingen met het steunen op kunstmatige intelligentie op meer holistische wijze de risico's van klanten en transacties kunnen beoordelen en monitoren.[100] In het rapport 'Van herstel naar balans' stelt DNB dat KI in potentie kan bijdragen aan effectievere en efficiëntere transactiemonitoring. DNB geeft daarbij wel aan dat de kwaliteit van data hoog moet zijn en dat adequate waarborgen moeten worden ingesteld, mede om onbewuste discriminatie te voorkomen.[101] Aanvullend op het gebruik voor transactiemonitoring, wijst KPMG nog op de mogelijkheden voor KI op het gebied van sanctiescreening.[102]

3. Blockchaintechnologie

Blockchain staat bekend als de techniek achter de cryptomunten, maar de techniek is breder toepasbaar. Blockchaintechnologie betreft technologie die kan worden gebruikt voor het transparant maken en automatiseren van processen. Steeds meer bedrijven maken gebruik van blockchaintechnologie voor het afhandelen van bijvoorbeeld financiële transacties en het ondersteunen van bepaalde kernprocessen. Met behulp van cryptografie wordt informatie versleuteld opgeslagen. Wat blockchaintechnologie bijzonder maakt, is dat informatie decentraal wordt opgeslagen. Dit betekent dat gegevens kunnen worden opgeslagen zonder de tussenkomst van een centrale autoriteit of onafhankelijke derde en controle. Het systeem is daarmee niet afhankelijk van één centrale database.

(93) DNB 2022, p. 29-30.
(94) Europees Parlement, *Artificiële intelligentie: Kansen en gevaren*, beschikbaar via deze link.
(95) KPMG 2023.
(96) FATF 2021, p. 4.
(97) Zie Institute of International Finance 2018; FATF 2021.
(98) FATF 2021, p. 24.
(99) EBA 2020, p. 20.
(100) Wolfsberg Group 2022a.
(101) DNB 2022.
(102) KPMG 2021.

In het kader van de bestrijding van witwassen en financieren van terrorisme kan de blockchaintechnologie een mogelijk geschikt middel zijn voor het (gedecentraliseerd) uitwisselen van informatie of het verifiëren van de identiteit van burgers en bedrijven. Het voordeel van de technologie is dat het beheer van informatie bij de 'eigenaar' van de informatie blijft.(103) Nadelen van blockchaintechnologie zijn de complexiteit en noodzaak voor specialistische kennis. Ook moeten alle partijen – vanwege afwezigheid van een centrale autoriteit – willen meewerken.

3.2.5 De ontwikkelingen van privacyregelgeving en de impact op de uitvoering van de Wwft en Sanctiewet

Sinds 25 mei 2018 is in de Europese Unie de Algemene verordening gegevensbescherming (AVG) van kracht.(104) De AVG – ook wel bekend onder de Engelse naam General Data Protection Regulation (GDPR) – heeft gezorgd voor een versterking en uitbreiding van de privacyrechten van betrokkenen. De verordening legt de nadruk meer dan voorheen op de verantwoordelijkheid van organisaties en bedrijven om aan te tonen dat zij de AVG naleven en heeft een strikter toezicht- en handhavingsregime geïntroduceerd. Door de invoering van de AVG en de toegenomen media-aandacht voor privacy-incidenten en datalekken bij publieke en private organisaties – zoals de Toeslagenaffaire of boete voor TikTok – staan privacy en het ethisch omgaan met persoonsgegevens hoog op de maatschappelijke agenda.(105) Ook is het bewustzijn omtrent privacy aanzienlijk toegenomen.(106) Een mogelijke verklaring hiervoor ligt in de verdere ontwikkelingen in de digitale transformatie die de samenleving doormaakt en waarbij de vraag steeds nadrukkelijker naar voren komt hoe verantwoord en/of ethisch alle technische ontwikkelingen zijn.(107) Ondanks de toegenomen aandacht voor het onderwerp, blijft het vertrouwen van Nederlanders in de omgang met privacy door bedrijven en overheidsorganisaties afnemen. Bovendien maakt meer dan de helft van de Nederlanders zich zorgen over de opkomst van kunstmatige intelligentie (zoals algoritmes) met betrekking tot hun privacy.(108)

De afgelopen jaren heeft ook de Nederlandse privacytoezichthouder, de Autoriteit Persoonsgegevens (AP), een steeds prominentere rol verworven. Zo heeft de AP in de afgelopen twee jaar meerdere zware boetes uitgedeeld.(109)

Daarnaast valt op dat de toezichthouder zich steeds vaker mengt in het publieke debat over initiatieven van de overheid met betrekking tot het verwerken van persoonsgegevens.(110) Dit resulteert in sommige gevallen in maatschappelijke discussies, zoals duidelijk het geval bij het wetsvoorstel Wet plan van aanpak witwassen.

Het spanningsveld tussen privacywetgeving, de Wwft en de Sanctiewet

Gezien het toenemende belang van, en de toenemende aandacht voor, privacy valt steeds vaker op dat de bescherming van privacy botst met andere belangen die de overheid heeft te behartigen. De botsing tussen de bescherming van privacy en andere belangen uit zich veelal bij de beginselen van proportionaliteit en subsidiariteit. Bij een beoordeling van de proportionaliteit en subsidiariteit wordt gekeken of inbreuken op de privacy in redelijke verhouding staan tot het na te streven doel, bijvoorbeeld het bestrijden van witwassen, en of er alternatieven zijn om hetzelfde doel te bereiken met middelen die een minder grote inbreuk maken op de privacy van betrokkenen.(111)

(103) Hier wordt verder aandacht aan besteed in hoofdstuk 4.
(104) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, *PbEU* L-119, p. 1-88.
(105) Autoriteit Persoonsgegevens, *Boete Belastingdienst voor discriminerende en onrechtmatige werkwijze*, 7 december 2021, beschikbaar via deze link; Autoriteit Persoonsgegevens, *Boete TikTok vanwege schenden privacy kinderen*, 21 juli 2021, beschikbaar via deze link.
(106) KPMG 2023a, p. 1.
(107) In dit kader valt in de context van het anti-witwasbeleid te wijzen op DNB, *Leidraad Wwft/Sw*, september 2022, beschikbaar via deze link, p. 57-58 waarin is opgenomen dat wanneer transactie-monitoringsystemen vormen van kunstmatige intelligentie gebruiken, de instelling een modelvalidatie of audit kan laten doen om te laten beoordelen of het systeem kwalitatief goed en effectief werkt. Zie tevens DNB's General principles for the use of Artificial Intelligence in the financial sector, waarin degelijkheid ('soundness'), verantwoordelijkheid ('accountability), eerlijkheid ('fairness'), ethiek, vaardigheden en transparantie genoemd worden: DNB 2019a.
(108) KPMG 2023a, p. 2.
(109) Zie het overzicht boetes en andere sancties op de website van de Autoriteit Persoonsgegevens, beschikbaar via deze link.
(110) Het is voor overheden verplicht op grond van artikel 36(4) AVG om de AP om advies te vragen bij het opstellen van nieuwe wet- en regelgeving waarbij de verwerking van persoonsgegevens aan de orde is.
(111) In artikel 5 AVG worden de verwerkingsbeginselen met betrekking tot persoonsgegevens neergelegd; daarbij spelen proportionaliteit en subsidiariteit een belangrijke rol in het kader van dataminimalisatie.

Het spanningsveld tussen de Wwft en privacyregelgeving heeft recentelijk de nodige aandacht gekregen.[112] Zo heeft het Europese Hof van Justitie in november 2022 een belangrijke uitspraak gedaan inzake toegang tot openbare registers met informatie over uiteindelijk belanghebbenden (UBO's).[113] Het Hof oordeelde in twee zaken dat de privacy van natuurlijke personen disproportioneel geschonden wordt door het algemene publiek toegang te geven tot UBO-registers, en verklaarde de Europese norm waarop dit is gebaseerd ongeldig.[114] Als gevolg van deze uitspraak is het UBO-register in Nederland (tijdelijk) niet meer te raadplegen, met uitzondering van bevoegde autoriteiten zoals opsporingsdiensten. In de consultatie van het conceptwetsvoorstel Wijzigingswet beperking toegang UBO-registers wordt voorzien in (gedeeltelijke) toegang tot het UBO-register voor poortwachters en instellingen die uitsluitend onder de RtSw 1977 vallen (waaronder schadeverzekeraars).[115]

Dit is niet de eerste keer dat privacy in het kader van het UBO-register ter discussie stond. In 2019 stelde de AP dat de noodzaak voor toegang tot het 'afgesloten' deel van het UBO-register voor Wwft-instellingen onvoldoende onderbouwd was, en dat voor andere financiële instellingen op grond van de Sanctiewet de beschrijving van de aard en omvang van de problematiek onvoldoende duidelijk was.[116] Eerder was de AP al kritisch op de toegang van drie aangewezen bijzondere opsporingsdiensten tot het afgesloten deel van het UBO-register, omdat de rol van deze autoriteiten in de bestrijding van witwassen volgens de AP onvoldoende onderbouwd was.[117]

Ook op Europees niveau roeren de privacytoezichthouders zich op het gebied van de preventie van witwassen en financiering van terrorisme. In het kader van het eerder genoemde EU AML Package hebben de privacytoezichthouders, verenigd in de Europese Toezichthouder voor gegevensbescherming (European Data Protection Supervisor, EDPS) al meerdere opinies en brieven gepubliceerd.[118] In de meest recente brief heeft de EDPS zich uitgesproken tegen het onderhandelingsmandaat van de Raad van de Europese Unie dat ziet op het toestaan van het delen van persoonsgegevens tussen private en publieke partijen in het kader van publiek-private samenwerkingsverbanden, alsook het delen van persoonsgegevens tussen poortwachters. De EDPS geeft aan serieuze zorgen te hebben over de rechtmatigheid, noodzaak en proportionaliteit van deze bevoegdheden. De EDPS stelt dat dit onvoldoende gemotiveerd is en niet wordt omkleed met de juiste waarborgen. Daarom adviseert de EDPS deze bepalingen niet op te nemen in de definitieve tekst van de AMLR.[119]

Impact privacywetgeving op wetsvoorstel Wet plan van aanpak witwassen

De privacydiscussie is ook duidelijk aanwezig in het kader van het wetsvoorstel Wet plan van aanpak witwassen waarmee wordt geprobeerd de Wwft effectiever te maken.[120] Zoals aangegeven in paragraaf 3.2.1 introduceert dit wetsvoorstel wijzigingen op de Wwft die zien op het door banken gezamenlijk monitoren van transacties.[121] Het wetsvoorstel voorziet in het gezamenlijk monitoren van alle zakelijke transacties en alle transacties tussen particulieren met een drempelwaarde van EUR 100. De rationale is dat banken op dit moment individueel transacties moeten monitoren en bepalen of deze ongebruikelijk zijn. Banken hebben geen zicht op de gehele transactieketen en ongebruikelijke transactiepatronen kunnen daardoor onopgemerkt blijven.[122] Ook is in dit wetsvoorstel de verplichting opgenomen voor poortwachters die behoren tot 'dezelfde categorie' om informatie te delen over geweigerde, verleende of beëindigde diensten aan klanten met een hoger risicoprofiel, om 'shopgedrag' te voorkomen.

(112) Bijvoorbeeld RUSI 2016; EBA 2020; FATF 2021; FATF 2021a; Lagerwaard 2022; FATF 2022; Ipenburg 2023; Nuijten 2023.
(113) Hof van Justitie EU, 22 november 2022, C-37/20 en C-601/20, ECLI:EU:C:2022:912 (*WM v Luxembourg Business Registers* en *Sovim v Luxembourg Business Registers*).
(114) Ministerie van Buitenlandse Zaken | Expertisecentrum Europees recht, 'EU-regeling voor onbeperkte toegang van het publiek tot informatie over de uiteindelijk begunstigden van vennootschappen is ongeldig', nieuwsbericht 2 december 2022.
(115) Zie het voorgestelde artikel 22a lid 1 Handelsregisterwet 2007 in de consultatie van de Wijzigingswet beperking toegang UBO-registers. Zie voor nadere toelichting tevens p. 14-19 van de bijbehorende concept-Memorie van toelichting. De consultatie voor de Wijzigingswet beperking toegang UBO-registers is op 30 mei 2023 gestart en is beschikbaar via deze link.
(116) Autoriteit Persoonsgegevens 2019b.
(117) Autoriteit Persoonsgegevens 2019a.
(118) EDPS 2020; EDPS 2021; EDPS 2023.
(119) EDPS 2023.
(120) Ipenburg 2023; Autoriteit Persoonsgegevens, 'Nieuwe wet opent deur naar ongekende massasurveillance door banken', persbericht 21 oktober 2022; Autoriteit Persoonsgegevens 2023; C. de Horde, R. Betlem, 'Felle verdeeldheid onder voor- en tegenstanders van nieuwe witwaswet', *FD* 26 januari 2023; Nuijten 2023, p. 146-147.
(121) Voor het gezamenlijk monitoren van transacties door banken is Transactie Monitoring Nederland B.V. (TMNL) opgericht. Zie paragraaf 4.2.1 en bijlage B.
(122) Kamerstukken II, 2022/2023, 36 228, nr. 3, p. 9-10.

De Autoriteit Persoonsgegevens heeft grote bezwaren tegen het wetsvoorstel. Volgens de AP opent het voorstel voor het gezamenlijk monitoren van transacties een deur *"naar ongekende massasurveillance door banken"* wat in de ogen van de AP neerkomt op een *"bancair sleepnet"*.[123] De AP heeft kenbaar gemaakt zorgen te hebben over de mate van inbreuk op de privacy van personen en meent dat het wetsvoorstel niet noodzakelijk en in strijd met het proportionaliteitsbeginsel is. In het position paper dat de AP heeft opgesteld als inbreng op het rondetafelgesprek met de Vaste Kamercommissie van Financiën van de Tweede Kamer, stelt de AP dat de surveillance kan leiden tot uitsluiting van personen tot het betalingsverkeer en dat er gevaar op ongerechtvaardigde discriminatie bestaat door de verwerking van bijzondere persoonsgegevens zoals ras, etniciteit en religie.[124] Het wetsvoorstel ligt momenteel ter behandeling bij de Tweede Kamer.

Impact privacywetgeving op het wetsvoorstel Wet gegevensverwerking door samenwerkingsverbanden

Het wetsvoorstel Wet gegevensverwerking door samenwerkingsverbanden (WGS) biedt een juridische basis voor de (systematische) verwerking van persoonsgegevens (waaronder profilering) door samenwerkingsverbanden.[125] Deze verbanden betreffen primair samenwerking tussen overheidsinstanties, en in beperkte mate tussen publieke en private partijen.[126] Het gaat bij de WGS om samenwerkingsverbanden die een zwaarwegend belang hebben bij het voorkomen en bestrijden van ernstige criminaliteit, grootschalig of systematisch ernstig gebruik van overheidsgelden en -voorzieningen, grootschalige of systematische ontduiking van wettelijke verplichtingen tot betaling van belastingen, retributies en rechten bij in- en uitvoer. Samenwerkingsverbanden die in het wetsvoorstel zijn opgenomen zijn het Financieel Expertise Centrum (FEC), de Infobox Crimineel en Onverklaarbaar Vermogen (iCOV), de Regionale Informatie en Expertisecentra (RIEC's) en de Zorg- en Veiligheidshuizen.[127]

Het wetsvoorstel is relevant voor een effectieve samenwerking en bestrijding van ernstige criminaliteit, waaronder ook financieel-economische criminaliteit. Ook hier toont het spanningsveld tussen criminaliteitsbestrijding enerzijds, en privacy anderzijds. De AP heeft meerdere kritische adviezen uitgebracht en opgeroepen om het wetsvoorstel in de voorgestelde vorm niet aan te nemen.[128]

Samengevat ziet de kritiek van de AP erop dat het doel van samenwerkingsverbanden om persoonsgegevens te delen en verwerken onvoldoende duidelijk omschreven is. Ook het moment van delen en verwerken acht de AP te vaag ('vage signalen') en ook de categorieën persoonsgegevens zijn te ruim. Net als bij het wetsvoorstel Wet plan van aanpak witwassen spreekt de AP hier van het risico op *"onbegrensde surveillance"*.[129]

Het voorgaande toont het spanningsveld tussen privacyregelgeving en het beschermen van de integriteit van de financiële sector c.q. het voorkomen en bestrijden van (financieel-economische) criminaliteit. Wat dit betekent voor poortwachters en klanten wordt verder uitgewerkt in de volgende paragraaf.

(123) Autoriteit Persoonsgegevens, 'Nieuwe wet opent deur naar ongekende massasurveillance door banken', persbericht 21 oktober 2022; Autoriteit Persoonsgegevens 2023.
(124) Autoriteit Persoonsgegevens 2023.
(125) Het huidige wetsvoorstel is op 17 december 2020 aangenomen door de Tweede Kamer en ligt momenteel voor goedkeuring bij de Eerste Kamer.
(126) Deelname door private partijen wordt strikt beperkt tot de private partijen die op dit moment aan FEC-PPS deelnemen: banken. Voor toetreding van nieuwe private partijen aan gereguleerde samenwerkingsverbanden zal een voorhangprocedure en bijzondere nahangprocedure bij de Eerste en Tweede Kamer gelden. Zie: consultatie voor het Besluit gegevensverwerking door samenwerkingsverbanden, 20 februari 2023, beschikbaar via deze link; Eerste Kamer, Memorie van Antwoord Regels omtrent gegevensverwerking door samenwerkingsverbanden, Kamerstukken I, 2022/2023, 35 447, K, p. 22-23.
(127) Het WGS voorziet in de mogelijkheid om andere samenwerkingsverbanden onder de werkingssfeer van de wet te brengen.
(128) Autoriteit Persoonsgegevens 2019c; Autoriteit Persoonsgegevens 2019; Autoriteit Persoonsgegevens, 'AP adviseert Eerste Kamer: neem WGS niet aan', persbericht 9 november 2021.
(129) Autoriteit Persoonsgegevens, 'AP adviseert Eerste Kamer: neem WGS niet aan', persbericht 9 november 2021.

3.3 De uitvoering in de praktijk en knelpunten

Hoofdstuk 2 heeft laten zien dat poortwachters vanuit de overheid een grote verantwoordelijkheid hebben gekregen bij het voorkomen van witwassen en financieren van terrorisme, en in het verlengde daarvan bij het 'schoonhouden' van het financiële stelsel. De achterliggende gedachte van deze responsabilisering van poortwachters is dat witwassen en terrorismefinanciering met de inzet van de private sector effectiever en efficiënter kan worden bestreden dan uitsluitend via de overheid.(130) In dit hoofdstuk worden knelpunten die een effectieve en efficiënte naleving van antiwitwaswetgeving in de weg staan, uiteengezet. Omdat een aantal ervaren knelpunten van poortwachters en klanten voortkomt uit, of samenhangt met, kritiek op de effectiviteit van het anti-witwasbeleid in algemene zin begint dit hoofdstuk met een uiteenzetting van enkele belangrijke kritiekpunten.

3.3.1 Kritiek op de effectiviteit van het anti-witwasbeleid

Onderzoek naar de effectiviteit van het anti-witwasbeleid door de jaren heen geeft een teleurstellend beeld: witwassen en terrorismefinanciering lijken ondanks ruim 30 jaar (uitdijend) beleid nog steeds een groot probleem te zijn.

Uit de literatuur kunnen enkele rode draden worden gehaald ten aanzien van de kritiek op de effectiviteit van het anti-witwasbeleid. Deze zien op (i) het afscheiden van het anti-witwasbeleid van de bredere strijd tegen (ondermijnende) criminaliteit, (ii) het gegeven dat witwassen voor het overgrote deel een internationaal fenomeen is maar vooral lokaal wordt bestreden, (iii) de onmeetbaarheid van de effecten van het beleid, (iv) de disbalans in de rollen en verantwoordelijkheden tussen overheid en de private sector en (v) de disbalans in de verplichtingen en bevoegdheden van poortwachters. Deze rode draden worden hierna beschreven.

1. Preventie van witwassen en terrorismefinanciering vs. bestrijden criminaliteit

Een eerste kritiekpunt dat uit de literatuur naar voren komt is dat het anti-witwasbeleid als het ware is losgekoppeld van de bredere criminaliteitsbestrijding, en dat dit een te nauwe focus met zich brengt.(131)

De oorzaak lijkt te liggen in het mandaat van de FATF, dat beperkt is tot de bestrijding van witwassen, terrorismefinanciering en proliferatie van massavernietigingswapens. Het gevolg is dat de beleidsdoelen van de FATF – en daarmee ook Europees en nationaal anti-witwasbeleid – zijn gericht op de beperkte lens van het tegengaan van de activiteit van witwassen in plaats van op het hogere, overstijgende doel van het voorkomen van criminaliteit.(132)

Er wordt – zeker ook in Nederland – onderkend dat de bestrijding van witwassen en terrorisme-financiering nauw samenhangt met het bredere vraagstuk van ondermijnende criminaliteit.(133) Echter, de juridische kaders, de betrokken partijen, en de rollen en verantwoordelijkheden van deze partijen binnen de respectievelijke kaders zijn anders. Dat maakt onderlinge afstemming op beleidsniveau ingewikkeld(er) doordat meer, en verschillende, belangen moeten worden behartigd. Voornoemde verschillen bemoeilijken ook op praktisch niveau een effectieve samenwerking tussen partijen, omdat elke partij een eigen (juridisch) kader heeft voor het verzamelen en gebruik van gegevens. Een overkoepelend kader dat ervoor zorgt dat partijen effectief en efficiënt met elkaar kunnen samenwerken om de eigen (en gezamenlijke) wettelijke doelstellingen te bereiken, ontbreekt momenteel.(134)

(130) Van Wingerde & Hofman 2022, p. 105; Alldridge 2016, p. 13-14.
(131) Pol 2018, p. 302-303; Reuter 2013, p. 224.
(132) Pol 2018, p. 303.
(133) Een voorbeeld betreft de brede inzet van tien Regionale Informatie- en Expertise Centra (RIEC's) en het Landelijk Informatie- en Expertise Centrum (LIEC) met aandacht voor drugscriminaliteit, mensenhandel en-smokkel, criminele motorbendes, fraude in het vastgoed en witwassen en financieel-economische criminaliteit.
(134) In het Coalitieakkoord 2021-2025, *Omzien naar elkaar, vooruitkijken naar de toekomst*, 15 december 2021, beschikbaar via deze link, geeft de regering bij het voornemen om de aanpak van ondermijning te versterken aan lessen te willen trekken uit de bestrijding van de maffia in Italië. Deze 'anti-maffia strategie' is een geïntegreerde aanpak met daarin de preventie van witwassen. Er bestaat daardoor een brede grondslag voor informatiedeling tussen (publieke) partijen.

2. Witwassen een internationaal fenomeen; de bestrijding is lokaal

Een tweede punt van kritiek betreft het feit dat de daadwerkelijke bestrijding van witwassen en terrorismefinanciering voornamelijk lokaal plaatsvindt. Hoewel de FATF globale standaarden heeft uitgevaardigd om witwassen, terrorismefinanciering en de proliferatie van massavernietigingswapens te bestrijden – en dit beleid dus is opgezet met de intentie een internationaal beleid te voeren – kent elk land door de omzetting van die standaarden een eigen nationaal kader. Dit maakt het anti-witwasbeleid vanuit globaal perspectief versnipperd, of zelfs *"an uneven playing field"*.(135) Witwassen is bij uitstek een globaal fenomeen kan dit alleen effectief worden bestreden met een daadwerkelijk internationale aanpak.(136)

3. Onmeetbaarheid van de effecten van het beleid

Ook bestaat er kritiek rondom de onmeetbaarheid van het anti-witwasbeleid. Deze kritiek is zowel gericht op de onbekendheid met de omvang van het probleem – met andere woorden: hoeveel wordt er witgewassen? – als op de outputzijde: welke doelstellingen heeft het beleid en zijn deze doelstellingen behaald?(137)

Hoewel er berekeningen bestaan van de omvang van het witwasprobleem, blijven dit veelal schattingen.(138) In 2006 werd in een onderzoek naar de aard en omvang van witwassen, verricht in opdracht van het ministerie van Financiën, opgemerkt dat de meeste literatuur over de effecten van de bestrijding van witwassen *"pure speculatie"* betreft en dat empirische data vaak ontbreekt.(139) Meer recente publicaties geven nog altijd aan dat betrouwbare schattingen ontbreken op zowel nationaal als internationaal niveau en in het recent gepubliceerde boek 'The war on dirty money' worden berekeningen van de omvang van witwassen nog altijd *"guesstimates"* genoemd.(140)

Verder draagt het gebrek aan concrete, specifieke doelstellingen in relatie tot het beschermen van de integriteit van het financiële stelsel c.q. het verminderen van criminaliteit bij aan de onmeetbaarheid van de effectiviteit van het beleid.(141) Uit vergelijkend onderzoek naar de doelstellingen van het anti-witwasbeleid in de Europese Unie blijkt ook dat verschillende landen met het anti-witwasbeleid andere doelen nastreven.(142) Ook wordt in de literatuur gewezen op de verschillende doelstellingen die door betrokken partijen worden nagestreefd met het anti-witwasbeleid: de publieke actoren richten zich primair op het pakken van criminelen door het volgen van de geldstromen, terwijl de private sector zich richt op de bescherming van (de reputatie van) het financiële stelsel.(143) In het derde onderzoek naar de bestrijding van witwassen, concludeert de Algemene Rekenkamer dat de ministers van Financiën en Justitie en Veiligheid nog altijd *"onvoldoende zicht hebben op de doelmatigheid en doeltreffendheid van hun aanpak van witwassen"* en dat dit komt *"omdat de ministers niet concreet hebben geformuleerd wat ze willen bereiken met hun aanpak"*.(144) Ook in de wetenschapstoets bij het recent ingediende wetsvoorstel Wet plan van aanpak witwassen is het gebrek aan meetbare doelen benoemd.(145)

4. Disbalans in rollen en verantwoordelijkheden publieke en private sector

Op basis van de responsabiliseringsgedachte zijn poortwachters medeverantwoordelijk gemaakt voor een van origine publieke taak, waarmee het zwaartepunt van het anti-witwasbeleid verschoven is van de publieke naar de private sector. Investeringen in mensen en middelen die door de private sector worden gedaan, vinden echter geen weerklank in het vervolg van de keten. Zo bestaat een grote discrepantie tussen de inzet aan mensen en middelen van de poortwachters in vergelijking met de publieke sector, en staan uitkomsten van het beleid ook niet in verhouding tot de middelen die er aan de voorkant in worden gestoken.(146)

(135) Verhage 2017, p. 485.
(136) R. Betlem en M. Rotteveel, 'Machine tegen witwassen draait niet', *FD* 10 januari 2023; RUSI 2018; 'The war against money laundering is being lost', *The Economist* 21 april 2021.
(137) Verhage 2017, p. 478-479; Levi, Reuter en Halliday 2017; Zavoli en King 2021, p. 29.
(138) RUSI 2019, p. 15; Levi, Reuter en Halliday 2017, p. 310 and 324.
(139) Unger et al. 2006, p. 102.
(140) Reuter 2013, p. 226; Levi, Reuter en Halliday 2017, p. 310; Gilmour en Hicks 2023, p. 49.
(141) Zie RUSI 2018; Amicelle 2017, p. 221.
(142) Unger et al 2013, p. 27.
(143) Amicelle 2017, p. 221-222.
(144) Algemene Rekenkamer 2022, p. 48.
(145) *Wetenschapstoets wetsvoorstel Plan van Aanpak Witwassen*, 20 januari 2023, beschikbaar via deze link.
(146) Rakké en Huisman 2020, p. 10. Zie bijvoorbeeld ook H.W. Smits en H. Rasch, 'Anti-witwasbeleid kost miljarden en levert weinig op', *FTM* 8 juli 2021; FD Redactioneel Commentaar, 'Banken voeren eenzame oorlog tegen witwassen', *FD* 25 oktober 2021.

Daarbij moet wel worden opgemerkt dat cijfers lastig door te vertalen zijn en weinig ruimte laten voor enige nuancering en contextualisering.[147]

Desalniettemin levert dit in zekere zin frustraties op aan de zijde van poortwachters. In een onderzoek van KPMG naar de vraag hoe leiders omgaan met risico's stelt een van de geïnterviewden: *"De Wwft is nou echt een voorbeeld van wetgeving voor de bühne. Jaarlijks zijn er 7.000 meldingen bij de Financial Intelligence Unit, die zouden moeten worden beoordeeld door 80 mensen. Het schiet zijn doel van het bestrijden van witwassen en terrorismefinanciering geheel voorbij en dit is niet bespreekbaar met De Nederlandsche Bank".*[148] Een bankbestuurder zegt daarover in hetzelfde onderzoek: *"Alleen al bij onze bank zijn er elke dag meer mensen bezig met compliancetaken om witwassen en terrorismefinanciering tegen te gaan dan dat er in Nederland politiemensen op straat lopen. Dat geeft te denken."* [149]

Ter illustratie: uit het DNB-rapport 'Van herstel naar balans' wordt voor uitsluitend de bankensector al opgemerkt dat de kosten voor het bestrijden van witwassen en terrorismefinanciering in 2021 in totaal 8% van de totale lasten van de vier grootste banken in Nederland betreft. Concreet gaat het om EUR 1,1 miljard en ruim 10.000 fte's. Voor de gehele sector bedroegen deze kosten rond de EUR 1,4 miljard in 2021 en komt het aantal ingezette fte's bijna op 13.000.[150] Daartegenover staat dat FIU-NL – die als 'cruciale spil in dit systeem' wordt aangemerkt *"omdat [FIU-NL] tussen de private en publieke actoren opereert"* – eind 2021 in totaal 82 fte's in dienst had op een budget van EUR 9 miljoen.[151] Overigens is deze informatie enigszins gedateerd: in 2023 is circa 100 fte's werkzaam bij FIU-NL en werkt FIU-NL toe naar uitbreiding tot circa 130 fte's gedurende het jaar.[152] Kijkend naar het eind van de keten blijkt uit het Jaaroverzicht criminele geldstromen 2022 van het OM dat in totaal op ruim EUR 246 miljoen crimineel vermogen beslag is gelegd in dat jaar.[153]

Het achterblijven van resultaten in de vorm van geconfisqueerd crimineel vermogen in vergelijking met de kosten en inzet van de private sector komt ook in internationale studies naar voren.[154] Ook de Algemene Rekenkamer merkt dit op. In het eerder aangehaalde onderzoek constateert de Rekenkamer dat *"opsporingsdiensten en het OM niet kunnen garanderen dat de meest risicovolle signalen nader onderzocht worden om te kijken of zij opvolging nodig hebben".* De Rekenkamer concludeert vervolgens dat er kansen zijn *"om witwassen doelmatiger en doeltreffender te bestrijden, zodat ook meer recht wordt gedaan aan de inspanningen van private partijen (…)".*[155]

De discussie over rollen en verantwoordelijkheden en de verdeling tussen de publieke en private sector, alsook over de effectiviteit van het anti-witwasbeleid, vindt niet alleen plaats in Nederland. In reactie op parlementair onderzoek naar de stand van zaken in het Britse anti-witwas- en sanctieregime in 2018 stelde UK Finance (de brancheverenigingen voor de financiële sector) dat in het huidige system te veel wordt geïnvesteerd in compliance-activiteiten die weinig bijdragen aan het detecteren van criminelen c.q. het beschermen van klanten. Bovendien leiden de toegenomen compliance- en rapportageverplichtingen niet tot een toename in het voorkomen van financieel-economische criminaliteit.[156] Het gevoerde anti-witwasbeleid heeft volgens UK Finance ook gevolgen voor financiële instellingen, met name voor kleinere partijen en nieuwe toetreders, die de snelheid van de veranderingen en administratieve lasten niet of nauwelijks kunnen bijbenen en stelt dat *"[t]hese demands are exacerbated by the absence of prioritisation on competing demands from the public sector on economic crime resource within the financial sector. Firms also note that whilst the financial sector has increased resource on economic crime, there has been a reduction in public sector resource in this area".*[157]

(147) Zie bijvoorbeeld Openbaar Ministerie 2022, p. 16 dat '(…) dat gepubliceerde cijfers met onvoldoende nuance worden gelezen'. Daarbij wijst het OM op onderscheid tussen transacties (meldingen) en dossiers (samenstel van meldingen) en het feit dat transacties verdacht worden verklaard op basis van reeds bestaande 'eigen opsporingsinformatie'. Uit het FIU Jaaroverzicht 2021 komt bovendien een duidelijk verschil tussen objectieve en subjectieve meldingen naar voren. Hoewel objectieve meldingen zeer relevant zijn als intelligence vindt verdachtverklaring in veel mindere mate plaats (FIU 2021, p. 7 en 10).
(148) KPMG 2022, p. 6.
(149) KPMG 2022, p. 25.
(150) DNB 2022, p. 15.
(151) Lagerwaard 2022, p. 147; FIU 2021, p. 32.
(152) Interview met FIU.
(153) Openbaar Ministerie 2022, p. 8.
(154) RUSI 2019, p. 16 verwijst naar schattingen door UNODC en Europol.
(155) Algemene Rekenkamer 2022, p. 47.
(156) UK Finance 2018, p. 1-2.
(157) UK Finance 2018, p. 2.

5. Disbalans in verplichtingen en bevoegdheden van poortwachters

Er wordt in de literatuur gewezen op het feit dat de Wwft een brede onderzoeksplicht met bijbehorende verplichtingen, maar geen bevoegdheden bevat.(158) Van poortwachters wordt verwacht dat zij 'de poort bewaken', maar poortwachters ervaren dat de middelen die ze hiertoe hebben in veel gevallen ontoereikend zijn.(159) Een van de geïnterviewden voor dit onderzoek benoemt dit als *"het bewaken van de poort met een klappertjespistool"*.

Om hun rol als poortwachter te kunnen vervullen, hebben poortwachters bevoegdheden nodig. Poortwachters missen echter soms bepaalde bevoegdheden om hun taak goed te kunnen vervullen, in het bijzonder voor de steeds zwaardere onderzoeksplicht die op hen rust. Uit de recente FATF-evaluatie van Nederland blijkt bijvoorbeeld dat veel poortwachters moeite hebben met het identificeren van UBO's omdat zij geen geschikte informatie hebben of kunnen raadplegen. Dat geldt in het bijzonder voor complexe (internationale) structuren.(160)

> *"Het voelt alsof we de poort bewaken met een klappertjespistool"*

Wettelijke bevoegdheden zijn vooral nodig waar poortwachters informatie moeten verzamelen die persoonsgegevens of anderszins privacygevoelige informatie bevatten.(161) Voorbeelden van bevoegdheden die poortwachters momenteel niet hebben maar dat voor de uitoefening van hun poortwachtersfunctie wel noodzakelijk achten, zien op het feit dat de meeste poortwachters geen toegang hebben tot de Basisregistratie Persoonsgegevens (BRP) en dat het UBO-register niet breed toegankelijk (en tijdelijk geheel niet toegankelijk) is voor poortwachters. Het UBO-register is een belangrijke bron van informatie voor poortwachters, maar ook voor partijen die uitsluitend onder de Sanctiewet vallen zoals schadeverzekeraars. Schadeverzekeraars vallen niet onder de Wwft en maken in het kader van onderzoek op grond van de Sanctiewet en de RtSw 1977 gebruik van de informatie uit het UBO-register.(162)

Vóór de situatie dat het UBO-register in het geheel gesloten werd, als gevolg van de uitspraak van het Europees Hof van Justitie(163), hadden poortwachters enkel toegang tot het openbare gedeelte van het register, terwijl het afgesloten gedeelte ook relevante informatie voor poortwachters bevatte.(164) Daarbij ging het bijvoorbeeld om de geboortedatum en -plaats en het woonadres van UBO's.(165) Ook het ontbreken van een zoekfunctie op naam in het Handelsregister is een doorn in het oog van meerdere poortwachters.(166) Soms is wel wet- en regelgeving in de maak, maar vaak duurt dit maanden of zelfs jaren. Een voorbeeld betreft het centraal aandeelhoudersregister: het initiatiefwetsvoorstel dateert uit 2017 en is anno 2023 nog altijd in behandeling in de Tweede Kamer.(167) Ook hier is door geïnterviewden de toegang tot het UBO-register genoemd als voorbeeld. Sinds het UBO-register is gesloten, zijn poortwachters in afwachting van spoedwetgeving die hen weer toegang kan geven. Het kabinet heeft aangegeven de spoedwet rond de zomer in te dienen bij de Tweede Kamer, ruim een half jaar na de uitspraak van het Europees Hof van Justitie.(168)

Specifiek met betrekking tot de Sanctiewet wordt gewezen op het feit dat sanctielijsten niet altijd volledig (genoeg) zijn, wat soms kan leiden tot onevenredige inspanning die instellingen moeten verrichten om voor een bepaalde relatie de structuur en zeggenschap te bepalen om naleving van de Sw te bewerkstellingen. Er is dan ook gesuggereerd dat een overheidsinstantie of opsporingsdienst de onderzoeken naar de structuur en UBO/zeggenschap zou kunnen verrichten. De uitkomsten van die onderzoeken zouden eventueel kunnen leiden tot aanvullende listings, waarop instellingen vervolgens mogen leunen.(169)

(158) Nuijten 2023, p. 144.
(159) Zie ook Hoogenboom 2021, p. 39-40; Nuijten 2023, p. 144.
(160) FATF 2022b, p. 126 en 129.
(161) Nuijten 2023, p. 144.
(162) Verbond van Verzekeraars, 'Meer duidelijkheid toegang UBO-register', nieuwsbericht 24 januari 2023.
(163) Hof van Justitie EU, 22 november 2022, C-37/20 en C-601/20, ECLI:EU:C:2022:912 (*WM v Luxembourg Business Registers* en *Sovim v Luxembourg Business Registers*).
(164) Nuijten 2023, p. 145.
(165) NVB 2019; Hoogenboom 2021, p. 40.
(166) Hoogenboom 2021, p. 40.
(167) Zie Eerste Kamer, *Initiatiefvoorstel-Nijboer en Alkaya Wet centraal aandeelhoudersregister*, beschikbaar via deze link.
(168) Op 30 mei 2023 is de consultatie voor de Wijzigingswet beperking toegang UBO-registers gestart, beschikbaar via deze link.
(169) Hoff en Hoff 2023, p. 11.

Het gebrek aan mogelijkheden om informatie over (gezamenlijke) cliënten te delen met andere poortwachters wordt eveneens als een beperking ervaren.(170)

Tot slot blijkt uit interviews verricht in het kader van dit onderzoek dat poortwachters niet de ruimte voelen om te kunnen steunen op werkzaamheden die andere poortwachters reeds hebben verricht, hoewel dit juridisch is toegestaan (dat wil zeggen: het introducerend cliëntenonderzoek).(171) Poortwachters geven aan dat het dusdanig veel inspanning vereist om aan te kunnen tonen dat zij mogen vertrouwen op het beleid en de processen van de introducerende instelling, dat het efficiënter is om zelf het cliëntenonderzoek te verrichten.

De disbalans in verplichtingen en bevoegdheden van poortwachters – of het gebrek aan adequate bevoegdheden in het licht van de uitgebreide onderzoeksplicht – resulteert ook concreet in enkele knelpunten voor poortwachters. Deze komen in de paragraaf hierna aan de orde.

3.3.2 Knelpunten ervaren door poortwachters

Poortwachters hebben een rol en verantwoordelijkheid opgelegd gekregen in het bewaken van de integriteit van de financiële sector en – zoals uit voorgaande blijkt – is de effectiviteit van de bijdrage van alle inspanningen aan het daadwerkelijk voorkomen van financieel-economische criminaliteit niet vast te stellen. Dit maakt dat het draagvlak voor naleving van verplichtingen niet vanzelfsprekend is.(172) De uitvoering van de poortwachtersrol brengt op hoofdlijnen vier knelpunten met zich mee die in deze paragraaf uiteen worden gezet. Daarbij gaat het om het spanningsveld tussen commerciële belangen en de poortwachtersfunctie, conflicten in wet- en regelgeving, een beperkte ondersteuning door de overheid en het feit dat de poortwachtersrol onder een vergrootglas ligt.

1. Uiteenlopende belangen

Er bestaat een spanningsveld tussen enerzijds de commerciële belangen van private organisaties, inclusief hun klantrelaties, en anderzijds het publieke belang een bijdrage te leveren aan het voorkomen van financieel-economische criminaliteit.(173) Die belangen zijn nauw met elkaar verweven: hoge boetes door toezichthouders en reputatieschade hebben impact op de commerciële resultaten. Dit spanningsveld wordt door Van Wingerde en Hofman ‘de existentiële spagaat’ genoemd.(174) Uit onderzoek blijkt dat het commerciële belang een belangrijke rol speelt bij de keuze van poortwachters om ongebruikelijke transacties te melden. Het spanningsveld tussen het commerciële belang en het voorkomen van financieel-economische criminaliteit komt veelal naar voren in interne discussies tussen ‘de business’, waar het commerciële belang de boventoon voert, en de complianceafdelingen van organisaties.(175) In aanvulling op het publieke belang ten aanzien van het voorkomen van financieel-economische criminaliteit hebben poortwachters ook nog te maken met maatschappelijke verwachtingen. Zo wordt van banken in toenemende mate een actieve bijdrage verwacht aan breed gedragen maatschappelijke ambities op het gebied van onder meer duurzaamheid, klimaat, milieu, gezondheid, mensenrechten en governance.

Het spanningsveld tussen commerciële belangen enerzijds, en de uitvoering van de poortwachtersrol – soms nog aangevuld met maatschappelijke verwachtingen – anderzijds, geldt in principe voor alle poortwachters.(176) Commerciële druk kan door kleine poortwachters als hoger worden ervaren, omdat zij afhankelijker zijn van een kleinere groep klanten of meer moeten concurreren met grotere partijen en doorgaans over relatief minder financiële en personele middelen beschikken om uitvoering te geven aan de Wwft.(177) De afweging tussen commerciële en publieke belangen heeft ook impact op investeringen die worden gedaan om Wwft-compliant te zijn. De administratieve lasten en kosten van naleving van de Wwft worden door poortwachters als enorm ervaren, en stijgen verder door toename van de verplichtingen.(178)

(170) Kamerstukken II, 2022/2023, 36 228, nr. 3, p. 4. Zie ook Wolfsberg Group 2022, p. 1.
(171) Artikel 5, eerste lid, Wwft.
(172) Van Wingerde en Hofman 2022, p. 16.
(173) Van Wingerde en Hofman 2022, p. 16; Rakké en Huisman 2020, p. 8; Stichting Maatschappij en Veiligheid 2022, p. 33-34.
(174) Van Wingerde en Hofman 2022, p. 67.
(175) Rakké en Huisman 2020, p. 8-9.
(176) Yeoh 2020; Van Wingerde en Hofman, p. 69; Hoogenboom 2021, p. 39.
(177) Van Wingerde en Hofman 2022, p. 69; EY 2021, p. 47.
(178) Hoogenboom 2021, p. 40; Zavoli en King 2021, p. 26.

Vanwege de risicogebaseerde benadering en daarbij behorende open normen is het bovendien niet altijd op voorhand duidelijk wanneer een instelling over voldoende kwaliteit en kwantiteit van personeel en technologische middelen beschikt om onregelmatigheden te detecteren. Ook kan commerciële druk als knelpunt worden ervaren voor het delen van informatie tussen poortwachters, namelijk als het delen van informatie als een competitief voordeel voor de andere partij wordt gezien doordat zichtbaar wordt welke klanten een partij bedient of dat een van de twee partijen het cliëntenonderzoek heeft verricht met de daarbij behorende kosten.(179)

Uit onderzoek van Nyenrode Business Universiteit blijkt dat het draagvlak voor de Wwft en de poortwachtersrol bij makelaars/taxateurs en notarissen toeneemt.(180) Tegelijkertijd worden de kernbepalingen van de Wwft nog niet altijd goed nageleefd. Onderzoekers spreken van 'opstandige betrokkenheid'(181) van individuele beroepsbeoefenaars en noemen als een van de oorzaken commerciële belangen. Onderzoekers stellen dat er grijze gebieden zijn *"waarin de context van de zakelijke relaties, de deal en de commerciële belangen variëren. Afhankelijk van die wisselende contexten worden beslissingen genomen die niet altijd worden ingegeven door de normativiteit van de Wwft".*(182) Andere oorzaken zijn te vinden in de (gepercipieerde) complexiteit van de Wwft en andere regelgeving en het ontbreken van adequate bevoegdheden om de poortwachtersrol te kunnen vervullen.(183) Op conflicten in wet- en regelgeving en de ondersteunende rol van de overheid wordt verder in deze paragraaf ingegaan.

Hoewel geen literatuur bekend is die ingaat op het spanningsveld tussen de commerciële belangen van poortwachters en de naleving van de Sanctiewet, kan hier mogelijk tot op zekere hoogte een parallel worden getrokken met de Wwft. Ook de naleving van de Sanctiewet brengt een zekere onderzoeksplicht – en daarmee kosten – met zich mee; in het bijzonder voor de poortwachters die aan de RtSw 1977 moeten voldoen en onder toezicht staan. En ook hier geldt dat boetes en andere vormen van handhaving van de toezichthouder impact kunnen hebben op commerciële resultaten en/of de reputatie.

2. Conflicterende wet- en regelgeving

Een ander knelpunt betreft het bestaan van conflicterende belangen tussen verschillende wet- en regelgeving of in relatie tot de professionele verantwoordelijkheid van de verschillende poortwachters. Zo zijn notarissen in beginsel verplicht werkzaamheden die uit de wet voortvloeien uit te voeren, de zogenaamde ministerieplicht.(184) Weigering mag alleen indien de werkzaamheden naar de redelijke overtuiging of het vermoeden van de notaris in strijd zijn met het recht of de openbare orde, wanneer zijn medewerking wordt verlangd bij handelingen die kennelijk een ongeoorloofd doel of gevolg hebben of wanneer hij andere gegronde redenen voor weigering heeft.(185) Het werkelijke doel van de dienstverlening is echter niet altijd te achterhalen, waardoor de grens tussen het moeten verlenen van notarisdiensten en het staken van dienstverlening op grond van vermoedens van witwassen diffuus is.(186)

Een breder conflict tussen wetgeving van sommige beroepsbeoefenaars en de Wwft betreft de vertrouwelijkheid en geheimhouding in de cliëntrelatie. De geheimhouding is een fundamentele waarde bij de beroepsuitoefening van advocaten, notarissen en accountants en kan in afgeleide vorm ook van toepassing zijn op belastingadviseurs. Deze geheimhouding kan op gespannen voet staan met de vereiste openheid en transparantie voor het vastleggen van gegevens en het melden van ongebruikelijke transacties op grond van de Wwft.(187) De geheimhouding staat ook op gespannen voet met (Europese) sanctieverplichtingen. Vanwege de geheimhoudingsplicht is er momenteel voor gekozen om geen meldplicht op te leggen aan het notariaat, de advocatuur en accountancy.(188)

(179) Maxwell 2021, p. 9.
(180) Hoogenboom 2021, p. 64.
(181) Hoogenboom 2021, p. 37.
(182) Hoogenboom 2021, p. 64.
(183) Hoogenboom 2021, p. 110-111.
(184) Van Wingerde en Hofman 2022, p. 75.
(185) Art. 21 lid 2 Wet op het notarisambt.
(186) FATF 2022b, p. 128; Van Wingerde en Hofman 2022, p. 75.
(187) Van Wingerde en Hofman 2022, p. 16.
(188) Nationaal coördinator sanctienaleving en handhaving 2022, p. 13.

Nederland heeft de Europese Commissie verzocht deze geheimhoudingsplicht te doorbreken ten behoeve van een sanctiemeldplicht. In het kader van de modernisering van het sanctiestelsel wordt ook onderzocht of dit op nationaal niveau kan worden geregeld.(189) Poortwachters die tegelijkertijd ook geheimhouders zijn ervaren een tweestrijd bij de toepassing van de geheimhouding enerzijds en meldplichten anderzijds, beide ingegeven vanuit hun rol en verantwoordelijkheden.(190) Ook botst de professionele geheimhouding met de wens om in het kader van de bestrijding van financieel-economische criminaliteit meer informatie binnen de beroepsgroep en met andere poortwachters uit te wisselen.(191)

"Er zit momenteel een privacyslot op de criminaliteitsbestrijding in Nederland"

Tevens bestaat een inherent spanningsveld tussen privacy en de bestrijding van witwassen en terrorismefinanciering. In dit kader stelt de FATF dat beide een belangrijk publiek belang behartigen: *"both serve important objectives, including upholding human rights and fundamental freedoms (such as the right to privacy) and protecting the public from criminal activities, including terrorism. These interests are not in opposition nor inherently mutually exclusive".*(192) De FATF stelt dat een effectief anti-witwasbeleid veronderstelt dat de publieke en private sector zowel de vereisten uit de anti-witwasregelgeving als de privacyregelgeving naleven. De privacywetgeving, en in het bijzonder de rol van de Autoriteit Persoonsgegevens in het maatschappelijk debat in Nederland, worden ook in interviews verricht in het kader van dit onderzoek veelvuldig aangehaald als een grote beperkende factor op de uitvoering van de Wwft. In een van de interviews werd door geïnterviewden gesteld dat er momenteel *"een privacyslot zit op de criminaliteitsbestrijding in Nederland"*.

Het spanningsveld tussen de bescherming van privacy van burgers en bedrijven enerzijds, en effectieve criminaliteitsbestrijding anderzijds komt duidelijk naar voren bij het wetsvoorstel Wet plan van aanpak witwassen dat juist de effectiviteit van de Wwft beoogt te vergroten door meer informatie-uitwisseling, zoals uitgewerkt in paragraaf 3.2.5.

Ook bestaat een spanningsveld tussen de zorgplicht van financiële instellingen op grond van de Wet op het financieel toezicht (Wft) en de naleving van de Wwft.(193) Om de integriteitsrisico's beheersbaar te houden of om invulling te geven aan de maatschappelijke verwachtingen of de eigen ambities op het gebied van duurzaamheid, klimaat, milieu, gezondheid, mensenrechten en governance, besluiten financiële instellingen om (sommige) klanten met een hoger risicoprofiel te weigeren of beperkte diensten te verlenen.(194) Op grond van de algemene zorgplicht kunnen zij echter in sommige gevallen de relatie niet weigeren of beëindigen, omdat de gevolgen onevenredig zijn voor klanten. Dit kan het geval zijn wanneer de klant geen alternatief kan vinden en met het opzeggen van de relatie de toegang tot het betalingsverkeer wordt ontzegd. Dat geldt in het bijzonder voor natuurlijke personen, die een recht op een bankrekening hebben.(195) Uit jurisprudentie blijkt dat het weigeren of opzeggen van dienstverlening vanwege risico's op witwassen en terrorismefinanciering op gespannen voet kan staan met (de plicht tot) het verschaffen van toegang tot de financiële sector.(196)

Recentelijk stelde de Nationaal Coördinator tegen Discriminatie en Racisme nog dat banken en financiële instellingen moslims structureel discrimineren als gevolg van de toepassing van de Wwft.(197) Van poortwachters wordt verwacht dat zij risicogebaseerd onderzoek doen en dat zij ongebruikelijke transacties identificeren en melden. Daarbij verwerken zij informatie over klanten en transacties. Ook in het kader van de naleving van de Sanctiewet kan het voorkomen dat instellingen nadere informatie opvragen.(198)

(189) Nationaal coördinator sanctienaleving en handhaving 2022, p. 13; Brief minister van Buitenlandse Zaken over de stand van zaken rondom sanctienaleving, het toezicht daarop en de handhaving daarvan: Kamerstukken II, 2022/2023, 36 045, nr. 120, p. 3; Hoff en Hoff 2023, p. 8.
(190) Zie voor de relatie geheimhouding en Wwft-verplichtingen: Van Wingerde en Hofman 2022, p. 72-73.
(191) Ipenburg 2023, p. 27.
(192) FATF 2022, p. 3.
(193) Nuijten 2023, p. 145.
(194) NVB 2022a, p. 15.
(195) Dit betreft de basisbetaalrekening op grond van artikel 4:71f Wft. Tot op heden bestaat een dergelijk recht niet voor rechtspersonen.
(196) Zie bijvoorbeeld: Gerechtshof Amsterdam, 21 januari 2020, ECLI:NL:GHAMS:2020:121; Rb. Amsterdam, 5 januari 2022, ECLI:NL:RBAMS:2022:42; Rb. Amsterdam, 15 juni 2022, ECLI:NL:RBAMS:2022:3871; Rb. Amsterdam, 14 september 2022, ECLI:NL:RBAMS:2022:5340.
(197) 'Racismecoördinator: 'Structurele discriminatie van moslims bij banken', *NOS.nl* 6 april 2023, NVB, 'Openheid en transparantie in uitvoering anti-witwaswet', nieuwsbericht 6 april 2023.
(198) Zie bijvoorbeeld College voor de Rechten van de Mens, 'Verzoek geweigerd – Mogen banken klanten afwijzen op grond van nationaliteit?', nieuwsbericht 4 april 2023.

Tot slot ervaren makelaars nog een ander conflict in wet- en regelgeving. Op grond van het Burgerlijk Wetboek is het makelaars verboden om tweezijdig te bemiddelen, dat wil zeggen: om namens zowel de koper als de verkoper op te treden.(199) Tegelijkertijd rust op de makelaar de plicht om onderzoek te doen naar de zakelijke relatie c.q. de (vastgoed)transactie. Om te kunnen beoordelen of een transactie ongebruikelijk is of niet, of dat een transactie wordt gebruikt om sancties te omzeilen, is het voor makelaars noodzakelijk om onderzoek te doen naar de wederpartij. Met het oog op potentiële schade voor de onderhandelingspositie blijken wederpartijen in de praktijk vaak terughoudend in het verstrekken van de benodigde informatie over de omvang en de herkomst van de eigen middelen.(200) Ook leidt dit – wanneer de koper en verkoper elk een eigen makelaar hebben – tot de situatie dat beide makelaars elkaars klanten betrekken in hun eigen cliëntenonderzoeken. Daarmee worden onderzoek 'dubbelop' gedaan. De leidraad van de Belastingdienst/Bureau Toezicht Wwft geeft aan dat makelaars het onderzoek naar de wederpartij kunnen uitbesteden aan de notaris (wanneer deze de koopakte opstelt) of aan de eigen cliënt; hoewel dit laatste een potentieel hoger risico met zich brengt wat extra maatregelen van de makelaar vereist. In het geval van betrokkenheid van meerdere makelaars geeft de leidraad aan dat de makelaars de respectievelijke cliëntenonderzoeken bij de wederpartij aan elkaar kunnen uitbesteden.(201)

3. Beperkte ondersteuning door overheid

In een systeem waarbij (steeds grotere) waarde wordt gehecht aan de poortwachtersfunctie verricht door private partijen, is het belangrijk dat de overheid diezelfde poortwachters ook in staat stelt om hun rol effectief en efficiënt te kunnen vervullen. Met een ondersteunende overheid wordt in dit onderzoek gedoeld op het creëren van juiste randvoorwaarden voor de taakuitoefening van poortwachters. Uit interviews verricht in het kader van dit onderzoek blijkt dat poortwachters zich momenteel onvoldoende gesteund voelen om hun rol op effectieve wijze te vervullen door de overheid die hen de poortwachtersrol heeft toebedeeld en in dat kader steeds meer van hen verwacht. Eerder in dit rapport is al gewezen op de disbalans tussen de verplichtingen in bevoegdheden en verantwoordelijkheden van poortwachters (paragraaf 3.3.1), maar ook de fragmentatie en gebrek aan prioritering van overheidsbeleid en een gebrek aan guidance en feedback voeden dit gevoel aan de private zijde.

Fragmentatie en gebrek aan prioritering van overheidsbeleid

Poortwachters hebben te maken met veel verschillende overheidspartijen: binnen het anti-witwasbeleid, bij de sanctieregelgeving, en bij de bredere aanpak van georganiseerde criminaliteit.(202) In Nederland valt te denken aan verschillende departementen (bijv. ministerie van Financiën, ministerie van Justitie en Veiligheid, ministerie van Binnenlandse Zaken), Wwft-toezichthouders, andere toezichthouders zoals de Autoriteit Persoonsgegevens en Autoriteit Consument en Markt, FIU-NL, het OM en opsporingsdiensten (politie, FIOD, Koninklijke Marechaussee), overheidsdiensten (Douane), gemeenten en andere instanties met overheidstaken (Kadaster en KVK). Al deze partijen hebben een eigen taak in het kader van de bestrijding van ondermijning en/of financieel-economische criminaliteit, en hebben daarmee hun eigen belangen te behartigen. Uit interviews komt het beeld naar voren dat er veel wordt 'gepolderd' tussen deze partijen en hun belangen. Als gevolg van de versnippering aan de zijde van de overheid ontbreekt duidelijk eigenaarschap voor en sturing van het anti-witwas- en sanctiebeleid.(203) Prioriteiten worden niet vastgesteld of eenduidig gecommuniceerd naar de private sector.(204)

Het gebrek aan duidelijk eigenaarschap en sturing betreft een knelpunt tot op het hoogste niveau binnen de overheid.

(199) Artikel 7:427 jo. 7:417 Burgerlijk Wetboek.
(200) Hoogenboom 2021, p. 41.
(201) Belastingdienst Bureau Toezicht Wwft, *Leidraad Wwft voor makelaars, bemiddelaars en taxateurs onroerende zaken*, maart 2022, beschikbaar via deze link, p. 39.
(202) Verhage 2017, p. 480 noemt dit de *'AML complex'*; Hoff & Hoff 2023, p. 7.
(203) RUSI 2019, p. 19-20; Nationaal coördinator sanctienaleving en handhaving, 2022, p.15.
(204) Dit probleem beperkt zich niet tot Nederland. Ook in het Verenigd Koninkrijk is opgemerkt dat het anti-witwasbeleid in het Verenigd Koninkrijk *"underpowered, poorly coordinated"* is en dat het strategisch toezicht en visie mist: RUSI 2018.

Zo komt uit interviews verricht in het kader van dit onderzoek de duidelijk gedeelde wens naar voren dat de overheid een duidelijke keuze maakt tussen privacy en de bestrijding van criminaliteit en zal moeten accepteren dat het toekennen van een groter belang aan één belang een beperking met zich meebrengt aan het andere belang. Zolang die keuze niet wordt gemaakt kunnen er geen of slechts beperkte stappen worden gezet in het terugdringen van witwassen, terrorismefinanciering en andere criminaliteit.

Gebrek aan guidance en feedback

Bij poortwachters leeft de behoefte om een beter begrip te krijgen van de daadwerkelijk grootste bedreigingen voor de integriteit van de financiële sector. Overheden zijn verplicht om de risico's op witwassen en terrorismefinanciering te identificeren, te analyseren, te begrijpen en te mitigeren, en dienen hun risicobeoordelingen actueel te houden.(205) Veelal vullen overheden deze in via National Risk Assessments (NRA's). Uit onderzoek blijkt dat NRA's zich nog in een vroeg stadium bevinden: *"they lack conceptual clarity, the data are highly limited, most are analytically weak or fail to explain the methodology, and the whole goal of the NRA – to inform policy decisions – is often missed or at least not made explicit in the published version".*(206) Anderen stellen dat NRA's mede vanwege hun generieke aard weinig bruikbaar zijn als basis voor risicogebaseerd anti-witwasbeleid.(207) Uit interviews met meerdere poortwachters komt naar voren dat de Nederlandse NRA's op dit moment onvoldoende concrete handvatten bieden voor de poortwachters. Zo ervaren zij dat risico's aan hele sectoren of activiteiten worden opgehangen, zonder te duiden waar de risico's echt zitten of hoe via die weg kan worden witgewassen. Andere geïnterviewden geven aan dat de NRA een leerproces is en inderdaad een verdiepingsslag kan gebruiken; tegelijkertijd wijzen zij op de rol van poortwachters in het aanleveren van informatie die de NRA kan versterken.

Ook bestaat behoefte aan gecoördineerde guidance van en continue dialoog met de Wwft/Sw-toezichthouders, bijvoorbeeld inzake gedeelde thematiek waar meerdere poortwachters bij betrokken zijn (bijvoorbeeld vastgoed) en waarin duidelijk wordt ingegaan op situaties waar vanuit risicoperspectief een hogere inzet van poortwachters wordt verwacht en in het bijzonder waar minder mogelijk is en mag.(208) Vooral het laatste lijkt belangrijk; uit interviews komt naar voren dat, hoewel risicogebaseerde normen op papier tot minder regels leiden, poortwachters in de praktijk toch vaak meer doen dan strikt noodzakelijk, omdat niet op voorhand duidelijk is wanneer aan de risico-inspanning wordt voldaan of wat (concreet) de verwachting is van de toezichthouder.(209)

Het voeren van een continue dialoog tussen poortwachters en toezichthouders over adequate risicobeoordeling en -beheersing wordt als een waardevolle aanvulling beschouwd op het toezicht dat achteraf op poortwachters plaatsvindt.(210) In dit opzicht kan het initiatief van DNB uit 2022 om rondetafelgesprekken te organiseren met banken en sectoren die hinder ondervinden van anti-witwasmaatregelen over de risicogebaseerde benadering van de Wwft en de inzet van innovatieve middelen als een positieve ontwikkeling worden beschouwd.(211) Op basis van deze rondetafelgesprekken zijn in mei 2023 de eerste vijf NVB Standaarden gepubliceerd.(212)

Verder blijkt uit de literatuur en de interviews verricht in het kader van dit onderzoek dat poortwachters behoefte hebben aan een effectieve feedbackloop vanuit FIU-NL, opsporing en toezichthouders.(213) Deze feedbackloop is belangrijk voor het lerend vermogen van organisaties en om de kwaliteit van meldingen te verhogen. Wanneer deze feedback ontbreekt kan dit impact hebben op de motivatie van poortwachters om te melden.(214)

(205) FATF-aanbeveling 1 en artikel 7 AMLD5. Deze verplichting is in artikel 1f Wwft geïmplementeerd. Op grond van de Wwft dient de Nederlandse NRA elke twee jaar te worden geactualiseerd.
(206) Ferwerda en Reuter 2022, p. 22.
(207) Gilmour en Hicks 2023, p. 132-133.
(208) Zie bijv. Zavoli en King 2021, p 26 en p. 28.
(209) Nuijten 2023, p. 145. Zie ook verder in deze paragraaf.
(210) NVB 2022a, p. 24.
(211) DNB, 'Partijen voortvarend van start met gerichte risicogebaseerde witwasaanpak', nieuwsbericht 23 november 2022.
(212) NVB, 'Minder klantimpact door NVB Standaarden voor risicogebaseerd witwasonderzoek', persbericht 30 mei 2023. De NVB Standaarden zijn gemaakt in overleg met de toezichthouder De Nederlandsche Bank (DNB) en het ministerie van Financiën.
(213) Rakké en Huisman 2020, Van Wingerde en Hofman 2022, Zavoli en King 2021, p. 42, Algemene Rekenkamer 2022, p. 32, Stichting Maatschappij en Veiligheid 2022, p. 32, FATF 2022b, p. 121, 123 en 140; Wolfsberg Group 2022, p. 1; Verhage 2017, p. 482.
(214) Rakké en Huisman 2020, p. 11.

In het Jaaroverzicht Criminele Geldstromen 2022 meldt het OM dat het samen met de FIOD, FIU-NL en politie binnen de verdachte transactie (VT)-werkgroep werkt aan: *"betere dossieroverdracht van VT's aan opsporing, meer inzicht in gebruik en bruikbaarheid van VT's, versterken van de feedbackloop en betere ketensamenwerking"*.(215) In de eerste helft van 2023 is de bankensector ook aangesloten bij deze werkgroep.

Een ander knelpunt gerelateerd aan het doen van meldingen bij FIU-NL betreft de angst voor represailles. Wanneer meldingen van ongebruikelijke transacties door poortwachters leiden tot, of worden meegenomen in, een strafrechtprocedure, worden de naam en andere gegevens van de meldende instelling bekend bij de verdachte, door opname van deze gegevens in het strafdossier. Uit literatuur, alsook interviews verricht in het kader van dit onderzoek, blijkt dat dit poortwachters ervan kan weerhouden belangrijke meldingen te doen uit angst dat zij door de onderwereld worden aangepakt, zeker in combinatie met de verharding in de georganiseerde criminaliteit.(216) Daar zijn sinds 2020 al enkele maatregelen voor genomen. FIU-NL stelt alleen de naam van de organisatie ter beschikking aan opsporing wanneer een ongebruikelijke transactie verdacht wordt verklaart. Ook neemt de opsporing altijd contact op met melders wanneer het voornemen bestaat om een melding in het strafdossier op te nemen om te bepalen of er bepaalde dreigingsrisico's jegens de melder zijn. Ook kan de melder aangifte doen of contact opnemen met de politie. In uitzonderlijke gevallen kunnen de gegevens in het strafdossier worden geanonimiseerd. Desalniettemin blijft in het bijzonder de groep 'kleine' poortwachters dit als een knelpunt ervaren, zo blijkt uit interviews. Het gevoel heerst dat waar de poortwachters een door de overheid opgelegde plicht hebben om te melden, diezelfde overheid de plicht heeft om melders te beschermen.

In mei 2023 heeft de minister van Justitie en Veiligheid in antwoord op Kamervragen aangekondigd verschillende oplossingen te verkennen om (het gevoel van) veiligheid van melders te versterken.(217) Hierbij geeft de minister aan dat het *"ook van belang [is] om, naast de verkenning van aanvullende maatregelen om de veiligheid en het gevoel van veiligheid onder poortwachters te versterken, nog beter te communiceren over onder meer het nut en belang van de meldingsplicht en de al bestaande waarborgen"*.(218)

4. Poortwachtersrol onder vergrootglas

De disbalans tussen bevoegdheden en verplichtingen in combinatie met de ervaring van een beperkte ondersteuning door de overheid wordt nog verder versterkt door het risico voor poortwachters om zelf hard aangepakt te worden wanneer zij, naar de mening van diezelfde overheid, hun poortwachtersrol niet of niet voldoende vervullen.(219) Dit betreft zowel bestuurs- of tuchtrechtelijke handhaving door de toezichthouders als de strafrechtelijke handhaving door het OM. Zonder direct betrokken te zijn geweest bij witwassen of financiering van terrorisme zijn er gevallen geweest waarin poortwachters strafrechtelijk zijn aangepakt voor het niet goed vervullen van hun poortwachtersrol.(220) Volgens Nuijten wekt dit de indruk *"dat de speciale en generale preventieve werking van bestraffing van poortwachters groter wordt geacht dan van bestraffing van witwassers"*.(221)

Een hiermee samenhangende relevante ontwikkeling betreft ook de toegenomen focus op de rol van bestuurders: op grond van de regelgeving wordt steeds meer gekeken naar de kwaliteit en verantwoordelijkheden van bestuurders (zowel individueel als collectief) en andere personen met een sleutelpositie in het anti-witwasbeleid van poortwachters.(222)

(215) Openbaar Ministerie 2022, p. 15.
(216) Hoogenboom 2021, p. 39 en p. 136; K. van Doorne, 'Met knikkende knieën ongebruikelijke transacties melden? Dat kan toch niet', column *VNO-NCW*, 5 april 2023.
(217) Kamerstukken II, 2022/2023, Aanhangsel van de Handelingen, 2595.
(218) Kamerstukken II, 2022/2023, Aanhangsel van de Handelingen, 2595, p. 7.
(219) Dit gebeurt zowel door Wwft/Sw-toezichthouders als het Openbaar Ministerie. Te denken valt aan bestuursrechtelijke en tuchtrechtelijke handhaving door toezichthouders, alsook de schikkingen van het OM met ING en ABN AMRO, vervolgingen van of transacties met poortwachters voor het niet-melden van ongebruikelijk transacties (bijv. Rb. Amsterdam 22 april 2021, ECLI:NL:RBAMS:2021:2600; Gerechtshof Den Haag 1 februari 2019, ECLI:NL:GHDHA:2019:187; Openbaar Ministerie, 'Trustkantoor Vistra betaalt 3,5 ton voor niet melden ongebruikelijke transacties', nieuwsbericht 3 september 2019). Zie ook: AMLC, *Strafrechtelijke aanpak via de Wwft*, beschikbaar via deze link.
(220) Van Wingerde en Hofman 2022, p. 13; Daalderop 2019, p. 50; Nuijten 2023, p.144.
(221) Nuijten 2023, p. 144.
(222) Nuijten 2023, p. 144; Zwinkels 2020. In dit laatste artikel wordt onderzocht in hoeverre het reëel is dat ook compliance officers bestuursrechtelijk of strafrechtelijk worden aangepakt. Hoewel nog niet gebeurd, concludeert auteur onder verwijzing naar gevallen in het buitenland, dat het niet uitgesloten is dat DNB en het OM gebruik kunnen en zullen maken van hun bevoegdheden jegens compliance officers.

Te denken valt aan de ontwikkelingen rond de betrouwbaarheids- en geschiktheidstoetsingen, en specifieke vereisten die volgen uit EBA-richtsnoeren.(223) Ook wordt bij handhaving steeds vaker gekeken of bestuurders – al dan niet naast de Wwft-instelling zelf – ook persoonlijk aangesproken kunnen worden bij niet of onvoldoende naleving van de Wwft.(224) Dit levert een extra hoge druk op voor instellingen en hun bestuurders.

Uit een recent interview met topmannen van het OM en VNO-NCW in het FD kwam ook naar voren dat het vervolgen van bestuurders *"voor veel onrust zorgt in boardrooms"*.(225) Het OM meent dat de aanpak van poortwachters nog altijd belangrijk is: *"[w]aar mogelijk zal worden gekeken naar commune feiten, maar de ervaring leert dat bewijstechnisch vaak alleen voor misdrijven in de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)/Wet economische delicten (WED) kan worden vervolgd"*.(226)

Deze aanpak van poortwachters resulteert in een situatie dat poortwachters verkrampen en zich gedwongen voelen om meer te doen dan nodig, wat ook wel wordt aangemerkt wordt als het 'rule-based' invullen van risicogebaseerde normen of 'compliancegerichte' naleving, om maar aan te kunnen tonen te hebben voldaan aan alle vereisten.(227) De verkramping uit zich in weerstand bij bestuurders om risico's te nemen; deze worden vermeden omdat het voorkomen van negatieve scenario's de status quo is geworden.(228) Hierover zegt een bankbestuurder in een onderzoek van KPMG: *"[i]edereen is voorstander van een goede poortwachtersfunctie voor banken, maar het is voor elke bank ontzettend lastig om daarbij naar de geest van de wet te handelen. Eigenlijk is het volgen van de letter van de wet de makkelijkste optie. Dan kom je niet in problemen en kom je daarmee ook niet negatief in de pers. Maar maatschappelijk gezien schiet niemand daar wat mee op"*.(229) Deze verkramping en angst voor fouten vertaalt zich ook in de uitvoering van de poortwachtersrol op de werkvloer. Uit interviews komt naar voren dat personeel van poortwachters betrokken in de dagelijkse Know Your Client/Client Due Diligence (KYC/CDD) processen behoefte hebben aan duidelijke kaders en instructies.

De compliancegerichte naleving uit zich in het bijzonder in de context van het meldgedrag van poortwachters. Het gevolg is dat meldingen worden gedaan vanuit de gedachte de instelling 'in te dekken' tegen mogelijke juridische gevolgen van het niet-melden. Compliance is dan de drijfveer voor het melden, in plaats van voorkomen van financieel-economische criminaliteit. Dit wordt ook wel 'defensive reporting' of het 'crying wolf'-probleem genoemd en heeft als gevolg dat er veel meldingen van lage(re) kwaliteit worden gedaan aan FIU-NL.(230) Deze input heeft gevolgen voor de rest van de anti-witwasketen: schaarse middelen moeten worden ingezet om deze te analyseren en ze dragen ook niet bij aan het voorkomen van witwassen en terrorismefinanciering.(231)

3.3.3 Knelpunten ervaren door klanten

Ook klanten, zowel particulieren als bedrijven, ervaren knelpunten bij de uitvoering van de Wwft door poortwachters. Enkele van de ervaren knelpunten door klanten zijn een spiegeling van een ervaren knelpunt door de poortwachters. Vanwege het verschil in perspectief is er desalniettemin voor gekozen om deze knelpunten ook in deze paragraaf terug te laten komen. Daarbij gaat het om de verminderde toegang tot het financiële stelsel, doorlooptijden en kosten, en herhaalde en onnodige uitvragen. In deze paragraaf volgt een uiteenzetting van deze drie knelpunten vanuit het perspectief van de klant.

(223) Bijvoorbeeld European Banking Authority, *Richtsnoeren inzake de rol en verantwoordelijkheden van de compliance officer op het gebied van AML/CFT*, EBA/GL/2022/ 05, 14 juni 2022, beschikbaar via deze link.
(224) Te denken valt aan de strafrechtelijke vervolging van voormalig ING-topman Hamers en het aanmerken van meerdere oud-bestuurders als verdachten in een strafrechtelijk onderzoek van het OM naar ABN AMRO.
(225) M. Pols, E. van der Schoot, 'OM-topman: 'Ik mis de verontwaardiging over criminaliteit die het bedrijfsleven ondermijnt'', *FD* 21 april 2023.
(226) Openbaar Ministerie 2022, p. 17.
(227) DNB 2022, p. 20-21; RUSI 2019, p. 19-20; Stichting Maatschappij en Veiligheid 2022, p. 35-36; Hoogenboom 2021, p. 180-181. Zie ook Michael Levi en Tom Keatinge in KPMG 2022a, p. 28 en 32.
(228) KPMG 2022, p. 4.
(229) KPMG 2022, p. 25.
(230) Unger en Van Waarden 2013; Takáts 2007; Amicelle 2017, p. 219; Vogel 2022, p. 53. Takáts maakt voor buitensporig melden een analogie met de oude Griekse fabel 'De jongen die wolf riep'. In het boek doet de jongen zo vaak alsof een wolf zijn schapen aanvalt, dat op het moment dat dit daadwerkelijk gebeurt niemand meer naar hem luistert en hij opgegeten wordt.
(231) UK Law Commission 2019, p. 31; Gilmour & Hicks 2023, p. 128.

1. Verminderde toegang tot het financiële stelsel

Mede door de toegenomen regeldruk en de beperkte ondersteunende rol van de overheid, gecombineerd met de druk vanuit toezichthouders en het OM, zijn poortwachters steeds scherper op de vraag of zij bepaalde risico's wel of niet kunnen en willen accepteren en mitigeren. Op basis van een risicoanalyse kunnen poortwachters per geval besluiten of zij diensten willen verlenen aan een klant. Het afwegen van kosten en baten voor de uitvoering van de Wwft en Sw door poortwachters kan ertoe leiden dat zij aan bepaalde klanten geen diensten meer (willen) verlenen.(232) Particulieren en bedrijven met hogere integriteitsrisico's, bijvoorbeeld klanten uit industrieën waar veel contant geld in omloop is, verenigingen of stichtingen, of klanten die aangemerkt zijn als PEP, kunnen te maken krijgen met weigering van of beperking in de dienstverlening.(233) Hetzelfde zou gelden voor bepaalde bevolkingsgroepen, zoals gesteld door de Nationaal Coördinator tegen Discriminatie en Racisme.(234) Wanneer sprake is van het categoraal uitsluiten of beperken van klanten, wordt dit 'de-risking' genoemd.(235) Uit onderzoek van de Europese Bankenautoriteit (EBA) blijkt dat de-risking negatieve impact kan hebben op de bestrijding van financieel-economische criminaliteit, het bevorderen van financiële inclusie, concurrentie en stabiliteit op de financiële markten.(236) Tevens merkt DNB op dat onnodige de-risking potentieel kan leiden tot *"verlies van effectiviteit van en draagvlak voor de naleving van de Wwft en voor het toezicht".*(237) Interviews verricht in het kader van dit onderzoek bevestigen het beeld dat bepaalde groepen ondernemers en bedrijven moeite hebben om een bankrekening te openen. Dit geldt opvallend genoeg ook voor poortwachters zelf: de afgelopen jaren zijn er meerdere rechtszaken geweest over het beëindigen van de relatie met trustkantoren.(238) Ook de FATF heeft hier in de evaluatie van Nederland aandacht aan besteed en bestempelt dit als zorgwekkend.(239)

2. Lange doorlooptijden, toename in kosten en administratieve lasten

Cliëntenonderzoeken kosten tijd en geld, en klanten ervaren lange doorlooptijden bij aanvang van de dienstverlening.(240) Wanneer klanten tot een segment met verhoogde integriteitsrisico's behoren, zijn onderzoeken extra tijdrovend en duur. Steeds vaker worden deze additionele kosten aan de klanten doorberekend.(241) Uit schattingen van de Nederlandse Vereniging van Banken (NVB) en PwC kunnen kosten voor een zakelijke bankrekening met tot wel EUR 2.000 toenemen.(242) Tussen 2018-2022 zijn de gemiddelde kosten van bankieren met 42% gestegen, deels door de banken beargumenteerd vanuit witwasoogpunt.(243) Daarbovenop hebben klanten vaak zelf nog te maken met extra kosten vanwege de complexiteit en omvang van opgevraagde informatie.(244) In een van de interviews verricht in het kader van dit onderzoek gaven geïnterviewden aan dat bedrijven en ondernemingen niet zelden externe adviseurs moeten inhuren om te kunnen voldoen aan informatie-uitvragen van poortwachters.

3. Herhaalde en onnodige uitvragen

Zowel particulieren als bedrijven hebben op verschillende momenten in tijd met verschillende poortwachters te maken. Ter illustratie zijn hierna een klantreis van een ondernemer uit het midden- en kleinbedrijf en van een particulier opgenomen. Daaruit wordt duidelijk dat klanten met meerdere poortwachters te maken krijgen, zowel bij het verrichten van één transactie in hetzelfde tijdframe (bijvoorbeeld bij de aankoop van vastgoed) als gedurende een langere periode (bijvoorbeeld bij de uitbreiding van een onderneming).

(232) NVB 2022a, p. 13.
(233) Zie bijvoorbeeld: R. Betlem, 'Rabobank sluit kleine autodealers uit vanwege risico op witwassen', *FD* 1 juli 2021; Goede Doelen Nederland, *Tweede brandbrief aan Kaag over gevolgen de-risking banken*, 21 april 2022, beschikbaar via deze link; 'Banken weigeren goede doelen om 'witwasrisico', *RTL Nieuws* 15 november 2022; 'ING te druk met witwasonderzoek, weert stichtingen en verenigingen', *NOS.nl* 29 augustus 2022. Per 1 juni 2023 is het voor stichtingen en vereniging weer mogelijk om een nieuwe rekening te openen, staat op de ING-website aangegeven.
(234) 'Racismecoördinator: 'Structurele discriminatie van moslims bij banken', *NOS.nl* 6 april 2023. Zie bovendien paragraaf 3.3.2 met betrekking tot conflicterende wet- en regelgeving.
(235) DNB 2017, p. 8.
(236) EBA 2022, p. 2.
(237) DNB 2022, p. 22.
(238) Bijvoorbeeld: Rb. Amsterdam, 1 december 2020, ECLI:NL:RBAMS:2020:6245; Rb. Amsterdam, 5 januari 2022, ECLI:NL:RBAMS:2022:42.
(239) FATF 2022b, p. 121.
(240) NVB 2022a, p. 14; R. Vaessen, 'Even een rekening openen', *Accountant.nl* 6 september 2019.
(241) R. Betlem, 'Zakelijke rekeningen duurder door stijgende kosten witwasonderzoek', *FD* 30 augustus 2022.
(242) NVB 2022a, p. 14.
(243) P. de Waard, 'Kosten voor bankrekening blijven stijgen, ABN AMRO gooit er in een keer 51,3 procent bovenop', *Volkskrant* 3 mei 2022; 'Bedrijven, stichtingen en kerken moeten van banken meebetalen aan witwasonderzoek', *NOS.nl* 27 december 2022.
(244) NVB 2022a, p. 14.

Omdat iedere poortwachter zijn eigen informatie en klantdossier dient te hebben, moeten klanten steeds (min of meer) gelijke gegevens aanleveren aan elke individuele poortwachter.(245)

Ook dienen poortwachters gedurende de relatie hun cliëntenonderzoek opnieuw te verrichten, wat ook weer kan leiden tot herhaalde uitvragen bij klanten.

Figuur 2: Klantreis van een ondernemer uit het midden- en kleinbedrijf

Figuur 3: Klantreis van een particulier

Uit eerder onderzoek en uit interviews verricht in het kader van dit onderzoek wordt duidelijk dat klanten zich storen aan het herhaaldelijk aanleveren van gegevens, zeker indien de informatie hetzelfde of vergelijkbaar is.(246) In het rapport 'Van herstel naar balans', geeft DNB aan dat zij meldingen heeft ontvangen waaruit blijkt dat klanten vinden dat banken onnodige informatie opvragen, of informatie die zij liever niet willen delen.(247)

(245) RUSI 2019, p. 20.
(246) NVB 2022a, p. 13.
(247) DNB 2022, p. 21. Zie ook Maxwell 2020, p. 9.

3.3.4 Knelpunten geconstateerd door toezichthouders en het OM

Uit de publiek beschikbare Wwft-handhavingsbesluiten van de AFM en DNB, en de tuchtklachten van het Bureau Financieel Toezicht (BFT) jegens notarissen, blijkt dat poortwachters verschillende normen uit de Wwft overtreden.(248) Overtredingen variëren van een gebrekkige of geheel afwezige risicobeoordeling of systematische integriteitsanalyse(249) tot het onterecht niet verrichten van verscherpt cliëntenonderzoek(250), het ontoereikend monitoren van transacties (251), en het niet of niet-tijdig melden van ongebruikelijke transacties(252). Niet alleen kernverplichtingen worden overtreden. In de handhavingsbesluiten en tuchtklachten komen ook gestelde overtredingen voor het ontbreken van een onafhankelijke compliancefunctie(253), uitbesteding (artikel 10)(254), de bewaarplicht (artikel 33 Wwft)(255) en de opleidingsplicht (artikel 35 Wwft)(256) naar voren.

Waar de handhavingsbesluiten van de toezichthouders veelal technisch van aard zijn en gericht zijn op het bewijzen van de overtredingen, geven de strafrechtelijke onderzoeken en schikkingen van het Openbaar Ministerie een verdiepende kijk op de oorzaken van geconstateerde overtredingen. In 2018 trof ING Bank een schikking met het OM vanwege "*ernstige nalatigheden bij het voorkomen van witwassen*".(257) In 2021 trof ABN AMRO Bank een schikking met het OM vanwege hetzelfde verwijt.(258)

In beide feitenrelazen – respectievelijk Houston en Guardian – is te lezen hoe de bedrijfscultuur, de 'tone at the top', en een gebrekkige communicatie en bedrijfsorganisatie een rol hebben gespeeld bij de overtredingen van de Wwft.(259) Enkele van deze (organisatie)culturele knelpunten zijn:

- Gebrekkige 'tone at the top' en onvoldoende aandacht en prioriteit voor het anti-witwasbeleid. Uit het feitenrelaas Houston komt naar voren dat er in het geval van ING Bank onvoldoende awareness was bij het hoger leidinggevend personeel van het belang van naleving van de Wwft en dat daarmee de 'tone at the top' dit onvoldoende uitdroeg.(260) Om tot effectieve naleving van wettelijke verplichtingen te komen, is het communiceren van de juiste 'tone at the top' belangrijk.(261) De bevindingen in het geval van ING Bank staan niet op zichzelf: onderzoek wijst uit dat complianceafdelingen weerstand van hoger management ervaren bij de uitoefening van hun taken.(262)
- Cultuur. In het geval van ABN AMRO Bank stelt het OM dat de niet-naleving van de Wwft ook voortvloeit uit de cultuur. Volgens het OM werd een mooiere voorstelling gegeven van de zaken dan in werkelijkheid het geval was, waardoor het idee ontstond problemen op te kunnen lossen in 'business as usual'.

(248) De website van de Belastingdienst/Bureau Toezicht Wwft toont uitsluitend bestuurlijke sancties jegens (auto)handelaren (tot en met 2021). Er zijn geen openbare handhavingsbesluiten voor overtredingen van de Sanctiewet gepubliceerd door DNB en AFM, omdat de toezichthouders deze bevoegdheid op grond van de Sanctiewet 1977 niet hebben.

(249) AFM, *Aanwijzing Zwaan Finance B.V.*, 25 maart 2022, beschikbaar via deze link; AFM, *Bestuurlijke boetes Revo Capital Management B.V.*, 25 mei 2022, beschikbaar via deze link; DNB, *Aanwijzing MUFG Bank (Europe) N.V.*, 29 juli 2019, beschikbaar via deze link; DNB, *Bestuurlijke boete Suri-Change B.V.*, 25 november 2014, beschikbaar via deze link; AFM, *Bestuurlijke boete Robeco Institutional Asset Management B.V.*, 31 maart 2022, beschikbaar via deze link.

(250) Zie bijvoorbeeld: AFM, *Aanwijzing STX Fixed Income B.V.*, 8 juni 2021, beschikbaar via deze link; Kamer voor het notariaat Amsterdam, 10 maart 2022, ECLI:NL:TNORAMS:2022:8; Kamer voor het notariaat Den Haag, 15 juli 2022, ECLI:NL:TNORDHA:2022:14; Kamer voor het notariaat Den Bosch, 19 september 2022, ECLI:NL:TNORSHE:2022:31; CBb, 18 oktober 2022, ECLI:NL:CBB:2022:707 (Bunq).

(251) Zie bijvoorbeeld AFM, *Bestuurlijke boete Robeco Institutional Asset Management B.V.*, 31 maart 2022, beschikbaar via deze link; DNB, *Bestuurlijke boete Suri-Change B.V.*, 25 november 2015, beschikbaar via deze link; CBb, 18 oktober 2022, ECLI:NL:CBB:2022:707 (Bunq).

(252) DNB, *Bestuurlijke boete JTC Institutional Services Netherlands B.V.*, 14 juni 2021, beschikbaar via deze link; DNB, *Bestuurlijke boete Travelex N.V.*, 2 februari 2023, beschikbaar via deze link; AFM, *Bestuurlijke boete FlatexDeGiro*, 23 december 2021, beschikbaar via deze link; Kamer voor het notariaat Den Bosch, 19 september 2022, ECLI:NL:TNORSHE:2022:31; Kamer voor het notariaat Den Haag, 15 juli 2022, ECLI:NL:TNORDHA:2022:14; AFM, *Bestuurlijke boete Robeco Institutional Asset Management B.V.*, 31 maart 2022, beschikbaar via deze link.

(253) Zie bijvoorbeeld Kamer voor het notariaat Den Haag 25 mei 2022, ECLI:NL:TNORDHA:2022:10 (tuchtklacht ongegrond verklaard) en CBb, 3 maart 2020, ECLI:NL:CBB:2020:120.

(254) Rabobank, *Rabobank heeft voorgenomen aanwijzing ontvangen van DNB*, 16 november 2021, beschikbaar via deze link.

(255) Zie bijvoorbeeld: AFM, *Aanwijzing STX Fixed Income B.V.*, 8 juni 2021, beschikbaar via deze link; Rabobank, 'Rabobank heeft voorgenomen aanwijzing ontvangen van DNB', persbericht 16 november 2021.

(256) Zie bijvoorbeeld: AFM, *Aanwijzing Zwaan Finance B.V.*, 25 maart 2022, beschikbaar via deze link; AFM, *Aanwijzing STX Fixed Income B.V.*, 8 juni 2021, beschikbaar via deze link.

(257) Openbaar Ministerie 2018.

(258) Openbaar Ministerie 2021.

(259) Openbaar Ministerie 2018, p. 13; Openbaar Ministerie 2021, p. 21-22.

(260) Openbaar Ministerie 2018, p. 13.

(261) Zie ook David Lewis in KPMG 2022a, p. 35.

(262) Rakké en Huisman 2020, p. 11.

- Business boven compliance. Er werd onvoldoende geïnvesteerd in systemen en capaciteit van personeel vanwege commerciële doelstellingen. Uit het feitenrelaas Guardian komt naar voren dat hoewel 'geld geen probleem' zou zijn, er niet daadwerkelijk een budget beschikbaar was. Deze bevinding houdt verband met het eerder genoemde knelpunt bij poortwachters dat zij spanning ervaren tussen het commerciële belang en de poortwachterstaak.
- Gebrekkige interne organisatie. In beide feitenrelazen komt naar voren dat de 'three lines of defence' gebrekkig functioneerden, dat de organisatie zo was ingericht dat deze verzuiling/silovorming veroorzaakte, dat signalen het hoger management niet bereikten en gebrekkig werd gecommuniceerd. Daardoor ontstond een beperkt overzicht van de daadwerkelijke omvang van niet-naleving en ontbrak ook een overzicht van de benodigde herstelmaatregelen.

De bevindingen van het OM in deze zaken staan niet op zichzelf. In een analyse naar de betrokkenheid van banken bij enkele witwasschandalen in de Europese Commissie, merkt de Europese Commissie ook op dat het niet adequaat invullen van de poortwachtersrol te herleiden is tot structurele governanceproblemen. Daarbij noemt de Commissie het gebrekkig functioneren van de 'three lines of defence' en de interne meld- en escalatieprocessen, de cultuur waarbij het commerciële de boventoon voerde en dat het hoger leidinggevend personeel onvoldoende geïnformeerd werd.(263)

3.4 Concluderende opmerkingen over de uitvoering van de Wwft en Sanctiewet

De uitvoering van de Wwft en Sw wordt geraakt door verschillende wetgevingsontwikkelingen. Wat opvalt is dat in het bijzonder de ontwikkelingen rondom de Wwft en Wtt erg snel gaan.

Ook vinden momenteel ontwikkelingen plaats op het gebied van sancties. Met de toenemende maatschappelijke aandacht voor privacy en de actieve rol van de AP die vaak kritisch van toon is in het publieke debat over de bestrijding van criminaliteit, waaronder witwassen en terrorismefinanciering, komt dat spanningsveld ook steeds duidelijker voor het voetlicht. Ook technologische ontwikkelingen zoals kunstmatige intelligentie, de digitale identiteit en portemonnee en blockchain raken de uitvoering van de Wwft en Sw; deze kunnen een positieve rol spelen in de effectieve en efficiënte naleving van de Wwft en Sw. Uiteraard is het van belang om bij deze ontwikkelingen oog te hebben voor waarborgen rondom bijvoorbeeld privacy en cybersecurity.

Figuur 4: Samenvatting knelpunten poortwachters, klanten en toezichthouders

Figuur 4 toont de geïdentificeerde knelpunten bij de uitvoering van de Wwft en Sanctiewet in de praktijk. Het valt op dat knelpunten die worden ervaren door poortwachters en klanten, en de knelpunten die worden geconstateerd door toezichthouders en het Openbaar Ministerie, te herleiden zijn tot een aantal fundamenten van het anti-witwasbeleid.

(263) Europese Commissie 2019, p. 4-5. Zie ook: Yeoh 2020.

Er lijkt een vicieuze cirkel te bestaan waarbij heldere doelen van het beleid ontbreken, duidelijke centrale sturing afwezig is of ten minste zo wordt ervaren, en de verwachtingen over de respectievelijke rollen tussen, en inzet van, publieke en private sector over en weer uiteenlopen. Ook de disbalans tussen verplichtingen en bevoegdheden voor poortwachters speelt daarbij een rol.

Wat betreft de poortwachtersrol kan worden geconstateerd dat er spanningen bestaan met de commerciële bestaansredenen van de poortwachters en de invulling van hun poortwachtersrol, en dat zij op verschillende vlakken ervaren onvoldoende gesteund te worden door de overheid aan de voorkant, bijvoorbeeld via duidelijke sturing en prioriteitstelling, guidance en feedback. Dit kan frustratie opleveren en is schadelijk voor hun motivatie om als poortwachter scherp 'de poort te bewaken'. Wanneer zij dat niet doen, vereist dat weer inzet van de overheid aan de achterkant in de vorm van verschillende vormen van handhaving. Tegelijkertijd blijkt uit de handhavingsinformatie dat niet-naleving door poortwachters niet uitsluitend komt door voornoemde redenen. De gevolgen van de vicieuze cirkel zijn zichtbaar in de knelpunten die worden ervaren door klanten: financiële uitsluiting en hogere kosten. Alle knelpunten tezamen leiden weer terug tot de – tot noch toe niet te beantwoorden – kernvraag van het anti-witwasbeleid: in hoeverre worden witwassen en terrorismefinanciering daadwerkelijk voorkomen?

Verkenning in binnen- en buitenland

4

4.1 Inleiding

In het licht van de onderzoeksvraag en de geïdentificeerde relevante ontwikkelingen en knelpunten uit het voorgaande hoofdstuk, is een verkenning verricht naar initiatieven die in binnen- en buitenland ontplooid zijn en die als mogelijke oplossingen of alternatieven voor een effectieve(re) en efficiënte(re) naleving van de Wwft en Sanctiewet kunnen dienen. Daarbij is gekeken naar randvoorwaarden, succesfactoren en geleerde lessen die bij de ontwikkeling van oplossingsrichtingen in dit onderzoek meegenomen worden.

Uit de verkenning verricht voor dit onderzoek komt naar voren dat denkrichtingen voor mogelijke oplossingen of alternatieven vooral moeten worden gezocht in **technologie** en **samenwerking**. Samengevat gaat het om de volgende denkrichtingen:

1. Dit betreft in de eerste plaats de mogelijkheid voor informatiedeling tussen poortwachters. Daarbij gaat het bijvoorbeeld om de ontwikkeling van private samenwerkingsverbanden of utiliteiten, veelal met als hoofddoel het efficiënter maken van cliëntenonderzoeken en/of de voortdurende controle.(264) Het kan ook gaan om het gebruik van waarschuwingssystemen om de cliëntenonderzoeken van poortwachters effectiever te maken en het financiële systeem 'schoon' te houden.(265) Verschillende aspecten zoals technologie (denk aan distributed ledger technologie en blockchaintechnologie), privacybescherming en juridische (on)mogelijkheden voor informatiedeling, spelen een belangrijke rol en zijn ook (deels) van invloed op de mate van succes van initiatieven die in binnen- en buitenland ontplooid worden.
2. In de tweede plaats betreft dit de ontwikkeling en het gebruik van de digitale identiteit – ook wel digitale ID-portemonnees ('wallets') of financiële paspoorten genoemd. Hier wordt in binnen- en buitenland veel aandacht aan besteed en dit is eerder in paragraaf 3.2.4 kort toegelicht als een relevante technologische ontwikkeling.(266) Er bestaan al verscheidene (commerciële) initiatieven in binnen- en buitenland, maar het gebruik daarvan in het kader van het cliëntenonderzoek lijkt zich nog in een vroeg stadium te bevinden. Afhankelijk van de vormgeving kunnen samenwerkingsverbanden tussen private partijen zoals de utiliteiten en het gebruik van digitale identiteit samenlopen, maar dit hoeft niet het geval te zijn.(267)
3. In de derde plaats wordt publiek-private samenwerking gezien als middel om de preventie van witwassen, terrorismefinanciering en naleving van sanctieregelgeving effectiever te maken. Met de gedachte dat financieel-economische criminaliteit beter kan worden teruggedrongen door samen te werken en kennis en 'intelligence' te delen.

   In de evaluatie van het Nederlandse anti-witwasbeleid heeft de FATF de binnenlandse samenwerking, zowel publiek-publieke als publiek-private samenwerking, geprezen en zelfs een *"key feature"* van het Nederlandse systeem genoemd.(268) Het voorgaande hoofdstuk heeft wel laten zien dat een effectieve feedbackloop en een balans tussen de input van de private sector aan de voorkant en output in de vorm van (strafrechtelijke) veroordelingen en inbeslagnames door de publieke sector daarbij essentieel zijn.
4. Voorts blijkt uit het voorgaande hoofdstuk een duidelijke behoefte aan een overheid die (meer) centraal aanstuurt, meer met één stem spreekt, duidelijke keuzes maakt en prioriteert. Knelpunten zoals de fragmentatie van overheidsbeleid, conflicterende wet- en regelgeving, een ervaren gebrek aan guidance en feedback zijn terug te herleiden tot dit punt. Dit geldt ook voor de knelpunten die worden ervaren door klanten. Daarom is ook dit punt ook meenomen in de verkenning van dit onderzoek.

In de hiernavolgende paragrafen worden deze denkrichtingen verder uitgewerkt. Aan de hand van elk van de denkrichtingen wordt ingegaan op geselecteerde initiatieven uit binnen- en buitenland.

(264) BIS 2023, p. 12-13.
(265) Zie voor KYC-utiliteiten en informatiedeling tussen private partijen onder meer FATF 2017; T. Lyman en L. de Koker, 'KYC Utilities and Beyond: Solutions for an AML/CFT Paradox', *CGAP Blog Series Beyond KYC Utilities* 1 maart 2018; Zetzsche et al. 2018; CGAP 2019; FATF 2022.
(266) Zie bijvoorbeeld Zetzsche et al. 2018; Leung et al. 2022; DNB 2022.
(267) Zetzsche et al. 2018. Zie bijlage B voor MyInfo-dienst op Singpass, waar een samenloop lijkt te zijn.
(268) FATF 2022b, p. 52.

De gedetailleerde analyses van deze initiatieven zijn beschreven in bijlage B van dit onderzoeksrapport. Bij de selectie van initiatieven is rekening gehouden met een balans tussen nieuwe en oude(re) initiatieven, succesvolle en minder succesvolle initiatieven, en initiatieven met gedeelde kenmerken maar ook met elk hun verschillen. Voor elk thema zijn enkele aandachtspunten of 'lessons learned' geïdentificeerd. Deze verkregen inzichten kunnen worden meegenomen in de uitwerking van mogelijke oplossingsrichtingen in antwoord op de voorliggende onderzoeksvraag.

4.2 Informatiedeling tussen poortwachters

4.2.1 Gezamenlijke voorzieningen en 'grijze' lijsten

"It takes a network to defeat a network".(269) Het vormen van netwerken, partnerschappen en samenwerkingsverbanden – zowel privaat-privaat als publiek-privaat (zie paragraaf 4.4) – wordt (steeds vaker) gezien als de manier om effectiever en efficiënter op te treden in de strijd tegen witwassen, terrorismefinanciering en onderliggende criminaliteit door (georganiseerde) criminele organisaties.(270) Effectieve informatiedeling wordt door de FATF als een van de hoekstenen van een effectief anti-witwasbeleid genoemd.(271)

Delen van informatie op typologie- en klantniveau over en weer leidt in de eerste plaats tot diepere kennis. Dit stelt poortwachters (en in het geval van publiek-private samenwerking ook publieke overheidspartijen) in staat hun rol beter te vervullen. Zij kunnen met de gedeelde informatie bijvoorbeeld een betere risico-inschatting van (potentiële) klanten maken, of een meer gerichte controle op de zakelijke relatie uitvoeren. Ook kan dit in de tweede plaats leiden tot het verhogen van de kwaliteit van meldingen van ongebruikelijke transacties.(272) In de derde plaats kan het delen van informatie over (gezamenlijke) klanten ook leiden tot efficiënter en klantvriendelijker cliëntenonderzoek. Klanten hebben vaak met meer dan één poortwachter te maken en het delen van klantinformatie tussen hen kan leiden tot het minderen van de uitvraag van herhaalde verzoeken om informatie, lagere kosten en administratieve lasten en snellere doorlooptijden.(273) Voor klanten leidt dit vooral tot minder gedoe en het geeft poortwachters de mogelijkheid hun beperkte middelen elders in te zetten.

"It takes a network to defeat a network"

In verschillende landen wordt geëxperimenteerd met het delen van informatie tussen poortwachters. Deze initiatieven worden veelal gedreven door of voor banken. Gezamenlijke voorzieningen, ook wel utiliteiten genoemd, waarin informatie over klanten en/of hun transacties worden gedeeld kunnen zich zowel richten op het CDD-proces als de voortdurende controle in de vorm van transactiemonitoring of sanctiescreening.(274) De zogenaamde gezamenlijke voorzieningen voor transactiemonitoring (TM-utiliteiten) hebben vooral de potentie om betrokken partijen een 'breder' beeld te geven dan enkel de transactie waar zij zelf bij betrokken zijn en daarmee ongebruikelijke of verdachte gedragspatronen te ontdekken dat anders ongedetecteerd zou blijven.(275) Op basis van onderzoek stelt de Bank for International Settlements (BIS) dat *"[u]tilising network analysis for detecting anomalous and suspicious networks shifts the focus from individual behaviour to the overall behaviour of suspicious networks, resulting in improved detection capabilities".*(276) De BIS concludeert dat *"[t]he main findings of Project Aurora suggest that behavioural-based transaction monitoring and analysis at national or international levels is more effective in detecting money launderers and suspicious networks than current siloed and rule-based monitoring".*(277) TM-utiliteiten lijken vooral relevant voor poortwachters met grote transactiestromen en duurzame zakelijke relaties, zoals banken, betaaldienstverleners, crypto-aanbieders en trustkantoren.

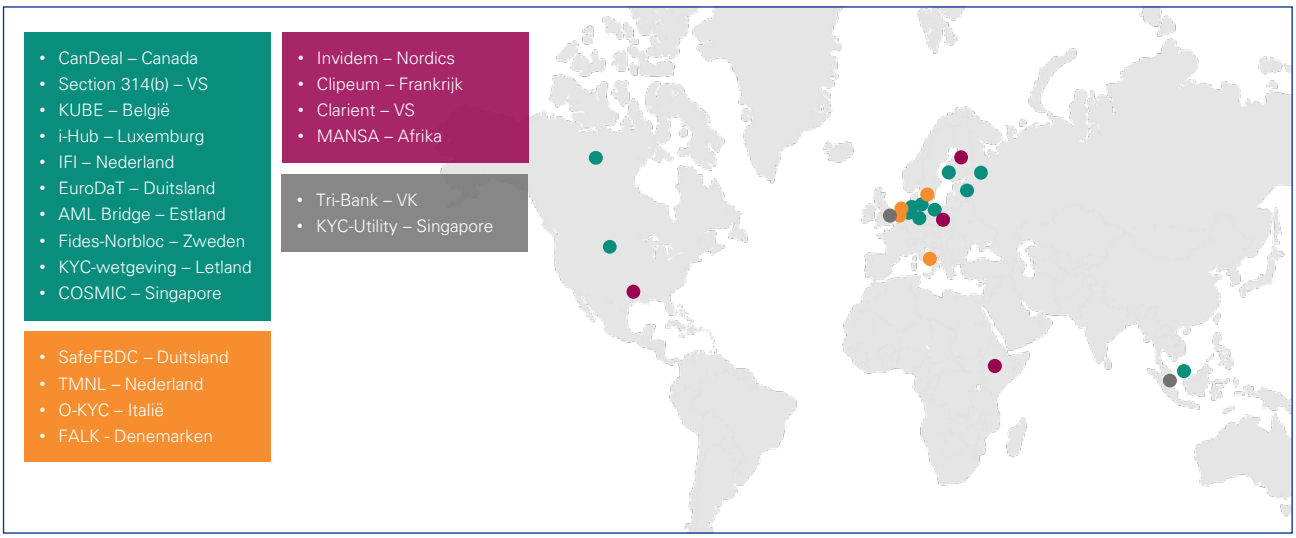
(269) Naar verluidt komt deze quote van de Amerikaans generaal Stanley McChrystal bij de beslissende fase in de oorlog tegen IS in Irak.
(270) RUSI 2017; FATF 2017; FATF 2022; RUSI 2022; KPMG 2022a; BIS 2023.
(271) FATF 2017, p. 2.
(272) FIU 2023, p. 2.
(273) KPMG 2018, p. 3.
(274) BIS 2023, p. 79; A. Clare, 'Sanctions screening regtech GSS secures $45mn in funding', *Fintech Magazine* 23 januari 2023.
(275) FATF 2022, p. 3; NVB 2022, p. 3; NVB 2023, p. 5; BIS 2023, p. 74.
(276) BIS 2023, p. 13.
(277) BIS 2023, p. 74.

Bekende voorbeelden van initiatieven voor gezamenlijke transactiemonitoring zijn Transactie Monitoring Nederland B.V. (TMNL), de TriBank pilot in het Verenigd Koninkrijk en COSMIC in Singapore.[278] TMNL en diens potentie om effectiever en efficiënter te worden in het detecteren van mogelijke ongebruikelijke transactiepatronen is nader uitgewerkt in bijlage B. Gezamenlijke voorzieningen op grond van (aspecten van) CDD – in het buitenland en de literatuur ook wel KYC-utiliteiten genoemd – hebben veelal als doel om cliëntenonderzoeken van poortwachters efficiënter te maken door herhaald gebruik van data (datacirculariteit) en de mogelijkheid om deze data te actualiseren en te optimaliseren (datamutualisatie).[279] Er zijn veel initiatieven voor dit soort gezamenlijke voorzieningen in binnen- en buitenland waarvan een geselecteerd aantal is uitgewerkt in bijlage B. De initiatieven laten een wisselende mate van succes zien: sommige initiatieven zijn recentelijk stopgezet, terwijl andere initiatieven nog moeten starten of net begonnen zijn.

Een andere vorm van informatiedeling tussen poortwachters betreft het ontwikkelen van een waarschuwingssysteem. Een waarschuwingssysteem kan poortwachters in staat stellen om hun rol effectiever uit te oefenen doordat zij op de hoogte zijn van incidenten en/of risico's rondom natuurlijke personen of rechtspersonen. Met die informatie zijn zij tijdens het cliëntenonderzoek beter in staat om de risico's van een (voorgenomen) klant te beoordelen en mitigerende acties te nemen. Ook kan ongewenst 'shopgedrag' worden voorkomen.[280] Vanuit het perspectief van privacy is het belangrijk om te kijken naar de waarborgen die met een dergelijk systeem gepaard dienen te gaan.[281] Het is belangrijk dat opname in een register niet een de facto weigering of beëindiging van een zakelijke relatie inhoudt.[282] In de Nederlandse context is het Incidentenwaarschuwingssysteem Financiële Instellingen een voorbeeld uit de financiële sector. De nadere uitwerking van dit waarschuwings-systeem is te vinden in bijlage B van dit onderzoeksrapport.

4.2.2 Overzicht van initiatieven voor informatiedeling tussen poortwachters

Figuur 5 toont een greep uit de initiatieven voor informatiedeling tussen poortwachters en hun status. Rode initiatieven zijn initiatieven die zijn gestopt, oranje initiatieven zijn in ontwikkeling of werkend met beperkingen (bijvoorbeeld in afwachting van aanpassing van wet- of regelgeving) en groene initiatieven zijn actief. Voor deze verkenning zijn enkele initiatieven met verschillende statussen onderzocht om inzicht te krijgen in relevante aspecten en 'lessons learned'.



Figuur 5: Overzicht initiatieven voor informatiedeling wereldwijd

(278) Zie FATF 2022, p. 20-22 (Tribank pilot) en 22-26 (COSMIC).
(279) KPMG 2018, p. 7.
(280) Zie hierover ook het wetsvoorstel en de bijbehorende Memorie van toelichting voor de Wet plan van aanpak witwassen met de introductie van een navraagplicht voor Wwft-instellingen: Kamerstukken II, 2022/2023, 36 228, nrs. 2 en 3. Voor trustkantoren is dit reeds een verplichting op grond van artikel 68 Wtt 2018.
(281) Berkvens 2011, p. 210-214.
(282) RUSI 2022, p. 36.

4.2.3 Verkregen inzichten uit initiatieven uit binnen- en buitenland

Inzichten op basis van gezamenlijke voorzieningen en 'grijze' lijsten

Wereldwijd wordt geëxperimenteerd met private samenwerkingsverbanden en utiliteiten, met wisselend succes. Naar aanleiding van pilots en projecten wordt wel gewezen op de voordelen die behaald kunnen worden met private samenwerkingsverbanden en utiliteiten. Te denken valt aan het verkorten van het cliëntenonderzoek en een daarbij gepaarde daling van kosten. Beschikbare data wordt als het ware hergebruikt en steeds geactualiseerd en verrijkt (datacirculatie en datamutualisatie).(283) Tegelijkertijd betekent dit ook dat herhaalde uitvragen naar klanten niet nodig zijn. Met betrekking tot TM-utiliteiten wordt nog gewezen op het feit dat met netwerkanalyses meer kan worden gezien dan een individuele bank dit zou kunnen. Zo is bijvoorbeeld in het kader van TMNL door FIU-NL al gewezen op de toegevoegde waarde voor het verhogen van de kwaliteit van meldingen van ongebruikelijke transacties.(284) Verder wordt ook wel gewezen op de mogelijke verhoogde efficiëntie van het transactiemonitoringproces, de verlaging van kosten door het gezamenlijk ontwikkelen en onderhouden van utiliteiten, en verbeterd risicomanagement.(285)

Bij de gezamenlijke voorzieningen die zijn geanalyseerd in deze verkenning is te zien dat deze uitsluitend door partijen uit de private sector worden opgezet en/of beheerd; de overheid heeft hier puur een ondersteunende rol, bijvoorbeeld door aanpassing van (interpretatie van) wet- en regelgeving of het geven van de mogelijkheid om te experimenteren. Verder valt op dat er een verschil zit tussen de soorten gezamenlijke voorzieningen op het gebied van CDD: waar sommige voorzieningen echt 'door en voor' de poortwachters zijn – al dan niet met ondersteuning van een platformbeheerder (KUBE, Invidem , O-KYC en gesloten gedeelde KYC-utiliteit in Letland) – zijn andere voorzieningen in feite diensten die door commerciële dienstverleners worden verleend aan wie poortwachters (een deel van) hun CDD-werkzaamheden kunnen uitbesteden (i-Hub KYC en open gedeelde KYC-utiliteiten in Letland).(286)

In het verleden zijn al meerdere initiatieven (voortijdig) beëindigd en ook de in dit onderzoek betrokken initiatieven bevinden zich in verschillende fases. Bij enkele initiatieven die gestopt of gepauzeerd zijn, of de pilotfase niet zijn ontstegen, wordt verwezen naar het feit dat het onderwerp technisch en operationeel gezien veel uitdagender bleek te zijn dan vooraf gedacht, en ook dat de gewenste schaalvoordelen niet gehaald konden worden.(287)

Het opzetten en operationeel krijgen van een utiliteit is dus geen sinecure. Uit de initiatieven en literatuur wordt duidelijk dat verschillende aspecten goed moeten worden doordacht. Daarbij gaat het om aspecten zoals:

- Technologie: welk technologisch platform wordt gebruikt? Gaat de voorkeur uit naar een centraal of decentraal platform? Elk type heeft voor- en nadelen. Zo wordt wel gezegd dat een gedecentraliseerd platform het voordeel heeft dat deelnemers beter in controle zijn van de data en dat dergelijke platformen minder risico's met zich meebrengen vanuit het perspectief van cybersecurity. In dat opzicht lijken decentrale platformen in de initiatieven de voorkeur te krijgen.(288) Veel gehoorde technologieën zijn de Distributed Ledger Technologie (DLT) en blockchaintechnologie, maar andere technologieën zijn niet uitgesloten: er is geen eenduidige oplossing die alle behoeftes vervult, ongeacht het land, het regelgevende kader en de omvang van (betrokken) instellingen.(289) Ook speelt bij het centraliseren van alle gegevens het kostenplaatje een rol: bijvoorbeeld bij het in 2018 gestopte KYC Utility-project in Singapore werd opgemerkt dat er hoge kosten verbonden waren aan het migreren van data naar een centraal platform.(290)

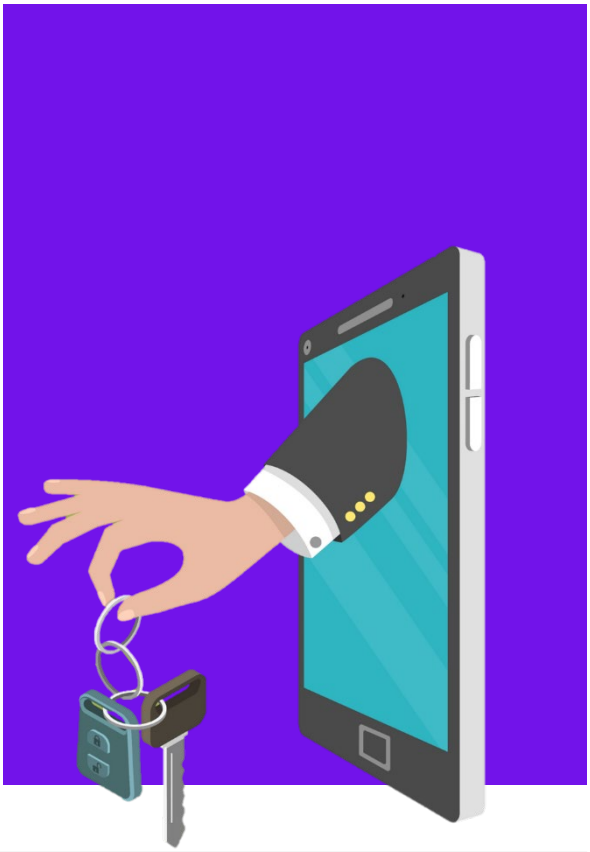
(283) Intesa, 'Progetto O-KYC, inizia la fase due', persbericht 5 oktober 2022.
(284) FIU 2023.
(285) BIS 2023, p. 80.
(286) Zie voor de uitwerking van de genoemde initiatieven bijlage B.
(287) ABS 2018, p. 1; M. Ciobanu, 'Interview Advancing modern financial crime prevention with KYC utilities – interview with Invidem', *ThePaypers* 25 juni 2021.
(288) Zetzsche et al. 2018, p. 140; N. Twomey, 'KYC Utilities: The Second Coming, Learning from Past Failures', *Finextra Blog* 13 november 2017; ABS 2018, p. 7.
(289) KPMG 2018, p. 6: "*(…) it is important to note that there is no one solution that will meet all needs, regardless of country, regulatory environment or size of institution*".
(290) ABS 2018, p. 7.

- Deelnemers: gezien de huidige kosten die gepaard gaan met het opzetten van een utiliteit, de omvang van de klantenportefeuille en mate van automatisering van cliëntprocessen is het niet vreemd dat de meeste initiatieven worden ontplooid in de bankensector. Voor elke utiliteit zal moeten worden nagedacht over de beoogde deelnemers: zijn dit financiële en/of niet-financiële instellingen, beperkt de utiliteit zich tot een sector of juist niet, en kan een utiliteit van toegevoegde waarde zijn op specifieke thema's, bijvoorbeeld vastgoed? Ook zal er sprake moeten zijn van onderling vertrouwen tussen deelnemers en de bereidheid om informatie met elkaar te delen.(291)
- Type informatie en actualisatie: vooraf zal goed moeten worden bedacht welke informatie gedeeld gaat worden. Huidige initiatieven laten zien dat het kan gaan om informatie die komt van de betrokken partijen zelf, maar ook om publieke informatie en informatie uit overheidsregisters zoals het UBO-register. Ook zal moeten worden nagedacht hoe vaak de informatie wordt geactualiseerd en door wie. Hierbij komen ook vragen op rondom aansprakelijkheid in het geval het fout gaat en de manier waarop dient te worden omgegaan met 'leverende' deelnemers en 'ontvangende' deelnemers.(292)
- Type klanten: in de onderzochte initiatieven zijn verschillende benaderingen waar te nemen: sommige initiatieven zijn gericht op zakelijke klanten, andere op natuurlijke personen. Het opzetten van een gezamenlijke voorziening op het gebied van CDD voor zakelijke klanten is complexer dan voor bijvoorbeeld 'mass retail' klanten (bijv. onderzoek naar de organisatiestructuur en UBO's, meerdere vertegenwoordigers en bestuurders); maar kan mogelijk wel meer opleveren voor deelnemers in termen van kostenreductie en verkorte doorlooptijden wanneer het cliëntenonderzoek kan worden gestandaardiseerd. Vooraf zal goed moeten worden nagedacht welke klanten in de reikwijdte van de utiliteit komen te vallen.
- Functies van de utiliteit: een gezamenlijke voorziening kan verschillende functies hebben. Het kan puur een kanaal zijn waar bestaande informatie door wordt geleid. Ook kan de utiliteit een rol hebben in de validatie van de gegevens die via de gezamenlijke voorziening worden gedeeld. Het i-Hub KYC Repository for Ongoing Due Diligence laat zelfs zien dat de KYC-utiliteit ook een rol kan spelen in de risicobeoordeling van de klant. Afhankelijk van de gewenste functies, zou ook kunnen worden nagedacht over de vraag of het voeren van het klantcontact wellicht door een KYC-utiliteit zou kunnen worden gedaan, bijvoorbeeld voor het verkrijgen van toestemming van de klant voor het delen van diens informatie via de utiliteit of het verzoek te doen actuele informatie aan te leveren.
- Datastandaardisatie: welke standaarden worden gebruikt voor het delen van data? Bepaalt elke deelnemer de eigen standaard of wordt toegewerkt naar een geharmoniseerde standaard? Ondanks dat dezelfde wet- en regelgeving van toepassing is, blijkt dat instellingen regelmatig andere informatie uitvragen. Uit het Invidem-initiatief, alsook het KYC-Utility-project uit Singapore blijkt dat een gedeelde datastandaard of taxonomie, samen met een goede datakwaliteit, als essentieel wordt gezien voor succesvolle informatiedeling.(293) Datastandaardisatie is ook van belang voor TM-utiliteiten.(294)
- Governance: de governance rondom een gezamenlijke voorziening is van fundamenteel belang. Daarbij spelen verschillende vragen: moet de voorziening een private onderneming zijn of beter een publieke organisatie? Kan het een organisatie met of zonder winstoogmerk zijn? Wie beheert de gezamenlijke voorziening op dagelijkse basis? Hebben de deelnemende partijen deelname- of stemrechten? Hoe worden nieuwe leden toegelaten en wie besluit dat?(295) Ook hier rijst de vraag wie aansprakelijk is in het geval het fout gaat.

(291) BIS 2023, p. 80.
(292) ABS 2018, p. 6.
(293) M. Ciobanu, 'Interview Advancing modern financial crime prevention with KYC utilities – interview with Invidem', *ThePaypers* 25 juni 2021; ABS 2018, p. 4; N. Twomey, 'KYC Utilities: The Second Coming, Learning from Past Failures', *Finextra Blog* 13 november 2017; Zetzsche et al. 2018, p. 141.
(294) BIS 2023, p. 80.
(295) Zie ook Zetzsche et al. 2018, p. 142.

Kijkend naar Letland en Luxemburg – waar het vooral om (van poortwachters) onafhankelijke dienstverleners gaat – kan het voor de overheid nog relevant zijn om te beoordelen of een vergunningenregime geïntroduceerd moet worden, al dan niet met toezicht door bijvoorbeeld een privacytoezichthouder.

- Privacy: het ontwerp en de operationalisering van een gezamenlijke voorziening moeten niet uitsluitend worden beschouwd vanuit het perspectief van de bestrijding van financieel-economische criminaliteit. Het delen van gegevens brengt risico's op verschillende vlakken met zich mee, in het bijzonder op het vlak van privacy. In dit kader is ook wel gesteld: *"Knowledge is power, and where there is a lot of knowledge, there is a lot of power".*(296) De initiatieven laten zien dat privacy op verschillende wijzen kan worden meegenomen. In TMNL worden gegevens bijvoorbeeld gepseudonimiseerd. Verschillende andere initiatieven steunen op het toestemmingsprincipe: de klant bepaalt wie welke gegevens (niet meer) te zien mag krijgen. Ook andere privacy-bevorderende maatregelen, zoals de aanstelling van een privacy officer en dataminimalisatie, worden in de initiatieven toegepast.(297)
- Intellectueel eigendom, mededinging, cybersecurity: ook deze aspecten moeten worden meegenomen bij de ontwikkeling van een KYC-utiliteit. Daarbij is ook van belang wie verantwoordelijk is voor deze aspecten en wie hier toezicht op houdt.
- Samenwerking met de overheid: verschillende initiatieven laten een interactie met de overheid zien. Een duidelijke 'lesson learned' bij het KYC Utility-project in Singapore is dat een gezamenlijke voorziening weinig kans van slagen heeft wanneer er geen intensieve publiek-private samenwerking plaatsvindt.(298) In het rapport over het KYC Utility-project wordt verwezen naar de meewerkende houding van publieke partijen bij het zoeken naar de bronnen ('golden sources').(299) Ook is de overheid belangrijk in het geval aanpassing van wet- en regelgeving, of interpretatie daarvan, nodig is. Ook de BIS benadrukt het belang van samenwerking tussen de private sector en overheid bij het ontwikkelen van utiliteiten.(300) De kritische houding van de AP jegens de gemeenschappelijke transactiemonitoring van banken in het kader van TMNL bevestigt nog maar eens het belang van een goede samenwerking met de overheid: een samenwerking die van twee kanten moet komen.(301) In het verlengde hiervan toont dit ook het belang dat de overheid met één stem spreekt en een duidelijke afweging durft te maken tussen (potentieel) conflicterende belangen.(302)
- Kosten: tot slot moet niet vergeten worden dat keuzes die worden gemaakt in relatie tot bovenstaande elementen een impact hebben op de kosten. Het gaat daarbij bijvoorbeeld om opstartkosten van de utiliteit en doorlopende (operationele) kosten. Het is belangrijk om continu de balans tussen kosten en baten in het oog te houden. Ook zal aandacht moeten worden besteed aan de vraag wie de kosten draagt en of duurzame financiering voor de utiliteit gegarandeerd kan worden.



(296) Zetzsche et al. 2018, p. 142.
(297) Zie verder ook BIS 2023, p. 48-63.
(298) ABS 2018, p. 6.
(299) ABS 2018, p. 5.
(300) BIS 2023, p. 14 en p. 72.
(301) Zie voor de kritische houding van de Autoriteit Persoonsgegevens paragraaf 3.2.5 van dit rapport.
(302) RUSI 2022, p. 95.

Belangrijke lessen voor het inrichten van een gezamenlijke voorziening op basis van initiatieven

Op basis van de reeds bestaande initiatieven rondom utiliteiten kunnen enkele belangrijke lessen worden getrokken:

1. Begin klein en laat het initiatief groeien.

- *Beperk de kring van deelnemers bij de start*: effectiviteit en efficiëntie zijn belangrijke factoren en kunnen het beste worden behaald wanneer zo veel mogelijk partijen meedoen. Tegelijkertijd komen er veel aspecten kijken bij de ontwikkeling van een gezamenlijke voorziening en wordt het lastiger om overeenstemming te bereiken over deze aspecten wanneer meer partijen deelnemen.
- *Beperk de functies van een eventuele utiliteit*: hoe meer functies een utiliteit dient te vervullen, hoe meer data het moet verwerken, des te complexer, duurder en risicovoller het project wordt.(303)

2. Houd het (juridisch) zo simpel mogelijk.

Hoe juridisch complexer, des te groter de kans op falen. Begin in ieder geval uitsluitend met gereguleerde instellingen – instellingen met een vergunning- en/of een registratieplicht. Voor instellingen die gebonden zijn aan (beroeps)geheimhouding moet worden bekeken of zij in ieder geval informatie kunnen 'halen'. Tot slot lijkt het verstandig om de reikwijdte van een eventuele gezamenlijke voorziening in eerste instantie binnen de landsgrenzen te laten.(304)

3. Zorg voor de juiste betrokkenheid vroeg in het proces.

Een gezamenlijke voorziening op het gebied van CDD heeft de grootste kans van slagen bij vroege betrokkenheid van hoger leidinggevend personeel van instellingen, en van relevante publieke partijen.

Inzichten op basis van waarschuwingssysteem IFI

Het Incidentenwaarschuwingssysteem Financiële Instellingen toont aan dat informatie-uitwisseling tussen verschillende (afgebakende) groepen partijen uit de private sector met als doel het effectiever voorkomen en bestrijden van misbruik van het financieel stelsel – in dit geval fraude en misleiding – mogelijk is. Belangrijk vanuit het oogpunt van privacy is dat de informatie-uitwisseling proportioneel en subsidiair is, en dat ook de opzet van het systeem voldoende waarborgen kent. Vanwege de verwerking van strafrechtelijke gegevens in het extern verwijzingsregister (EVR) heeft het AP het Protocol Incidenten-waarschuwingssysteem Financiële Instellingen beoordeeld en een vergunning afgegeven.

Een van de succesfactoren in het kader van de IFI lijkt de decentrale aard van informatie-uitwisseling te zijn: deelnemers blijven zelf verantwoordelijk voor de gegevens die zij van personen opnemen in het intern verwijzingsregister (IVR) of EVR (waar van toepassing) en wisselen uitsluitend informatie op een 'need-to-know' basis met elkaar uit (dataminimalisatie). Andere relevante factoren lijken te zijn:

- Reikwijdte van het waarschuwingssysteem. In dit geval is de reikwijdte van de verwerking van gegevens nationaal. Internationale gegevensuitwisseling, met name buiten de EU, compliceert het waarschuwingssysteem aanzienlijk.
- Afgebakende groep deelnemers. Deelnemers aan het IFI zijn uitsluitend financiële instellingen met vergunning op grond van Nederlandse financiële wet- en regelgeving en de vijf betrokken brancheorganisaties. Omdat het gereguleerde instellingen zijn, is de groep van deelnemers op voorhand afgebakend en wordt niet het risico gelopen dat de kring van deelnemers wijder wordt dan strikt noodzakelijk.
- Heldere governance. Hierbij gaat het onder andere om de rollen en verantwoordelijkheden van deelnemers en brancheverenigingen, de instelling van een begeleidingscommissie en vastlegging van het proces voor toetreding tot, en uittreding uit, IFI. Ook dient het voor de betrokkenen (personen wiens gegevens zijn opgenomen in de registers) duidelijk te zijn wie waarvoor verantwoordelijk is bij de verwerking van persoonsgegevens, zodat de betrokkenen weten waar ze terecht kunnen met vragen, verzoeken en klachten.

(303) Zie ook ABS 2018, p. 9.

(304) ABS 2018, p. 8.

- Toetsingssystematiek en stapsgewijze opbouw van het verwerkingsproces. Dit betreft in de eerste plaats opname in de interne registers, met de mogelijkheid voor ernstige(re) gevallen om opgenomen te worden in externe registers. Primair vindt informatiedeling plaats op basis van 'hit – no hit' . De verspreiding van informatie over verdere details van het incident wordt beperkt tot een afgebakende groep geautoriseerde personen (Veiligheidszaken) en vindt uitsluitend plaats na een eigen toetsing door de afdeling Veiligheidszaken van de bevraagde instelling aan het proportionaliteits- en subsidiariteitsbeginsel.
- Duidelijke rechten en verplichtingen voor deelnemers. Dit betreft onder meer eisen rondom de geheimhouding, beveiliging van gegevens, documentatie/vastlegging van de genomen acties en beoordelingen.
- Duidelijke vastlegging van rechten voor betrokkenen. Dit betreft onder andere het recht om geïnformeerd te worden en de mogelijkheid van een bezwaar- en geschillenprocedure. Ook hebben betrokkenen het recht om toegang tot financiële basisproducten te blijven houden.

4.3 De ontwikkeling en het gebruik van digitale identiteiten en authenticatiemiddelen

4.3.1 Digitale identiteiten en het anti-witwasbeleid

Een digitale identiteit, ook wel e-ID, is een digitale verantwoording waarmee de identiteit van een persoon kan worden gecontroleerd.(305) De hoeveelheid informatie die met de digitale identiteit wordt verzameld hangt af van het type digitale identiteit en de werking van het systeem. Een digitale identiteit kan zich beperken tot primair identificerende informatie zoals de voor- en achternamen, geboorteplaats en -datum en adresgegevens. Een e-ID kan ook de vorm hebben van een digitale portemonnee en aanvullende persoonsgegevens en herleidbare informatie bevatten.(306) Hierbij valt te denken aan informatie over reisdocumenten, rijbewijzen en de burgerlijke status, maar ook over opleiding en diploma's, financiële gegevens en gezondheid.

Digitale identiteiten zijn op zichzelf geen nieuw fenomeen en worden al langer gebruikt, vooral door overheden. Daarom zijn veel digitale identiteiten tot op heden ontwikkeld door en voor overheden zelf. Een voorbeeld dicht bij huis is de DigiD, dat al sinds 2005 door burgers in Nederland kan worden gebruikt om in te loggen bij overheidsinstanties of organisaties met een publieke functie (bijv. pensioenfondsen). Digitale identiteiten zijn tot op heden vooral ontwikkeld voor natuurlijke personen en nog in mindere mate voor bedrijven, al zijn hier enkele voorbeelden van zoals eHerkenning. De introductie van de wereldwijde Legal Entity Identifier (LEI) in 2012 als reactie op de financiële crisis is echter een belangrijke push geweest voor de ontwikkeling van *corporate digital identities*.(307) Ook zal de Europese digitale identiteit, zoals beschreven in bijlage B, voor ondernemingen naar verwachting per 2025 beschikbaar komen.(308)

De identificatie en verificatie van de identiteit van klanten is een belangrijk onderdeel van het cliëntenonderzoek, waarbij digitale identiteiten en toepassingen een steeds grotere rol spelen. Het aangaan van zakelijke relaties op afstand, ook wel 'non-face-to-face' of 'remote onboarding' genoemd, vindt steeds vaker plaats. De COVID-crisis wordt gezien als een belangrijke recente aanjager van deze ontwikkeling.(309) Bij het aangaan van zakelijke relaties op afstand valt te denken aan het openen van bankrekeningen of het afsluiten van verzekeringen via mobiele apps. Ook worden steeds meer innovatieve technologieën ontwikkeld om het aangaan van zakelijke relaties op afstand te faciliteren. Hierbij kan gedacht worden aan het identificeren en verifiëren van de identiteit van klanten via videobellen, het digitaal ondertekenen van documenten en biometrische technologie. Deze technologieën worden ook steeds vaker ontwikkeld en aangeboden door commerciële partijen.

(305) FATF 2020, p. 19.
(306) Voorbeeld is de digitale identiteit die in Europa ontwikkeld wordt: Europese Commissie, 'De architectuur en het referentiekader voor de Europese portemonnee voor digitale identiteit', nieuwsbericht 10 februari 2023.
(307) Zie voor meer informatie over het ontstaan en de werking van LEI: Leung et al. 2022, p. 16-24.
(308) Europese Commissie, *Een digitale identiteit voor alle Europeanen*, beschikbaar via deze link.
(309) European Banking Authority, *Richtsnoeren voor onboarding klanten op afstand*, EBA/GL/2022/15, 22 november 2022, beschikbaar via deze link, p. 4.

In de literatuur wordt gewezen op de mogelijke voordelen van digitale identiteiten. Zo worden deze bij uitstek gezien als middel voor financiële inclusie, bijvoorbeeld voor vluchtelingen, armen of kleine ondernemingen.(310) De FATF wijst erop dat digitale ID-systemen met hoge betrouwbaarheidsniveaus in potentie de betrouwbaarheid, veiligheid, privacy en het gemak van identificatie van natuurlijke personen bij een breed palet van dienstverlening kunnen verbeteren.(311) Specifiek in relatie tot KYC-processen en het cliëntenonderzoek wordt wel gewezen op de mogelijkheid om processen rondom de identificatie en de verificatie van de identiteit van klanten en UBO's te versimpelen, op versnelde doorlooptijden en daarmee ook verlaagde kosten voor klanten.(312)

Tevens wordt gewezen op lagere risico's op fouten (als gevolg van handmatige verwerking van de gegevens) en inconsistenties bij beoordelingen door werknemers wanneer digitale identiteiten worden gebruikt.(313) Voor instellingen bieden deze operationele efficiënties de gelegenheid om schaarse middelen te gebruiken voor andere doeleinden. Wanneer digitale identiteiten actueel gehouden worden, wordt ook gewezen op de voordelen bij het monitoren van de zakelijke relatie, bijvoorbeeld in transactiemonitoring, waar veranderingen direct meegenomen kunnen worden.(314)

Tegelijkertijd zijn er risico's verbonden aan het gebruik van digitale identiteiten. Daarbij gaat het in het bijzonder om zaken zoals cyberveiligheid, privacy en fraude.(315) Daarom wordt in verschillende landen gewerkt aan betrouwbaarheidskaders ('assurance frameworks') en technische standaarden voor digitale identiteiten en oplossingen. Hoe hoger het betrouwbaarheidsniveau en de veiligheid, des te meer vertrouwen kan worden gesteld in het elektronische identificatiemiddel. Door de FATF, Europese en nationale wetgevers worden voorwaarden neergelegd in wet- en regelgeving voor het gebruik van digitale identiteiten en toepassingen. Zo staat de Wwft het sinds mei 2020 toe dat instellingen bij het cliëntenonderzoek gebruikmaken van elektronische identificatie-middelen om de identiteit van cliënten vast te stellen en te verifiëren, mits deze middelen voldoen aan een substantieel of hoog betrouwbaar-heidsniveau.(316)

Ook worden aan de eerder genoemde uitbesteding en het introducerend cliëntenonderzoek verschillende eisen gesteld en blijft de verantwoordelijkheid voor de naleving van de Wwft (en Sw) bij de poortwachter zelf.(317) Tot slot hebben ook toezichthouders steeds meer aandacht voor het gebruik van digitale identiteiten en toepassingen.(318)

In bijlage B zijn twee buitenlandse initiatieven met betrekking tot digitale identiteiten verder uitgewerkt. Dit betreft zowel een privaat initiatief (Australia Post Digital iD) als een initiatief van overheidswege (Singpass/MyInfo uit Singapore). Daarnaast is in de verkenning ook aandacht besteed aan de aanstaande wijzigingen van de eIDAS-verordening in de Europese Unie, aangezien deze direct werkende Europese regelgeving in belangrijke mate het regelgevende landschap rondom digitale identiteiten en technologieën zal bepalen. Daarbij zijn ook bestaande commerciële oplossingen in Nederland betrokken. Ook deze uitwerking is te vinden in bijlage B van dit onderzoeksrapport.

4.3.2 Verkregen inzichten

De ontwikkelingen rondom (het gebruik van) digitale identiteiten in de EU, in het bijzonder gedreven door de Europese Commissie, bieden potentie voor het gebruik daarvan in de context van het cliëntenonderzoek en transactiemonitoring.

Het betreft een ontwikkeling los van – maar gekenmerkt door grote overeenkomsten met – de ontwikkeling van meer private samenwerking en informatiedeling zoals geschetst in paragraaf 4.2.

(310) Zetzsche et al. 2018, p. 133; Rainey et al. 2019; Leung et al. 2022, p. 10-11; FATF 2020, p. 14; CGAP 2019.
(311) FATF 2020, p. 13.
(312) Leung et al. 2022, p. 10; FATF 2020, p. 14; DNB 2022, p. 29.
(313) Leung et al. 2022, p. 10.
(314) Leung et al. 2022, p. 11.
(315) FATF 2020, p. 14; Leung et al. 2022, p. 28; ASPI 2022, p. 8-11.
(316) Artikel 11(1) eerste volzin Wwft juncto artikel 4(1) sub h Uitvoeringsregeling Wwft. Artikel 4(1) sub h Uitvoeringsregeling Wwft is per mei 2020 toegevoegd met de implementatie van de AMLD5: Implementatieregeling wijziging vierde anti-witwasrichtlijn, *Stb.* 2020, 47198.
(317) Zie artikelen 5 en 10 Wwft en ter illustratie DNB, *Leidraad Wwft/Sw,* september 2022, beschikbaar via deze link, p. 32-34 en 53-54.
(318) Zie bijvoorbeeld EBA, Richtsnoeren voor onboarding klanten op afstand, EBA/GL/2022/15, 22 november 2022, beschikbaar via deze link.

Waar het bij gezamenlijke voorzieningen op het gebied van (aspecten van) CDD gaat om onder andere persoonsgegevens die door de private sector bijeen worden gebracht op basis van eigen verkregen (en geverifieerde) informatie en uit overheidsregisters, worden ook binnen de digitale identiteit persoonsgegevens, 'eigen' informatie en overheidsgegevens gecombineerd. Een andere overeenkomst is dat voor gebruik van gegevens de toestemming van de betrokken persoon vereist wordt.

De initiatieven in Australië en Singapore, maar ook de huidige mogelijkheden in Europa, tonen dat zowel private als publieke partijen een belangrijke rol kunnen spelen. Naast de DigiD en eHerkenning zijn er in Nederland al meerdere private en commerciële aanbieders op het gebied van digitale identiteit, authenticatiemiddelen (waaronder digitale handtekening) en digitaal administratiebeheer.

Digitale identiteiten lijken momenteel nog voornamelijk gericht op natuurlijke personen; de voorgenomen digitale identiteit met portemonnee voor rechtspersonen lijkt een kans te zijn om CDD- en transactiemonitoringprocessen voor bedrijven efficiënter te maken.

De ervaringen met Singpass/MyInfo tonen één duidelijke 'lesson learned' voor digitale identiteiten en het gebruik daarvan voor CDD- en transactiemonitoringsdoeleinden. Om hierin te slagen is een ondersteunende overheid nodig die de ontwikkeling van de digitale identiteit, en het gebruik daarvan, zowel technologisch als juridisch mogelijk maakt. Zo stelt de Singaporese overheid alle broninformatie over de architectuur, de werking van de API en voorwaarden voor gebruik van Singpass/MyInfo open aan eenieder. De financieel toezichthouder Monetary Authority of Singapore maakt het voor financiële instellingen mogelijk om op specifieke identiteitsgegevens uit de digitale identiteit te steunen, zonder andere aanvullende onderzoeksactiviteiten te ondernemen.

4.4 Publiek-private samenwerking in Nederland

4.4.1 Samenwerking tussen publieke en private partijen

Zoals aangegeven in paragraaf 4.2 wordt informatiedeling gezien als een belangrijke hoeksteen voor een effectief anti-witwasbeleid. Publiek-private samenwerkingen (hierna ook: PPS) zijn veelal vormen van samenwerking binnen een specifiek kader tussen opsporing, FIU en de private sector, mogelijk aangevuld met partijen zoals ministeries, toezichthouders en beroepsorganisaties. In potentie kunnen PPS poortwachters helpen om hun interne processen zoals de transactiemonitoring te verbeteren en hun cliëntenonderzoek gerichter uit te voeren.(319)

Binnen de EU zijn PPS-verbanden in opmars, hoewel de structuur, doelstellingen, deelnemers en het type informatie dat wordt uitgewisseld, verschillen.(320) De Europese Commissie stelt dat PPS binnen het anti-witwasbeleid in het algemeen voor twee doeleinden worden opgezet:

- Het delen van strategische informatie tussen FIU en poortwachters op fenomeenbasis (bijvoorbeeld typologieën, trends en risico-indicatoren) of op specifieke basis (feedback op FIU-meldingen); en
- Het delen van operationele informatie tussen publieke partijen en poortwachters over personen of zaken die van belang kunnen zijn voor opsporing.(321)

Bij samenwerking in de vorm van PPS wordt in de literatuur aandacht gevraagd voor enkele (juridische) aspecten. Het gaat hierbij om privacy en de juridische mogelijkheden voor informatie-uitwisseling, de impact van informatiedeling op keuzes van betrokken partijen om bepaalde categorieën klanten niet te accepteren of de relatie te beëindigen ('de-risking'), en de rechten van verdachten in strafrechtelijke procedures.(322)

(319) Europese Commissie 2022a, p. 20.
(320) Europese Commissie 2022a, p. 2; Vogel 2022, p. 52. Ter illustratie: op 22 juni 2023 is bekend gemaakt dat in het Verenigd Koninkrijk twee pilots voorbereid worden voor meer datadeling tussen banken en publieke partijen. Voor een van de projecten is aangegeven dat het om een vorm van 'TMNL lite' gaat: I. Withers en K. Ridley, 'BREAKING: Six British banks to share fincrime information in a 'game changer' plan to crack down on money laundering; Lloyds, NatWest already involved in trials', *AML Intelligence* 22 juni 2023.
(321) Europese Commissie 2022a, p. 2-3. Zie ook Vogel 2022, p. 54.
(322) Vogel 2022, p. 56.

Uit onderzoek naar PPS in de bredere context van ondermijnende criminaliteit in Nederland blijkt tevens dat aspecten zoals de onderlinge samenhang tussen verschillende PPS-initiatieven, bewaken van gelijkwaardigheid in de relatie tussen publieke en private partners, en het voorkomen van complexiteit in de opzet van de samenwerking en de governance (bijvoorbeeld stroperige besluitvorming en polderen) relevant zijn.(323)

PPS worden vooralsnog voornamelijk nationaal opgezet, hoewel het Europol Financial Intelligence Public-Private Partnership project (EFIPPP) de eerste en meest bekende uitzondering daarop is.(324) Een tweede voorbeeld betreft de J5 waar in 2022 een start is gemaakt met publiek-private samenwerking tussen fiscale opsporingsdiensten en de grootste banken op het gebied van belastingcriminaliteit.(325)

In de FATF-evaluatie van Nederland roemt de FATF de publiek-private samenwerkingsinitiatieven.(326) Tegelijkertijd wordt wel gewezen op beperkingen vanuit het perspectief van privacy.(327)

In het kader van dit onderzoek zijn vier relevante Nederlandse PPS-initiatieven met verschillende deelnemers, doelstellingen en reikwijdtes nader verkend. Het gaat om Fintell Alliance NL, het Financieel Expertise Centrum (FEC), het Anti-Money Laundering Centre (AMLC) en het Landelijk Informatie- en Expertise Centrum (LIEC) en de Regionale Informatie- en Expertise Centra (RIEC's). De uitwerking van deze initiatieven is opgenomen in bijlage B van dit onderzoeksrapport.

4.4.2 Verkregen inzichten

De PPS geschetst in Nederland laten elk een andere vorm van publiek-private samenwerking zien:

De Fintell Alliance NL is een initiatief gericht op het uitwisselen van kennis en het versterken van de effectiviteit van het melden van ongebruikelijke transacties – op basis van de bestaande wettelijke mogelijkheden – tussen FIU-NL en zes banken. Medewerkers van FIU-NL en de deelnemende banken werken daarbij samen op één fysieke locatie. Begonnen als pilot, is het in 2021 opgeschaald naar een structureel PPS-verband vastgelegd in een alliantiedocument. Juridische beperkingen zijn aanwezig – waaronder het uitsluitend bilateraal (bank-FIU) kunnen delen van analyses(328) – maar FIU-NL en deelnemende banken hebben een manier gevonden om samen te werken binnen deze wettelijke kaders. Opsporingsautoriteiten zijn niet direct bij deze PPS betrokken, maar kunnen via het ter beschikking stellen van de uitkomsten van het werk binnen Fintell Alliance NL aan FEC-taskforces en -projecten wel kennisnemen en gebruikmaken van dit werk.(329) In de eindevaluatie over de Serious Crime Taskforce (SCTF) wordt Fintell Alliance positief bejegend voor het werk dat Fintell Alliance aan de SCTF oplevert.(330)

De FEC-PPS-samenwerking is ook gestart met pilots, en nadien vastgelegd in verschillende convenanten. Het richt zich vooral op informatiedeling tussen opsporingsinstanties, FIU-NL en verschillende banken. De informatiedeling in de taskforces SCTF en TFTF vindt plaats binnen de wettelijke kaders, hoewel ook hier de beperking speelt dat banken uitsluitend bilateraal met FIU-NL hun analyses kunnen delen. De FEC-PPS systematiek is dat opsporing – in afstemming met het OM – bepaalde 'intelligence' deelt met banken en FIU-NL. Banken kunnen deze informatie door hun systemen halen, daar mogelijk ongebruikelijke transacties identificeren en deze melden. FIU-NL kan de meldingen verdacht verklaren en zodoende beschikbaar stellen aan de opsporingsinstanties. Uit de eindevaluatie van de SCTF komen enkele interessante aspecten ten aanzien van de samenwerking en verhouding tussen publieke en private partijen aan bod:

(323) Nelen et al. 2023, p. 190-191.
(324) Europol, *European Financial and Economic Crime Centre – EFECC*, beschikbaar via deze link.
(325) J5 is een afkorting die staat voor Joint Chiefs of Global Tax Enforcement van vijf internationale fiscale opsporingsdiensten (Australië, Canada, Nederland, Verenigd Koninkrijk en de Verenigde Staten). Zie over de Global Financial Institution Summit in de J5-context: HM Revenue & Customs en HM Treasury, 'Tax crime chiefs summit commits to international action', persbericht 13 mei 2022.
(326) Zie FATF 2022b.
(327) Openbaar Ministerie 2022, p. 18.
(328) Eindevaluatie pilot Serious Crime Task Force (SCTF), Kamerstukken II, 2020/2021, 31 477, nr. 60, bijlage, p.15.
(329) FATF 2022b, p. 59.
(330) Eindevaluatie pilot Serious Crime Task Force (SCTF), Kamerstukken II, 2020/2021, 31 477, nr. 60, bijlage, p.15 en 22-23.

- Door de banken wordt ervaren dat de betrokken overheidspartijen te dominant, en daardoor niet altijd even transparant, zijn.(331) Dit draagt niet bij aan het vertrouwen.
- Aan de zijde van de banken leeft voorts enig ongemak en irritatie over de verhouding met de publieke partijen, geïllustreerd door de strafrechtelijke vervolgingen van banken de afgelopen jaren: *"Het staat haaks op vertrouwen en samenwerken, en dat is denk ik de grote discussie. Want hoe ga je met elkaar criminaliteit bestrijden als banken in de tussentijd ook zelf bestreden worden?"*.(332) Dat dit in bredere zin een knelpunt is dat ervaren wordt door poortwachters is in paragraaf 3.3.2 aan de orde gekomen.
- Wat betreft een mogelijke uitbreiding is gewezen op andere poortwachters die relevant zouden kunnen zijn voor het werk en de doelstelling van het SCTF. Zo worden de trustsector, het notariaat, de advocatuur, moneytransferbedrijven en betaaldienstverleners genoemd.(333) Voor de toetreding van private partners tot het SCTF wordt wel aangegeven dat deze te complex is: toetreding vereist instemming van de FEC-Raad, een aanpassing van het convenant en een apart besluit op grond van artikel 20 Wpg.(334) In de toekomst zal de WGS van invloed zijn op de toetreding van (nieuwe) private partijen bij PPS.(335)

In 2022 is binnen het FEC opvolging gegeven aan de aanbevelingen die voortvloeiden uit de eindevaluatie. Er is *"een 'gedeeld beeld' ontwikkeld over het doel (common object), de richting (common intent) en de kernwaarden (key principles) van de FEC PPS"*.(336) Het FEC wijst daarbij op de wijze waarop met elkaar gesproken is en stelt vast dat *"[d]aarmee […] verder begrip en vertrouwen [is] ontstaan, wat eveneens een stevige basis is voor een duurzaam vervolg van de FEC PPS"*.(337)

De FATF meent dat het AMLC een unieke positie heeft in het nationale anti-witwaslandschap.(338) Door het AMLC binnen de FIOD te positioneren, heeft het toegang tot veel opsporingsdata. Deze opsporingsdata kan het AMLC combineren met openbare informatie en – al dan niet in samenwerking met de private partners – vertalen naar nuttige informatie over witwasfenomenen en -typologieën voor poortwachters en de maatschappij in brede zin. Naast de toegevoegde waarde van de organisatie richting de publieke partijen bij het verrijken en analyseren van informatie ten behoeve van strafrechtelijke (voor)onderzoeken, lijkt het AMLC een belangrijke rol te kunnen vervullen in de door poortwachters gewenste feedback.

Het RIEC-LIEC is primair een publiek-publieke vorm van samenwerking vanuit een breder perspectief van ondermijning en georganiseerde criminaliteit. Het RIEC-LIEC-bestel heeft ook een sterke focus op regionale problematiek. In de bredere reikwijdte en de focus (ook) op regionale problematiek onderscheidt het LIEC-RIEC zich van de andere PPS-initiatieven hiervoor genoemd. Witwassen is een belangrijk thema binnen RIEC-LIEC. Publiek-private samenwerking is niet beperkt tot poortwachters, en vindt vooral plaats in de vorm van het delen van kennis en expertise in bijvoorbeeld fenomeentafels en bewustwordingsbijeenkomsten. Ook op projectbasis wordt samengewerkt tussen publieke en private partijen. Daarover is wel opgemerkt dat het feit dat niet altijd alle (private) projectpartners zijn aangesloten bij het RIEC-convenant de mogelijkheid tot informatie-uitwisseling bemoeilijkt.(339) Een andere beperking voor informatiedeling is de rechtsvorm van de RIEC's. Het RIEC is geen zelfstandige entiteit waar informatie mee kan worden gedeeld; het RIEC kan hoogstens als intermediair dienen.(340)

De PPS-initiatieven in Nederland laten zien dat publiek-private samenwerking verschillende doelen heeft.

(331) Eindevaluatie pilot Serious Crime Task Force (SCTF), Kamerstukken II, 2020/2021, 31 477, nr. 60, bijlage, p. 10. Uit de literatuur blijkt dit ook een aandachtspunt voor PPS in de bredere context van georganiseerde criminaliteit: Nelen et al. 2023, p. 139 stellen: *"[….] dat publiek-private samenwerkingsverbanden aan kracht en dynamiek inboeten zodra de publieke partijen daarin te nadrukkelijk de boventoon en regie gaan voeren"*.
(332) Eindevaluatie pilot Serious Crime Task Force (SCTF), Kamerstukken II, *2020/2021*, 31 477, nr. 60, bijlage, p. 19.
(333) Eindevaluatie pilot Serious Crime Task Force (SCTF), Kamerstukken II, 2020/2021, 31 477, nr. 60, bijlage, p. 37.
(334) Eindevaluatie pilot Serious Crime Task Force (SCTF), Kamerstukken II, 2020/2021, 31 477, nr. 60, bijlage, p. 27.
(335) Zie paragraaf 3.2.5.
(336) FEC 2022, p. 18.
(337) FEC 2022, p. 18.
(338) FATF 2022b, p.60.
(339) Nelen et al. 2023, p. 80-81.
(340) Arena Consulting & Pro Facto 2022, p. 63.

PPS kan plaatsvinden op operationeel niveau, met als doel het samenbrengen van informatie (netwerken) om witwassen en terrorismefinanciering effectiever te bestrijden. Fintell Alliance en de taskforces in de FEC-PPS zijn hier duidelijke voorbeelden van. PPS kan ook op fenomeenniveau plaatsvinden en tot doel hebben om kennis over fenomenen, trends en 'good practices' te delen. Het AMLC is hier een goed voorbeeld van. Wat opvalt is dat de focus voor PPS op operationeel niveau voornamelijk plaatsvindt met banken. Hoewel begrijpelijk gezien de hoeveelheid meldingen van ongebruikelijke transacties door banken en de focus vanuit de overheid op deze poortwachtersgroep, zijn de positieve ervaringen die worden opgedaan (waaronder betere kwaliteit meldingen en een kortere feedbackloop) mogelijk ook waardevol voor andere poortwachters. Samenwerking met andere groepen poortwachters zoals notarissen en makelaars vindt vooral plaats binnen/met het AMLC en in breder RIEC-LIEC-verband.

Uit de bestaande PPS-initiatieven betrokken in deze verkenning kunnen enkele lessen getrokken worden:

1. Eerst testen, dan bestendigen. PPS start doorgaans met een pilot, waarna dit bij succes wordt opgeschaald.
2. Gelijkwaardigheid. PPS staat of valt met vertrouwen en ervaren veiligheid; daarvoor zijn een gelijkwaardige relatie, commitment, begrip en voldoende transparantie – voor zover mogelijk binnen de wettelijke kaders tussen publieke en private partners belangrijk. Ook is een evenredige inzet qua middelen en mensen een belangrijk aspect. Samengevat moet *"[d]e samenwerking […] geen overheidsfeestje zijn waarvoor de private partijen toevallig ook zijn uitgenodigd".*(341)
3. Heldere governance en duidelijke vastlegging van doelen, partijen, en wederzijdse rollen en verantwoordelijkheden. Convenanten zijn een veelgebruikt middel bij PPS. De drempel voor (private) partijen om toe te treden tot PPS-initiatieven moet niet te hoog liggen. Er moet voor worden gewaakt dat de effectiviteit van PPS niet beperkt wordt door een grote hoeveelheid samenwerkingsvormen of initiatieven, alsook een complexe governance waarin overleg in plaats van actie de boventoon voert.

4.5 Centrale sturing overheid

4.5.1 De sturing van het anti-witwasbeleid in Nederland

Voor een centrale sturing is het hebben van een strategie gebaseerd op een nationale risicobeoordeling belangrijk. Een goede strategie stelt kaders, geeft richting en stelt in staat om prioriteiten aan te brengen. Als reactie op verscheidene witwasschandalen waarbij Europese banken betrokken waren, boden de ministers van Financiën en Justitie en Veiligheid in 2019 een gezamenlijk plan van aanpak witwassen aan de Tweede Kamer aan.(342) In oktober 2022 leidde dit plan tot het wetsvoorstel, eerder genoemd in paragrafen 3.2.1 en 3.2.5.

In september 2022 hebben de ministers van Financiën en Justitie en Veiligheid de beleidsagenda aanpak witwassen aan de Kamer toegestuurd.(343) De beleidsagenda is gebaseerd op verschillende onderzoeken naar het Nederlandse anti-witwasbeleid en aanbevelingen die daaruit volgen.(344) Aan de hand van deze onderzoeken hebben de ministers drie thema's opgenomen in de beleidsagenda: 1) streng waar nodig, 2) ruimte waar mogelijk, en 3) meten om te weten. Op het hoogste niveau zien de eerste twee thema's op de risicogebaseerde benadering en thema drie op het inzichtelijk maken van de effectiviteit van het anti-witwasbeleid. Elk thema kent subthema's waar voorgenomen activiteiten aan zijn gekoppeld. In totaal bevat de beleidsagenda 31 activiteiten. Uit de Kamerbrief van de minister van Justitie en Veiligheid over de aanpak van georganiseerde criminaliteit uit april 2022 blijkt dat het voorkomen en bestrijden van witwassen deel uitmaakt van een bredere aanpak van criminaliteit door de overheid.(345)

(341) Nelen et al. 2023, p. 139.
(342) Kamerstukken II, 2018/2019, 31 477, nr. 41.
(343) Kamerstukken II, 2022/2023, 31 477, nr. 80. De beleidsagenda betreft bijlage 1.
(344) Bijlage 2 bij de beleidsagenda.
(345) Kamerstukken II, 2021/2022, 29 911, nr. 348, p. 5.

Desalniettemin blijkt uit hoofdstuk 3 een duidelijke behoefte aan een overheid die (meer) centraal aanstuurt, meer met één stem spreekt, duidelijke keuzes maakt en prioriteert. Verschillende knelpunten die worden ervaren door poortwachters en klanten zijn te herleiden tot dit punt. Om na te gaan of, en zo ja waar, de sturing en prioritering van het anti-witwasbeleid in Nederland versterkt kan worden, zijn enkele buitenlandse NRA's nader bekeken en zijn de (recente) nationale strategieën en praktijken in Canada, de Verenigde Staten, het Verenigd Koninkrijk en Italië in de verkenning betrokken. De uitwerking is te vinden in bijlage B.

4.5.2 Verkregen inzichten

In de praktijk verschillen NRA's qua opzet, uitvoering en rapportage. Ook blijkt uit onderzoek dat de kwaliteit vaak beperkt is.[346] Dit maakt een vergelijking uitdagend. Desalniettemin komen uit de vergelijkende analyse enkele punten naar voren waar buitenlandse NRA's zich onderscheiden van de Nederlandse NRA's en die inspiratie bieden voor het verbeteren van de NRA in Nederland. Deze punten zien op de gebruikte analysemethoden en het betrekken van sectorale en geografische risico's in, of in aanvulling op, de NRA.

Voor Italië wordt opgemerkt dat het preventieve anti-witwasbeleid een sterke coördinatie kent via het Comitato di Sicurezza Finanziaria (CSF). In dit comité worden veel overheidspartijen vertegenwoordigd. Gegeven hun gezamenlijke taakstelling zijn zij in staat om informatie met elkaar te delen. Het CSF is behalve voor het coördineren van de aanpak van witwassen en terrorismefinanciering ook verantwoordelijk voor het opstellen van de NRA en het adviseren van de overheid door (beleids)voorstellen te doen voor het verbeteren van de anti-witwasaanpak.

Canada, de Verenigde Staten en het Verenigd Koninkrijk hebben allemaal recente (overheids)strategieën die zowel overeenkomsten als verschillen kennen. De strategieën van Canada en de Verenigde Staten zijn specifiek gericht op anti-witwasregelgeving, terwijl de strategie van het Verenigd Koninkrijk een holistische, integrale aanpak van economische criminaliteit bevat en waar de bestrijding van witwassen één van de prioriteiten is.

Waar de strategieën van Canada en de Verenigde Staten echte overheidsstrategieën zijn, is de strategie in het Verenigd Koninkrijk een gezamenlijk product van de publieke en private sector.

De drie strategieën zijn (mede) gebaseerd op de nationale risicobeoordelingen (NRA's). Gemeenschappelijke thema's in de strategieën betreffen de risicogebaseerde benadering c.q. het versterken van de operationele effectiviteit, en publiek-private samenwerking. Alle drie de strategieën hebben een gelaagdheid van prioriteiten op het hoogste niveau tot concrete acties. Daarin is de strategie van het Verenigd Koninkrijk veruit het meest gedetailleerd en concreet: acties zijn gericht op resultaten (en niet uitsluitend op inspanning), kennen een planning en deadlines, en een onderscheid tussen verantwoordelijke en betrokken partijen. De voortgang van de strategie wordt bewaakt door een commissie met vertegenwoordigers uit de publieke en private sectoren.

4.6 Van verkenning naar oplossingsrichtingen

De bovenstaande verkenning laat een verscheidenheid aan denkrichtingen – en daarbinnen initiatieven uit binnen- en buitenland – zien. Er zijn voor poortwachters verschillende manieren om door samenwerking verbeteringen in effectiviteit en efficiëntie van de naleving van de Wwft en Sanctiewet te realiseren. De verkenning toont echter ook aan dat om de effectiviteit van het anti-witwasbeleid in zijn geheel te verhogen, de rol van de overheid cruciaal is. Daarbij gaat het om prioriteren en keuzes maken (centrale sturing), het faciliteren op het gebied van informatiedeling en gebruik van technologische innovaties, en het aangaan van publiek-private samenwerking op operationeel niveau met meerdere groepen poortwachters.

Het volgende hoofdstuk gaat in op oplossingsrichtingen en verbindt de bevindingen uit de verkenning met de uitkomsten uit hoofdstukken 2 en 3.

(346) Ferwerda en Reuter 2022, p. 19.

Oplossingsrichtingen

5

5.1 Inleiding

Dit onderzoek heeft tot doel een verkenning te verrichten naar kansen en mogelijkheden om door samenwerking van de verschillende groepen poortwachters, dan wel door het toepassen van creatieve andere werkwijzen, een verbetering van de efficiëntie en effectiviteit van de anti-witwasketen en de naleving van de Sanctiewet te realiseren.

Op basis van de literatuurstudie en interviews zijn de rollen en verantwoordelijkheden van poortwachters op grond van de Sanctiewet en Wwft bekeken en is een inventarisatie gemaakt van de kritiek op de (in)effectiviteit van het anti-witwasbeleid en, meer concreet, van knelpunten die poortwachters en klanten bij de uitvoering van de Wwft en Sanctiewet in de praktijk ervaren, en die door de toezichthouders en het OM worden geconstateerd.

Wat daarbij opvalt is dat het anti-witwasbeleid een uniek en zelfstandig beleidsterrein binnen de bredere bestrijding van (georganiseerde) criminaliteit is. Uniek, omdat een zeer belangrijke rol door de overheid is belegd bij private partijen – variërend van grote financiële instellingen tot professionele dienstverleners zoals makelaars en notarissen. Zelfstandig, omdat een geheel eigen regelgevend kader is opgetuigd ten behoeve van het voorkomen van witwassen en het financieren van terrorisme. Poortwachters zijn aangewezen als belangrijke schakel in het voorkomen van witwassen en het financieren van terrorisme en moeten daarbij aan de vereisten uit de Wwft te voldoen. Het afgelopen decennium is er in toenemende mate aandacht geweest voor de invulling van de poortwachtersrol, in het bijzonder ingegeven door de handhavingsacties van toezichthouders en het OM. In combinatie met de onduidelijkheid die poortwachters ervaren 'aan de voorkant' van de overheid in de vorm van – onder andere – gebrek aan duidelijke sturing en prioritering door de overheid, conflicterende wet- en regelgeving, een gebrek aan bevoegdheden in het licht van de uitdijende onderzoeksplicht, onzekerheid over de interpretatie van de risicogebaseerde benadering en de beperkte mogelijkheid om te leren door het gebrek aan een effectieve feedbackloop, heeft dit ertoe geleid dat poortwachters vanuit een gevoel van verkramping de afgelopen jaren meer hebben gedaan dan strikt genomen noodzakelijk is op basis van de risicogebaseerde benadering. Klanten hebben dit ook in toenemende mate ervaren in de vorm van verminderde toegang tot het financiële stelsel, langere doorlooptijden, hogere kosten en herhaalde uitvragen. Desondanks zijn poortwachters – met ondersteuning van hun branche- en beroepsverenigingen – steeds meer doordrongen van het belang van de poortwachtersrol en willen zij deze rol effectiever en efficiënter inrichten: voor zichzelf en voor hun klanten.

Tegen deze achtergrond is een verkenning verricht naar kansen en alternatieven in binnen- en buitenland die als mogelijke oplossingen of alternatieven kunnen dienen voor een effectieve(re) en efficiënte(re) naleving van de Wwft en Sanctiewet door poortwachters. Uit de verkenning komt naar voren dat vooral ingezet moet worden op 1) samenwerking en 2) het gebruik van (nieuwe) technologieën.

Poortwachters kunnen daarin samen al de nodige concrete stappen nemen. Hoewel deze stappen al kunnen bijdragen aan een verbetering van de effectiviteit en efficiëntie, toont dit onderzoek ook aan dat om echt doeltreffender te worden in het voorkomen van witwassen en terrorismefinanciering en het bewaken van de integriteit van het financiële stelsel, de rol van de overheid cruciaal is. Dit ziet vooral op het ondersteunen van poortwachters, bijvoorbeeld via het wegnemen van (juridische) belemmeringen voor poortwachters en het inzetten op meer structurele samenwerking tussen poortwachters en publieke partijen, waardoor poortwachters beter hun rol kunnen pakken. Dit draagt naar verwachting ook bij aan de motivatie van poortwachters. Een voorzichtige eerste stap is daarbij gezet met de uitwerking van rondetafelgesprekken tussen DNB en de bancaire sector in de NVB Standaarden.(347)

(347) De eerste vijf standaarden zijn in mei 2023 gepubliceerd door de Nederlandse Vereniging van Banken: NVB, 'Minder klantimpact door NVB Standaarden voor risicogebaseerd witwasonderzoek', persbericht 30 mei 2023. De NVB Standaarden zijn gemaakt in overleg met de toezichthouder De Nederlandsche Bank (DNB) en het ministerie van Financiën.

Verder ziet dit voor de overheid op het pakken van de regie waarmee de overheid op hoofdlijnen centraal stuurt en prioriteert, waarmee een (nog) sterker fundament wordt gelegd voor een helder en gedragen beleid dat poortwachters in staat stelt om misbruik van het financiële stelsel door criminelen op effectieve en efficiënte wijze te bestrijden door witwassen en het financieren van terrorisme te voorkomen. Gegeven de uitkomsten van hoofdstukken 3 en 4 lijkt een belangrijke factor voor het verstevigen van het anti-witwasbeleid te liggen bij het maken van een duidelijke keuze in de afweging van het belang van privacy enerzijds, en het voorkomen van witwassen en terrorismefinanciering (en in het verlengde daarvan de bestrijding van criminaliteit) anderzijds.

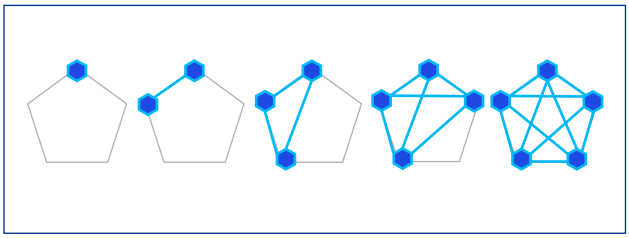
Dit hoofdstuk biedt een aantal geselecteerde oplossingsrichtingen die op kortere en langere termijn gerealiseerd kunnen worden om de naleving van de Wwft en Sanctiewet effectiever en efficiënter in te richten en die bijdragen aan het realiseren van een effectievere en efficiëntere anti-witwasaanpak. Daarbij is ervoor gekozen om de oplossingsrichtingen onder te verdelen in drie clusters:

1. Oplossingsrichtingen waarbij poortwachters primair aan zet zijn.
2. Oplossingsrichtingen waar poortwachters en overheid in gezamenlijkheid moeten optreden.
3. Oplossingsrichtingen waarbij de overheid aan zet is.

5.1.1 Complexiteit en impact van de oplossingsrichtingen

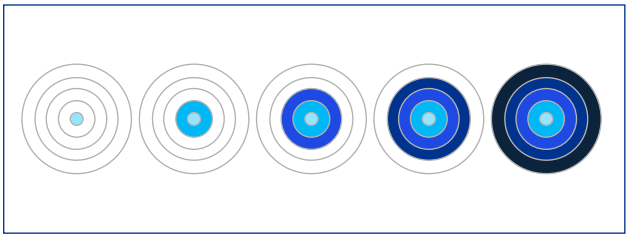
Bij de verschillende oplossingsrichtingen wordt op basis van de verwachte inspanning die gepaard gaat met het uitwerken van een oplossingsrichting duiding gegeven aan de mate van complexiteit die de oplossingsrichting kent. De verwachte inspanning is ingeschat aan de hand van factoren zoals nieuwe of uitgebreide(re) vorm van samenwerking, technologische benodigdheden, of nog weg te nemen belemmerende factoren, zoals wijziging van (conflicterende) wet- en regelgeving.

Dit is per oplossingsrichting weergegeven aan de hand van de volgende symbolen:



Figuur 6: Van weinig complex (links) tot zeer complex (rechts)

De verwachte opbrengst, oftewel de positieve impact van de oplossingsrichting op de mate waarin de effectiviteit van de naleving van de Wwft en Sanctiewet toeneemt, wordt per oplossingsrichting geduid aan de hand van de volgende symbolen:



Figuur 7: Van beperkte impact (links) tot grote impact (rechts)

5.2 Poortwachters

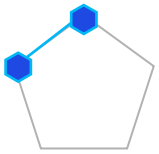
Uit dit onderzoek komen enkele kansen en mogelijkheden naar voren voor poortwachters om door samenwerking zelf al stappen te zetten om de efficiëntie en effectiviteit van de anti-witwasketen en de naleving van de Sanctiewet te verbeteren. Daarbij moet worden opgemerkt dat samenwerking tussen de poortwachters op alle niveaus belangrijk is. Waar hierna drie concrete mogelijkheden nader worden uitgewerkt, is hier in de basis wederzijds vertrouwen en kennis over en weer tussen de categorieën poortwachters voor nodig. Het is daarom belangrijk dat poortwachters zich (blijven) inzetten voor een (gedeeld) begrip van ieders specifieke rol en verantwoordelijkheden in de uitoefening van de gezamenlijke poortwachtersfunctie en kennis over de (aard van de) werkzaamheden van de verschillende poortwachters. Ook is het belangrijk om elkaar structureel op te zoeken om ontwikkelingen, trends en fenomenen te delen. Bovendien is het van belang dat poortwachters elkaar opzoeken en ondersteunen bij hulpvragen, gegeven de nuances in rollen, verantwoordelijkheden alsook de uiteenlopende expertise van de verschillende poortwachters. Met andere woorden: het is van belang dat poortwachters over de eigen sector heen de blik naar buiten richten.

Concreet zijn er drie mogelijkheden voor poortwachters die hierna verder worden uitgewerkt:

- Het ontwikkelen van een gemeenschappelijke KYC-taxonomie.
- Het opzetten van waarschuwingssystemen.
- Het ontwikkelen van gezamenlijke voorzieningen.

5.2.1 KYC-taxonomie

Een eerste oplossingsrichting voor poortwachters betreft het ontwikkelen van een gemeenschappelijke standaard op het gebied van KYC: de KYC-taxonomie.

Complexiteit	Impact
	

Wat is het?

Het beleid en de processen van poortwachters om de Wwft en de Sanctiewet na te leven zijn gebaseerd op verschillende bronnen variërend van wet- en regelgeving (Europees en nationaal), guidances van nationale en Europese toezichthouders en andere internationale organisaties, zoals de FATF, en guidances en aanvullende vereisten of interpretaties van branche- en beroepsorganisaties. Door de diversiteit aan bronnen kunnen de concrete eisen aan poortwachters verschillen; daardoor zullen ook het beleid en de processen van individuele poortwachters anders zijn. Als gevolg daarvan hanteren poortwachters in de praktijk bijvoorbeeld andere datapunten, vragen zij andere documenten op bij klanten en vereisen poortwachters meer/andere vormen van bewijs of ondersteunend materiaal om het cliëntenonderzoek af te ronden. Deze verschillen belemmeren een efficiënt CDD-proces voor zowel poortwachters als hun klanten. Een gedeelde KYC-taxonomie betreft een gezamenlijke interpretatie van wettelijke vereisten, bijbehorende datapunten en onderliggende documentatie.(348)

Waarom is het belangrijk?

Een gedeelde KYC-taxonomie zorgt ervoor dat poortwachters dezelfde informatie op een uniforme, dan wel geharmoniseerde, manier verzamelen. Het biedt poortwachters een opstap naar een effectievere en efficiëntere informatiedeling, doordat zij hetzelfde begrip hebben van de informatie en zodoende 'dezelfde taal' spreken. Een gedeelde KYC-taxonomie helpt bij het opzetten van een waarschuwingssysteem en gezamenlijke voorziening op het gebied van CDD (zie paragrafen 5.2.2 en 5.2.3) en kan als input dienen voor relevante informatie voor een digitale identiteit en 'portemonnee' (zie paragraaf 5.3.2).

(348) Zie ook NVB 2022a, p. 27.

Vanuit het perspectief van klanten biedt een gedeelde KYC-taxonomie duidelijkheid en voorspelbaarheid. Ook kan worden gewezen op de mogelijkheid van een verlaging van administratieve lasten en kosten.[349] Klanten kunnen immers dezelfde documentatie aan verschillende poortwachters verstrekken. Zodoende hebben klanten geen last van herhaalde verzoeken.

Welke concrete stappen kunnen poortwachters nemen?

Bij de te nemen stappen kan een onderscheid worden gemaakt tussen de stappen binnen de eigen categorie poortwachters, en de stappen tussen de verschillende categorieën poortwachters. Hoewel de stappen hierna gepresenteerd worden als opeenvolgende stappen, kunnen meerdere stappen in de praktijk samenlopen.

Concrete stappen binnen de eigen categorie poortwachters zijn:

1. Maak een inventarisatie van de wettelijke vereisten (inclusief guidances met eventuele verwachtingen van de eigen Wwft-toezichthouder), bijbehorende datapunten en brondocumenten via een sectorbrede uitvraag.
2. Identificeer de wettelijke bepalingen waarover binnen de sector verschillende interpretaties bestaan over de datapunten en/of brondocumenten.
3. Organiseer rondetafelgesprekken met een representatieve groep poortwachters om de verschillende interpretaties te bespreken. Daarbij kan worden beoordeeld welke interpretaties binnen de sector 'leidend' zijn en zodoende als voorstel voor een gedeelde KYC-taxonomie kunnen dienen.
4. Waar geen overeenstemming bereikt kan worden en interpretaties direct gerelateerd zijn aan de eigen interpretatie van wet- en regelgeving, is het aan te raden om navraag te doen bij andere sectoren van poortwachters over hun (gemeenschappelijke) interpretaties.
5. Creëer een gedeelde KYC-taxonomie voor de sector in concept.

Concrete stappen tussen de categorieën poortwachters zijn:

1. Houd elkaar gedurende het proces van het opstellen van de gedeelde KYC-taxonomie binnen de eigen sector op de hoogte en bespreek de verschillen in interpretaties tussen de sectoren.
2. Beoordeel voor welke onderwerpen een cross-sectorale gedeelde KYC-taxonomie noodzakelijk en mogelijk is.
3. Organiseer verschillende rondetafelgesprekken met een representatieve groep poortwachters uit de verschillende sectoren om de verschillende interpretaties te bespreken, en besluit wat de cross-sectorale interpretatie gaat zijn. Waar er afwijkingen tussen categorieën poortwachters (blijven) bestaan, bijvoorbeeld vanwege afwijkende wettelijke verplichtingen op grond van sectorale wet- en regelgeving of beroepsregelgeving, verdient het aanbeveling dit op transparante wijze te vermelden.
4. Stem de gedeelde KYC-taxonomie en eventuele sectorale afwijkingen af met de Wwft-toezichthouders.
5. Stel een definitieve gedeelde KYC-taxonomie vast, waarbij eventuele sectorale afwijkingen duidelijk aangegeven worden.
6. Publiceer de gedeelde KYC-taxonomie en breng dit onder de aandacht van de poortwachters, bijvoorbeeld via het organiseren van (sectorale of cross-sectorale) kennissessies en het publiceren van informatiemateriaal.
7. Evalueer de gedeelde KYC-taxonomie op periodieke basis, en ten minste bij relevante wijzigingen van wet- en regelgeving.

(349) NVB 2022a, p. 27.

Bij alle te nemen stappen is een belangrijke coördinerende rol weggelegd voor beroepsorganisaties en brancheverenigingen. Het verdient aanbeveling een (onafhankelijke) voorzitter en een secretaris aan te wijzen die de cross-sectorale afstemmingen begeleiden. Deze geven bij de start een tijdplanning mee als ijkpunt, om de cross-sectorale afstemmingen efficiënt te kunnen laten verlopen en tijdig af te ronden.

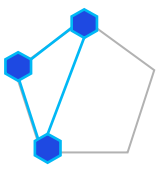
Wat hebben poortwachters nodig van de overheid?

Voor het toewerken naar een gedeelde KYC-taxonomie is geen wijziging van wet- en regelgeving nodig. Wel zou het poortwachters kunnen helpen als de Wwft-toezichthouders ondersteuning bieden bij de totstandkoming van een gedeelde KYC-taxonomie, bijvoorbeeld door hun interpretaties of verwachtingen te delen (bijv. in het geval poortwachters onderling geen overeenstemming kunnen bereiken), door poortwachters op basis van hun internationale contacten op de hoogte te houden van geldende interpretaties elders in Europa, en door te bevestigen dat zij akkoord zijn met de gedeelde taxonomie zoals voorgestaan door poortwachters.

Wat betreft het moment van afstemming met de Wwft-toezichthouders kunnen de branche- en beroepsorganisaties overwegen om de afstemming al in een eerdere fase te zoeken dan thans voorgesteld (stap 4). Omdat dit mogelijk het risico met zich meebrengt dat individuele Wwft-toezichthouders verschillende interpretaties of verwachtingen delen, is er in de volgordelijkheid nu voor gekozen om dit aan het einde van het proces voor te stellen wanneer poortwachters onderling eenzelfde interpretatie voor ogen hebben.

5.2.2 Waarschuwingssystemen

Een tweede oplossingsrichting voor poortwachters betreft het opzetten van waarschuwingssystemen.

Complexiteit	Impact
	

Wat is het?

Elke poortwachter is op grond van de Wwft wettelijk verplicht een eigen cliëntenonderzoek verrichten. Om een goede risico-inschatting te kunnen maken, heeft de poortwachter informatie nodig. Deze informatie komt bijvoorbeeld uit publieke registers of van de klant zelf. Waarschuwingssystemen kunnen de activiteiten die poortwachters verrichten om de integriteit van het financiële stelsel te beschermen en het witwassen en financieren van terrorisme te voorkomen, verder ondersteunen. Een waarschuwingssysteem is een systeem waarin de gegevens zijn opgenomen van natuurlijke personen en/of rechtspersonen die een mogelijk risico vormen voor individuele poortwachters of voor de integriteit van het financiële stelsel, bijvoorbeeld in het geval van zware verdenkingen of bewezenverklaring van fraude of ander crimineel gedrag. Deze informatie wordt (onder bepaalde strikte voorwaarden) verstrekt en gebruikt door poortwachters.

Waarom is het belangrijk?

Uit de verkenning is al naar voren gekomen dat informatiedeling als een van de hoekstenen van een effectief anti-witwasbeleid wordt gezien. Meerdere partijen weten en zien meer dan één: informatiedeling stelt poortwachters in staat om risico's beter en sneller te onderkennen, te beperken en om de juiste mitigerende maatregelen te nemen.

Het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (PIFI) toont dat het mogelijk is om – met inachtneming van de privacy van betrokkenen – proactief informatie met elkaar te delen over klanten die een dreiging (kunnen) zijn voor andere poortwachters of de integriteit van het financiële stelsel. Dergelijke gestructureerde gegevensdeling kan juist zorgen voor een adequate bescherming van persoonsgegevens, omdat duidelijke onderlinge afspraken schriftelijk worden gedocumenteerd.(350) Organisaties verwerken persoonsgegevens op gelijke wijze en kunnen elkaar ook controleren op dit punt. Met het PIFI wordt aangetoond dat kan worden voldaan aan belangrijke principes zoals datakwaliteit en dataminimalisatie.(351) Het toont ook dat het belangrijk is om oog te hebben voor zaken zoals de registratiecriteria, toegang tot de registers, bewaartermijnen, verwijdering van gegevens uit de registers en waarborgen tegen ongeautoriseerd gebruik van het stelsel van gegevensuitwisseling. Gegeven de dreiging die fraude, maar ook witwassen en terrorismefinanciering met zich meebrengen voor de integriteit van het financiële stelsel, ligt het in de rede dat andere poortwachters een soortgelijk systeem optuigen.

Voorgaande is extra relevant nu het kabinet in het wetsvoorstel Wet plan van aanpak witwassen uit oktober 2022 een verplichte gegevensdeling tussen instellingen van dezelfde categorie voorstelt wat betreft de uitvoering van het cliëntenonderzoek bij klanten met indicaties van een hoger risico op witwassen of financieren van terrorisme.(352) In de memorie van toelichting bij het wetsvoorstel wordt gesteld dat *"[o]m de kans te verkleinen dat een kwaadwillende cliënt door middel van shopgedrag toegang krijgt tot het financiële stelsel en om te voorkomen dat elke instelling van vooraf aan hoeft te beginnen met het verzamelen van relevante gegevens, is het noodzakelijk dat instellingen informatie uitwisselen bij een cliënt met indicaties van een hoger risico op witwassen of financieren van terrorisme"*.(353)

Hoewel het wetsvoorstel in zijn huidige vorm vragen met zich meebrengt aangaande het verplichte karakter, de uitvoerbaarheid, de beperkingen tot situaties met een hoog risico (terwijl 'shopgedrag' juist een indicator voor hoger risico is of kan zijn) en de beperking in de gegevensuitwisseling tussen instellingen van dezelfde categorie, toont dit wel aan dat het kabinet het belang van informatiedeling tussen poortwachters over risico's gelinkt aan gemeenschappelijke klanten onderkent.(354) Het conceptwetsvoorstel biedt bovendien een grondslag voor informatiedeling bij algemene maatregel van bestuur tussen verschillende categorieën poortwachters. Wanneer klanten met meerdere categorieën poortwachters te maken hebben draagt cross-sectorale informatiedeling bij aan het creëren van effectieve (informatie)netwerken om (potentiële) criminelen te weren. Een voorbeeld geldt voor vastgoedtransacties, waar klanten te maken hebben met makelaars, notarissen, banken, hypotheekverstrekkers en/of bemiddelaars in levensverzekeringen (dan wel direct levensverzekeraars). Grote internationale bedrijven kunnen vanwege de aard van hun business juist vaak te maken hebben met trustkantoren, banken, notarissen, belastingadviseurs en accountants. Voor trustkantoren bestaat verplichte gegevensdeling overigens al op grond van artikel 68 Wtt 2018. Deze onderzoeksplicht en onderlinge informatiedeling tussen trustkantoren over gebleken integriteitsrisico's geldt voor alle cliëntenonderzoeken (en, in tegenstelling tot het voorstel van artikel 3b Wwft, niet uitsluitend voor situaties van hoger risico) en betreft ook het delen van persoonsgegevens van strafrechtelijke aard.(355)

Een breder, proactief waarschuwingssysteem à la het Incidentenwaarschuwingssysteem Financiële Instellingen voor andere categorieën poortwachters dan banken en verzekeraars kan worden opgezet op grond van de huidige wet- en regelgeving. Het kan mogelijk (ook) gebruikt worden als instrument voor de verplichte informatiedeling op grond van (het toekomstige) artikel 3b Wwft. Dit is wel afhankelijk van de vraag hoe de (verplichte) gegevensdeling uiteindelijk juridisch wordt vormgegeven.

(350) Vgl. het PIFI in bijlage B.
(351) Vereist op grond van artikel 5 AVG.
(352) Artikel 3b wetsvoorstel Wet plan van aanpak witwassen.
(353) Kamerstukken II, 2022/2023, 36 228, nr. 3, p. 5.
(354) Zie o.a. *Reactie van NVM, VBO en VastgoedPro op het wetsvoorstel Wet plan van aanpak witwassen*, 2020, beschikbaar via deze link.
(355) Artikel 68, leden 1 t/m 3, Wtt 2018.

Welke concrete stappen kunnen poortwachters nemen?

Een concrete stap voor banken, verzekeraars en trustkantoren is:

Het delen van de ervaringen met IFI (banken en verzekeraars) en de verplichte informatiedeling op grond van artikel 68 Wtt 2018 (trustkantoren) met de overige categorieën poortwachters. Daarbij verdient het aanbeveling in te gaan op de gekozen opzet, de benodigdheden vanuit onder meer het juridisch en IT-perspectief (infrastructuur inclusief cybersecurity), de benodigde capaciteit, de van toepassing zijnde waarborgen en aanvullende relevante privacyoverwegingen. Verder kan worden ingegaan op de kosten van het waarschuwingssysteem – bij de opzet en op doorlopende basis – en kunnen, al dan niet aan de hand van casuïstiek, de baten worden toegelicht.

Concrete stappen voor de overige categorieën poortwachters zijn:

1. Het opdoen van kennis over de ervaringen van banken, verzekeraars en trustkantoren met waarschuwingssystemen en verplichte gegevensdeling.
2. Het (laten) maken van een eigen kosten-batenanalyse voor het opzetten van een waarschuwingssysteem binnen de sector, alsook een juridische analyse indien beroepsgeheim of andere regelgeving in de weg staat van het opzetten van een waarschuwingssysteem binnen de sector.
3. Het op basis van eerder genomen stappen maken van een geïnformeerde keuze over de wenselijkheid en haalbaarheid van een waarschuwingssysteem.
4. Indien wordt besloten tot het opzetten van een waarschuwingssysteem kunnen poortwachters voor de verdere concretisering en uitwerking inspiratie ontlenen aan het PIFI en de relevante factoren zoals uitgelicht in bijlage B van dit onderzoeksrapport.

Concrete stappen voor alle poortwachters zijn:

1. Het monitoren van de ontwikkelingen van het voorgestelde toekomstige artikel 3b Wwft als onderdeel van het wetsvoorstel Wet plan van aanpak witwassen en het anticiperen op mogelijke wijzigingen aan het waarschuwingssysteem. Daarbij is het voor zowel het bestaande IFI als de op te zetten waarschuwingssystemen van belang om – met het oog op mogelijke cross-sectorale gegevensdeling – uit te gaan van de gedeelde KYC-taxonomie (zie paragraaf 5.2.1).
2. Het met elkaar in dialoog gaan en blijven gedurende het wetgevingsproces en tijdens de ontwikkeling van de systemen om ervoor te zorgen dat de bestaande en/of te ontwikkelen waarschuwingssystemen zowel voldoen aan de wetgeving als compatibel met elkaar zijn en met elkaar kunnen worden verbonden ten behoeve van mogelijke (toekomstige) cross-sectorale gegevensdeling.

Wat hebben poortwachters nodig van de overheid?

Enkele categorieën poortwachters kunnen al aan de slag met het opzetten van een waarschuwingssysteem met als doel het effectiever voorkomen en bestrijden van misbruik van het financieel stelsel bijvoorbeeld door fraude of misleiding, zonder dat wijziging van wet- en regelgeving noodzakelijk is. Echter, voor ‘geheimhouders’ zoals notarissen zal de sectorale wetgeving (en/of beroepsregelgeving) moeten worden gewijzigd om de individuele geheimhouding die op deze beroepsbeoefenaars rust te doorbreken. In de context van het wetsvoorstel Wet plan van aanpak witwassen heeft de KNB al support uitgesproken voor een ‘collectieve notariële geheimhouding’ en geeft de KNB aan dat zij hier al langer voor pleit.(356) Voor het goed kunnen functioneren van waarschuwingssystemen is uit de verkregen inzichten in paragraaf 4.2.3 voorts naar voren gekomen dat de groep deelnemers definieerbaar moet zijn. Voor makelaars vereist dit actie van de overheid; zie hiervoor de aanbevelingen in paragraaf 5.4.1 over de regulering van het makelaarsberoep.

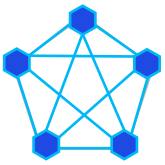
(356) A. Ploumen, KNB: ‘Onderlinge gegevensdeling tegen witwassen nodig en gewenst’, *MrOnline* 7 november 2022.

Gegeven het mogelijke gebruik van waarschuwingssystemen voor de verplichte gegevensdeling zoals opgenomen in het wetsvoorstel Wet plan van aanpak witwassen, is het ook noodzakelijk dat er zo spoedig mogelijk duidelijkheid komt over de vormgeving van artikel 3b Wwft. In dit onderzoek is al eerder aangehaald dat samenwerking in de vorm van netwerken, partnerschappen en samenwerkingsverbanden (steeds vaker) wordt gezien als dé manier om effectiever en efficiënter op te treden in de strijd tegen witwassen, terrorismefinanciering en onderliggende criminaliteit door (georganiseerde) criminele organisaties. Daarom valt het aan te bevelen om in nauw overleg met de poortwachters te bepalen voor welke situaties cross-sectorale gegevensdeling vanuit Wwft-optiek noodzakelijk, en tegelijkertijd vanuit privacy-optiek ook proportioneel, is. Daar kunnen zogenaamde klantreizen een belangrijke rol bij spelen.(357)

Poortwachters zullen bij de ontwikkeling van een waarschuwingssysteem aandacht moeten hebben voor de privacy van (rechts)personen die in het systeem worden geplaatst. Het IFI en het onderliggende protocol voldoen aan de eisen die worden gesteld op grond van de AVG. De Autoriteit Persoonsgegevens heeft aangegeven dat fraudebestrijding en de opsporing van daders van groot belang zijn, maar dat het bijhouden en delen van strafrechtelijke gegevens wel met grote terughoudendheid en zorgvuldigheid moet gebeuren.(358) Bij de concrete stappen hiervoor geschetst is aangegeven dat poortwachters het PIFI als uitgangspunt voor een eigen sectoraal waarschuwingssysteem kunnen gebruiken. Naar alle waarschijnlijkheid is daarvoor een vergunning van de AP nodig voor het verwerken van persoonsgegevens van strafrechtelijke aard. Om te borgen dat de sectorale waarschuwingssystemen voldoen aan het 'privacy-by-design' uitgangspunt, is het nodig dat de AP zich coöperatief opstelt zodat een juiste balans gevonden kan worden tussen het effectief tegengaan van fraude en witwassen enerzijds en de bescherming van persoonsgegevens anderzijds.

5.2.3 Gezamenlijke voorzieningen

Een derde oplossingsrichting voor poortwachters betreft het toewerken naar gezamenlijke voorzieningen.

Complexiteit	Impact
	

Wat is het?

In de verkenning is reeds aan de orde gekomen dat gezamenlijke voorzieningen, ook wel utiliteiten genoemd, zich kunnen richten op verschillende processen zoals transactiemonitoring, sanctiescreening of (aspecten van) het CDD-proces.

De initiatieven uit het binnen- en buitenland laten zien dat de ontwikkeling van gezamenlijke voorzieningen een relatief jonge ontwikkeling betreft. De initiatieven die zijn meegenomen in de verkenning (zie bijlage B) laten voorts zien dat dergelijke voorzieningen op verschillende manieren kunnen worden vormgegeven. Samengevat gaat het thans om drie voorkomende vormen:

1. Gezamenlijke voorziening ten aanzien van transactiemonitoring. Deze utiliteiten lijken vooral relevant voor poortwachters met grote transactiestromen en duurzame zakelijke relaties, zoals banken, betaaldienstverleners, levensverzekeraars, crypto-aanbieders en trustkantoren;
2. Gezamenlijke voorziening ten aanzien van (aspecten van) het CDD-proces in de vorm voor een 'voor en door'-model, waarbij informatie gehaald, gebracht en daarbij ook geverifieerd wordt door deelnemende poortwachters. Daarbij worden zij technologisch ondersteund door een platformbeheerder. Hier fungeert de gezamenlijke voorziening als een soort 'repository';

(357) Zie voor twee voorbeelden van klantreizen paragraaf 3.3.3.
(358) Autoriteit Persoonsgegevens, *Besluit inzake de vergunningaanvraag voor de verwerking van [PARTIJ] volgens het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen 2021*, 20 augustus 2021, kenmerk z2021-03355, beschikbaar via deze link.

3. Voorziening in de vorm van dienstverlening door een commerciële dienstverlener en waaraan poortwachters hun CDD-processen (deels) uitbesteden. De functies van de utiliteit kunnen worden uitgebreid al naar gelang de behoefte van de uitbestedende poortwachters.

Waarom is het belangrijk?

Gezamenlijke voorzieningen stellen poortwachters in staat netwerken te vormen om zo effectiever en efficiënter te kunnen handelen. Bij gezamenlijke transactiemonitoring wordt gewezen op het feit dat met netwerkanalyses meer kan worden gezien dan een individuele bank dit zou kunnen – en dus gerichter ongebruikelijk en verdacht gedrag kan worden geïdentificeerd – alsook op de mogelijke verhoogde efficiëntie van het transactiemonitoringproces, de verlaging van kosten door het gezamenlijk ontwikkelen en onderhouden van utiliteiten, en verbeterd risicomanagement. Gezamenlijke voorzieningen ten aanzien van (aspecten van) het CDD-proces hebben als voornaamste doel de cliëntenonderzoeken van poortwachters efficiënter te maken door herhaald gebruik van data en de mogelijkheid om deze data te actualiseren en te optimaliseren, de zogenoemde datacirculariteit en datamutualisatie. Samenwerking tussen poortwachters verhoogt de kwaliteit en betrouwbaarheid van de data voor poortwachters. Voor klanten is het voordeel dat zij geen, of minder, last hebben van herhaalde verzoeken en dat cliëntenonderzoeken efficiënter verlopen. Belangrijk voor de werking gezamenlijke voorzieningen ten aanzien van CDD en vanuit het oogpunt van privacy van de klanten is dat (gezamenlijke) verwerking van gegevens enkel plaatsvindt met toestemming van de klant en dat informatie uitsluitend op een 'need-to-know' basis tussen poortwachters wordt gedeeld (dataminimalisatie). Zodoende zijn klanten van (aangesloten) poortwachters 'in control' over hun gegevens.

Welke concrete stappen kunnen poortwachters nemen?

In aanvulling op de stappen die reeds door banken zijn gezet op het gebied van gezamenlijke transactiemonitoring en waar momenteel vooral actie aan de zijde van de overheid gewenst is (zie verder hierna bij 'Wat hebben de poortwachters nodig van de overheid'), kan het toewerken naar een gezamenlijke voorziening van verschillende categorieën poortwachters ten aanzien van (aspecten van) het CDD-proces een positieve bijdrage leveren aan de efficiënte en effectieve naleving van de Wwft/Sw. Deze oplossingsrichting ligt in het verlengde van de oplossingsrichtingen met betrekking tot de standaardisatie van datapunten via een gedeelde KYC-taxonomie en het opzetten van waarschuwingssystemen (paragrafen 5.2.1 en 5.2.2). Ook kan het samenlopen met de aanbeveling rondom het gebruik van digitale identiteiten in het kader van cliëntenonderzoeken (paragraaf 5.3.2).

Een gezamenlijke voorziening ten aanzien van (aspecten van) het CDD-proces is vanuit praktisch, juridisch en technologisch perspectief uitdagend om te implementeren. Poortwachters zullen in zekere mate afhankelijk zijn van de overheid indien de overheid in het licht van de bescherming van privacy een voorkeur heeft voor een sterkere juridische basis voor informatiedeling en gezamenlijke gegevensverwerking door poortwachters en waardoor wijziging van relevante wet- en regelgeving nodig blijkt te zijn. In de tussentijd kunnen poortwachters zelf al de volgende stappen zetten:

1. Het in onderling overleg opstellen van een plan van aanpak voor de oprichting en werking van een gezamenlijke voorziening op het gebied van CDD (pilot) aan de hand van initiatieven verkend in dit onderzoek en uitgewerkt in bijlage B van dit onderzoeksrapport. Het verdient daarbij aanbeveling dat de poortwachters daarbij minimaal de aspecten genoemd in paragraaf 4.2.3 betrekken.

   Daarbij gaat het onder andere om de groep deelnemers, type klanten, de gewenste functies van de utiliteit, het type informatie en actualisatie, de gewenste technologie voor het platform, de governance rondom de utiliteit en aspecten zoals privacy, mededinging en cybersecurity. Het advies is om bij aanvang af te wegen of ondersteuning wordt gezocht bij een onafhankelijke partij die ervaring heeft met het opzetten van een complexe governancestructuur, die kennis en ervaring heeft met het uitdenken en uitwerken van een complex technologisch platform en met het bewaken van de juiste privacyrichtlijnen.

   Op basis van de verkregen inzichten is het verder aan te raden om het initiatief klein te laten starten.

Dat kan door de kring van deelnemers en de functies van de utiliteit te beperken, bijvoorbeeld uitsluitend tot het identificeren en verifiëren van informatie. Ook is het zaak om de inrichting en werking van de voorziening juridisch zo simpel mogelijk te houden; daardoor is het aan te raden om het initiatief uitsluitend met gereguleerde instellingen te starten, beroepsbeoefenaars onderworpen aan geheimhouding uitsluitend informatie 'te laten halen', en een gezamenlijke voorziening in eerste instantie nationaal op te zetten.

2. Ondanks de aanbeveling om klein te starten kunnen (gereguleerde) poortwachters al intern beoordelen of er binnen de sector interesse is om deel te nemen aan de pilot. Daarbij moet onderkend worden dat het opzetten van, en deelnemen aan een gezamenlijke voorziening in de opstartfase (aanzienlijke) investeringen met zich mee kan brengen.
3. Uit de inzichten verkregen uit de verkenning is naar voren gekomen dat een vroegtijdige betrokkenheid van relevante publieke partijen zeer belangrijk is. Het in overleg treden met ten minste de Wwft-toezichthouders en primair verantwoordelijke departementen (het ministerie van Financiën en het ministerie van Justitie en Veiligheid) door poortwachters bij de ontwikkeling van het voorstel en de pilot is daarom belangrijk. Partijen kunnen eventuele onduidelijkheden bespreken en bekijken hoe de overheid de oprichting en werking van een gezamenlijke voorziening op het gebied van CDD verder kan ondersteunen (mogelijk ook in de vorm van financiering/subsidiëring en aanpassing van wet- en regelgeving).

Wat hebben poortwachters nodig van de overheid?

Uit de verkenning naar buitenlandse initiatieven is naar voren gekomen dat deze initiatieven allemaal door private partijen opgezet en/of beheerd worden en dat de overheid hier uitsluitend een ondersteunende rol heeft (gehad).

Wat betreft de gezamenlijke transactiemonitoring door banken voorziet het wetsvoorstel Wet plan van aanpak witwassen in de juridische grondslag van TMNL. Het is belangrijk dat deze wettelijke grondslag voor gezamenlijke transactiemonitoring er binnen afzienbare tijd komt, zodat het volle potentieel van TMNL benut kan worden. Bij de behandeling van het wetsvoorstel verdient het aanbeveling om gezamenlijke transactiemonitoring niet alleen mogelijk te maken voor banken, maar ook voor andere poortwachters met grote transactiestromen en duurzame zakelijke relaties, zoals betaaldienstverleners, levensverzekeraars, crypto-aanbieders en trustkantoren.

Initiatieven uit het buitenland laten (voorzichtig) zien dat gezamenlijke voorzieningen op het gebied van CDD al ontplooid kunnen worden zonder dat wijziging van wet- en regelgeving noodzakelijk is, vooral omdat deze uitgaan van het delen van informatie over gedeelde klanten met toestemming van de klant. Echter, gegeven het spanningsveld tussen privacy en de anti-witwasregelgeving is het niet ondenkbaar dat overheden een sterkere grondslag en meer waarborgen in de anti-witwasregelgeving wensen voor informatiedeling tussen, en gezamenlijke gegevensverwerking door, poortwachters. Hierbij kan reeds worden gewezen op een het feit dat de Nederlandse regering zich samen met regeringen uit Denemarken en Duitsland op Europees niveau bij de onderhandelingen over de AMLR (zie paragraaf 3.2.1) inzet voor het verhogen van de effectiviteit van de poortwachtersrol door samenwerking en innovatie.

In het in mei 2023 gepubliceerde 'Non-paper on enhancing gatekeepers' effectiveness through cooperation and innovation' wordt onderkend dat het delen van informatie over klanten of het uitbesteden van taken kan bijdragen aan het vervullen van de poortwachtersrol.(359) De regeringen stellen daarbij dat het belangrijk is dat de anti-witwasregelgeving duidelijke regels bevat over informatiedeling, verantwoordelijkheden en waarborgen. De regeringen geven aan dat het vanuit AVG-optiek belangrijk is dat een gemeenschappelijke verwerkingsgrond wordt neergelegd in de AMLR. Voorts stellen ze dat *"[s]ince joint utilities can take on different forms, it is more suitable to leave it to national law to prescribe the specific measures and safeguards that are required for the specific joint utility".*(360)

(359) Brief van de minister van Financiën over voortgang beleidsagenda aanpak witwassen: Kamerstukken I, 2022/2023, 31 477 en 34 08, D[1] (de letter D heeft alleen betrekking op 31 477). Het non-paper is opgenomen in bijlage 6.

(360) Kamerstukken I, 2022/2023, 31 477 en 34 08, D1, bijlage 6, pagina 4.

Verdere uitwerking van de vereisten van en waarborgen voor utiliteiten moeten dus volgens de Deense, Duitse en Nederlandse regeringen op nationaal niveau plaatsvinden. Het is op het moment van dit onderzoek nog onduidelijk of deze voorstellen hun weerslag gaan vinden in de uiteindelijke tekst van de verordening. Zoals opgemerkt in paragraaf 3.2.1. vinden op het moment van dit onderzoek de triloogonderhandelingen plaats.

Mocht de Europese regelgeving aangepast worden conform de voorstellen van de Nederlandse, Deense en Duitse regeringen, dan zou dat vanuit het perspectief van effectieve en efficiënte naleving van de anti-witwasregelgeving een positieve stap voor poortwachters (kunnen) zijn, omdat dit een sterkere grondslag biedt voor het (gezamenlijk) verwerken van persoonsgegevens dan wanneer dit uitsluitend met toestemming van klanten wordt gedaan. Op nationaal niveau zullen in dat geval nog verdere keuzes gemaakt moeten worden, waartoe de overheid reeds een aanzet kan doen. Hieronder volgen twee zaken die de overheid in elk geval zal moeten regelen:

1. De overheid zal zo spoedig mogelijk moeten verduidelijken hoe de voorzieningen ten aanzien van (aspecten van) het CDD-proces juridisch kwalificeren. Dit is in het bijzonder relevant bij gezamenlijke 'voor-en-door' voorzieningen. Indien het gaat om introducerend cliëntenonderzoek, dan zal voor trustkantoren een wijziging van de Wtt 2018 nodig zijn. Trustkantoren mogen thans uitsluitend gebruikmaken van introducerend cliëntenonderzoek indien de introducerende instelling ook een trustkantoor is en tot dezelfde groep als het trustkantoor behoort.(361) Dit beperkt trustkantoren om deel te nemen aan gezamenlijke voorzieningen op het gebied van CDD. Ook zal moeten worden bekeken of makelaars als introducerende instelling op mogen treden. Op dit punt is de Wwft immers strikter dan de huidige AMLD5.(362)
2. Ook zal de overheid zo spoedig mogelijk de wenselijkheid van een vergunningenregime moeten bepalen. Daarbij kan inspiratie worden gevonden in de (tot nu toe) enige EU-lidstaat met specifieke anti-witwasregels over KYC-utiliteiten: Letland.

5.3 Poortwachters en overheid

Uit dit onderzoek komen ook enkele andere kansen en mogelijkheden naar voren om de efficiëntie en effectiviteit van de anti-witwasketen en de naleving van de Sanctiewet te verbeteren, waarbij poortwachters en publieke partijen – weliswaar op basis van de eigen rollen en verantwoordelijkheden – gezamenlijk stappen moeten zetten.

Concreet gaat het hier om twee oplossings-richtingen: het versterken van de publiek-private samenwerking en het gebruik van digitale identiteiten in de context van het cliëntenonderzoek.

5.3.1 Publiek-private samenwerking

Een eerste oplossingsrichting voor poortwachters en overheid samen betreft het bestendigen en uitbreiden van structurele publiek-private samenwerking.

De vorming en bestendiging van publiek-private netwerken in de vorm van samenwerkingsverbanden is cruciaal voor de effectiviteit van het anti-witwasbeleid. Publiek-private samenwerking (PPS) binnen het anti-witwasbeleid kan plaatsvinden op 1) fenomeenbasis, via het onderling delen van kennis over fenomenen, trends en good practices en 2) op operationeel niveau, waarbij het doel is om informatie over transacties, meldingen en andere intelligence samen te brengen om witwassen en terrorismefinanciering effectiever te bestrijden.

(361) Artikel 21, eerste lid, Wtt 2018.
(362) Bij de Memorie van toelichting van de Implementatiewet vierde anti-witwasrichtlijn (Kamerstukken II, 2017/18, 34 808, nr. 3, p. 25) wordt daarbij gesteld: *"In artikel 5, eerste lid onderdeel a, ontbreekt onder meer een verwijzing naar domicilieverleners, makelaars, grootwaardehandelaren, kansspelaanbieders, taxateurs en pandhuizen. Dit is op grond van huidig recht reeds het geval. De keuze om hierin bij implementatie van de vierde anti-witwasrichtlijn geen wijziging aan te brengen, is erin gelegen dat de aard van genoemde instellingen dusdanig verschilt van de aard van andere Wwft-instellingen, dat het niet voor de hand ligt dat aan het cliëntenonderzoek van deze instellingen eenzelfde niveau van risicobeoordeling ten grondslag ligt."*

In Nederland vindt PPS-samenwerking zowel plaats op fenomeenbasis (bijv. AMLC, RIEC-LIEC) als op operationeel niveau (bijv. Fintell Alliance en FEC-PPS Serious Crime Task Force (SCTF)).

Uit de inzichten verkregen uit de verkenning volgt dat het creëren van een gelijkwaardige relatie tussen de publieke en private partners een belangrijk aandachtspunt is bij publiek-private samenwerking. Wederzijds vertrouwen, ervaren veiligheid, commitment, begrip en voldoende transparantie vormen een belangrijke basis voor een effectieve samenwerking. Ook een evenredige inzet van mensen en middelen speelt daarbij een belangrijke rol. De verkenning toont verder dat de PPS-initiatieven baat hebben bij een heldere (niet-complexe) governance en duidelijke vastlegging van doelen, partijen, en wederzijdse rollen en verantwoordelijkheden.

De onderzochte PPS-initiatieven in Nederland laten zien dat structurele samenwerking met operationele informatie (zoals transacties, meldingen en andere intelligence) in PPS-verband vooralsnog vooral plaatsvindt met banken. Hoewel beperkingen bestaan in de mogelijkheden voor gerichte informatiedeling, zijn de ervaringen daarbij in het algemeen positief te noemen. Daarom verdient het aanbeveling om deze vorm van PPS te bestendigen en uit te breiden naar andere categorieën poortwachters. Poortwachters en overheid dienen hier gezamenlijk stappen in te zetten. Daarbij dient er op grond van de verkregen inzichten wel voor te worden gewaakt dat niet te veel verschillende vormen van PPS opgezet worden en concrete acties ondergeschikt raken aan overleg en besluitvorming. Op basis van de verkregen inzichten is het aan te raden om deze nieuwe publiek-private samenwerking in eerste instantie via korte en concrete pilots op te starten, deze te evalueren om vervolgens tot een duurzame vorm van samenwerking te komen. Ook kan overwogen worden om andere categorieën poortwachters dan banken bij bestaande PPS-initiatieven aan te laten sluiten, zoals bij de SCTF.

Waar bovengenoemde aanbeveling zich richt tot zowel de poortwachters als de overheid, volgt hier nog wel een cruciale randvoorwaarde uit die door de overheid vervuld moet worden. Om écht effectief samen te kunnen werken en impact te kunnen maken, moet het juridisch mogelijk worden gemaakt om (gericht) informatie te delen – zowel tussen de publieke partners onderling, tussen de private partners onderling, als tussen de publieke en private partners.(363) Waar het wetsvoorstel Wet gegevensverwerking door samenwerkingsverbanden (WGS) oorspronkelijk de ambitie had om een gedegen grondslag te bieden voor de verwerking van persoonsgegevens door samenwerkingsverbanden, is het voorstel vanwege privacyoverwegingen meerdere keren aangepast, ingeperkt en nog altijd niet aangenomen.(364) Ook stoplichtconvenanten – bijvoorbeeld de samenwerking tussen makelaars, gemeenten en politie om criminaliteit in de huursector tegen te gaan – waar men zowel vanuit de private als de publieke sector positief over was, zijn beëindigd vanwege een gebrek aan juridische grondslag en beperkingen volgend uit de privacywetgeving.(365) Het wordt tijd dat in die rechtsgrond wordt voorzien.

Concrete stappen die poortwachters en overheid binnen het FEC-PPS kunnen nemen zijn:

1. Het verkennen van een eventuele uitbreiding van de SCTF in de vorm van een korte pilot met (in ieder geval) de trustkantoren en notarissen. Holland Quaestor en de KNB kunnen met de publieke deelnemers (de politie, het OM, FIU-NL en de FIOD) in gesprek gaan over de doelstellingen, werkwijze en governance van de pilot.
2. De beroepsorganisaties kunnen op basis van voorgaande binnen hun achterban nagaan welke organisaties bereid zijn om aan deze pilot deel te nemen, waarbij gegeven de verwachte inzet ook rekening wordt gehouden met de omvang van de instellingen.

(363) Zie ook de aanbeveling 'Creëer een waardevolle feedbackloop' in paragraaf 5.4.1.

(364) Zie paragraaf 3.2.5.

(365) Kamerstukken II, 2017/2018, 29 911, nr. 180.

3. Aan de hand van de eerste twee stappen kunnen betrokken poortwachters en de betrokken publieke partijen nadere afspraken maken over de korte pilot.
4. Op basis van bijvoorbeeld twee bijeenkomsten met de pilotgroep en betrokken publieke partijen kan de aanpak op de samenwerking worden aangescherpt en kan de groep van betrokken organisaties worden uitgebreid.

Een concrete stap die poortwachters en overheid hiervoor binnen het RIEC-LIEC kunnen nemen is:

Het opzetten van structurele, operationele samenwerking ten aanzien van vastgoed in de vorm van (hernieuwde) stoplichtafspraken tussen ten minste de makelaars, gemeenten en politie. Daarvoor is het belangrijk dat het RIEC-LIEC convenant voorziet in de mogelijkheid voor informatie-uitwisseling tussen huidige convenantpartners en relevante private partijen, zoals de makelaars. Het is daarbij bij gebrek aan regulering van het makelaarsberoep (zie aanbeveling in paragraaf 5.4.1) aan te raden om de samenwerking te beperken tot makelaars aangesloten bij de brancheverenigingen.

5.3.2 Digitale identiteit

Een tweede oplossingsrichting voor poortwachters en overheid samen betreft (het toewerken naar) het gebruik van digitale identiteiten in de context van het cliëntenonderzoek.

Zoals aangegeven in paragraaf 4.3 zijn digitale identiteiten op zichzelf geen nieuw fenomeen en spelen digitale authenticatiemiddelen een steeds grotere rol in de identificatie en verificatie van de identiteit van klanten, bijvoorbeeld in de context van 'non-face-to-face' onboarding. Het gebruik van digitale identiteiten en authenticatiemiddelen biedt zowel poortwachters als klanten verschillende operationele efficiënties bij cliëntenonderzoeken.(366) Voor de borging van privacy kan worden gewezen op het feit dat voor het gebruik van de gegevens de toestemming van de betrokken persoon vereist is.(367) Tevens worden op grond van de anti-witwasregelgeving en eIDAS-verordening eisen gesteld aan de betrouwbaarheidsniveaus van de digitale authenticatiemiddelen.

De inzichten verkregen uit de verkenning richten zich enerzijds op de poortwachters (er is al veel mogelijk) en anderzijds tot de overheid (ondersteun en maak mogelijk).(368)

Poortwachters

Poortwachters kunnen zelf al verschillende (voorbereidende) stappen zetten wat betreft het gebruik van digitale identiteiten en authenticatiemiddelen door:

1. Gebruik te (gaan) maken van digitale authenticatiemiddelen (eID-middelen) met eIDAS-niveau 'substantieel' of 'hoog' binnen de huidige juridische kaders van de Wwft/Sw. In afwachting van vaststelling door de overheid (zie aanbeveling 1 bij de overheid hierna) kunnen beroepsorganisaties en brancheverenigingen hun achterban al ondersteunen door voor hen te beoordelen welke aanbieders van authenticatiemiddelen aan de vereiste betrouwbaarheidsniveaus voldoen. Een externe partij kan een zogenaamde vendor-selectie voorbereiden, op basis van de kennis en ervaring met de technologische mogelijkheden en relevante randvoorwaarden, die zij inbrengt bij het opstellen van deze lijst.

(366) Zie paragraaf 4.3.1.
(367) Belangrijk voor de rechtsgeldigheid van het gebruik van toestemming conform artikel 6 lid 1 jo. artikel 4 sub 11 AVG is dat er in beginsel geen negatieve consequenties aan vast mogen zitten. Dat wil zeggen dat de betreffende (achterliggende) dienst ook op andere wijze voor de betrokkene beschikbaar moet zijn.
(368) Zie paragaaf 4.3.2.

2. Aan de hand van de gedeelde KYC-taxonomie (zie paragraaf 5.2.1) te bepalen voor welke datapunten en brondocumenten het wenselijk is om via 'de wallet' te koppelen aan digitale identiteiten, en door deze wensen te delen met de overheid. Daarbij moet rekening worden gehouden met het feit dat alleen die gegevens in de wallet worden opgenomen die afkomstig zijn van een betrouwbare en onafhankelijke bron.(369)

3. De mogelijkheden voor aansluiting bij, of de ontwikkeling van, een centraal afsprakenstelsel vanuit de poortwachters ten behoeve van de naleving van de Wwft/Sw te verkennen. Centrale afsprakenstelsels reguleren de (digitale) uitwisseling van persoonsgegevens, onder meer ten aanzien van governance, rollen en de verantwoordelijkheden van deelnemende partijen, verleende diensten, technische specificaties, veiligheidseisen (o.a. cybersecurity), privacy en juridische aspecten. Het is aan te bevelen dat daarbij andere stakeholders zoals vertrouwensdienstverleners, softwareleveranciers maar ook de overheid worden betrokken. Het perspectief van de klant (natuurlijke personen en rechtspersonen) is eveneens relevant om mee te nemen; aan de hand van klantreizen kan worden bepaald waar het gebruik van digitale identiteiten en zaken uit 'de wallet' de meeste waarde toevoegt.

Overheid

De overheid heeft een belangrijke taak bij het creëren van vertrouwen in het gebruik van digitale middelen in de context van de Wwft en Sanctiewet. Daar kunnen in elk geval twee stappen voor worden genomen:

1. Op de korte termijn is het belangrijk dat de overheid poortwachters ondersteunt bij het verduidelijken van welke (aanbieders van) identificatiemiddelen (e-ID-middel) voldoen aan het niveau 'substantieel' of 'hoog'. Vooralsnog wordt dit aan de individuele poortwachters zelf gelaten. Zo stelt de DNB Q&A Elektronische identificatiemiddelen en cliëntidentificatie het volgende: *"[i]nstellingen die in het kader van het uitvoeren van de vereiste cliëntonderzoeks-maatregelen een eID-middel overwegen te accepteren, stellen dus zelf vast, of door een ter zake deskundige, of het eID-middel in kwestie een voldoende betrouwbaar identificatiemiddel is als hiervoor bedoeld".*(370) Aangezien er geen duidelijk toetsingskader voor poortwachters bestaat, dit de nodige onduidelijkheid en een aanzienlijke inspanning voor poortwachters met zich brengt, belemmert dit (in het bijzonder kleine) poortwachters om van dergelijke middelen gebruik te maken. Wanneer de overheid deze informatie beschikbaar zou stellen, kunnen poortwachters zich richten op hun cliëntenonderzoek en het inrichten van een efficiënt(er) proces.

2. Op de middellange en lange termijn is het belangrijk dat de overheid werk maakt van een spoedige realisatie van het Europese digitaal paspoort en de attributen voor de 'wallet', waarbij zij de wensen van de poortwachters over datapunten en brondocumenten meeneemt (zie stap 2 bij de poortwachters). Ook is het belangrijk dat de overheid het gebruik hiervan in de Wwft/Sw-context stimuleert. Dat kan bijvoorbeeld door Europese digitale paspoorten als onafhankelijke en betrouwbare bron voor bepaalde (statische) klantgegevens aan te wijzen en toe te staan dat poortwachters uitsluitend op die informatie steunen bij het cliëntenonderzoek (i.e. geen aanvullende verificatie/bronnen nodig).(371)

5.4 Overheid

Om te komen tot een effectiever anti-witwasbeleid is het ook noodzakelijk dat de overheid – en waar het wijzigingen aan het wettelijk en regelgevend kader betreft: de wetgever – concrete stappen gaat zetten. Zoals reeds opgemerkt in de inleiding van dit hoofdstuk lijkt het moment aangebroken te zijn dat de overheid meer dan voorheen de poortwachters gaat motiveren om hun rol zo goed mogelijk te vervullen door hen duidelijkheid en ondersteuning 'aan de voorkant' te bieden.

(369) DNB 2022, p. 30.
(370) DNB, Q&A *Elektronische identificatiemiddelen en cliëntidentificatie*, beschikbaar via deze link.
(371) Zie bijlage B, paragraaf 2.

Terug naar de kern van het anti-witwasbeleid gaat het erom dat de overheid een duidelijke regierol pakt, waarmee zij (op hoofdlijnen) centraal stuurt en daarbij prioriteert op basis van de NRA.

Aanbevelingen specifiek gericht aan de overheid en wetgever richten zich in de eerste plaats op deze ondersteunende rol van de overheid richting poortwachters. Daarbij gaat het onder meer om het oplossen van conflicten of onduidelijkheden in wet- en regelgeving die een effectieve uitvoering van de poortwachtersfunctie in de weg staan en het geven van ondersteuning in de vorm van guidances en/of feedback. In de tweede plaats zien de aanbevelingen op het pakken van eigenaarschap en een sterkere centrale sturing, op het stellen van prioriteiten en het verbeteren van de risico-oriëntatie. Een sterkere centrale sturing, een beter inzicht in de daadwerkelijke risico's van witwassen, terrorismefinanciering en ontduiking van sancties, en een heldere prioritering aan de hand van de risico's stelt poortwachters maar ook de overheid zelf, in staat om de (beperkte) middelen zo effectief en gericht mogelijk in te zetten.

5.4.1 Ondersteunende overheid

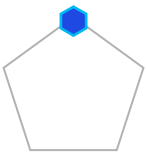
Poortwachters moeten hun klanten en de risico's die zij met zich meebrengen kennen en deze risico's zo veel mogelijk mitigeren om witwassen en terrorismefinanciering te voorkomen en daarmee de integriteit, stabiliteit en reputatie van het financiële stelsel te bewaken. Ondanks dat de bestrijding van criminaliteit een kerntaak is van de overheid, heeft de overheid binnen het anti-witwasbeleid een belangrijke rol aan poortwachters toebedeeld. Om tot een optimale invulling van de poortwachtersrol te komen, is het belangrijk dat poortwachters daartoe in staat worden gesteld, onder andere door hen het juiste instrumentarium en de benodigde duidelijkheid te bieden. Uit de knelpunten geïdentificeerd in hoofdstuk 3 komen enkele concrete wensen naar voren om de effectiviteit en efficiëntie van de naleving van de Wwft en Sanctiewet te verhogen. Dat leidt tot vijf aanbevelingen, die hierna verder worden uitgewerkt.

Wat betreft deze aanbevelingen kan de overheid al acties nemen, bijvoorbeeld door deze in bestaande wetgevingstrajecten mee te nemen. Bij de overige aanbevelingen is het wenselijk dat de overheid in overleg treedt met de brancheverenigingen en beroepsorganisaties van poortwachters over hoe en op welke termijn hier vervolg aan kan worden gegeven.

1 Maak werk van betrouwbare, publieke registers en zorg voor een adequate ontsluiting naar poortwachters

Als startpunt van relevante informatie en gegevens voor het cliëntenonderzoek is het belangrijk dat informatie uit publieke registers (zo) betrouwbaar (mogelijk) is. Om extra werk voor poortwachters te voorkomen, zouden zij in beginsel moeten kunnen vertrouwen op deze gegevens. Vijf concrete acties in relatie tot publieke registers zijn gewenst. Daarbij geldt dat voor sommige acties de overheid al eerder toezeggingen heeft gedaan, maar deze vooralsnog beperkt daadwerkelijk zijn geconcretiseerd.

1.a. Behoud de toegang tot het UBO-register voor poortwachters en alle instellingen die onder de RtSw 1977 vallen en geef aan hen ook toegang tot het afgesloten gedeelte

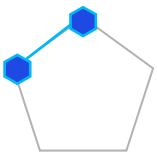
Complexiteit	Impact
	

In de consultatie van de Wijzigingswet beperking toegang UBO-registers wordt voorzien in de toegang tot het register voor poortwachters en instellingen die uitsluitend onder de RtSw 1977 vallen (waaronder schadeverzekeraars). Dit is een positieve eerste stap en poortwachters hopen dan ook dat de wijzigingswet binnen afzienbare tijd kan worden aangenomen.(372)

(372) Zie het voorgestelde artikel 22a lid 1 Handelsregisterwet 2007 in de consultatie van de Wijzigingswet beperking toegang UBO-registers. Zie voor nadere toelichting tevens p. 14-19 van de bijbehorende concept-Memorie van toelichting. De consultatie voor de Wijzigingswet beperking toegang UBO-registers is op 30 mei 2023 gestart en is beschikbaar via deze link.

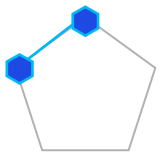
Wat vooralsnog niet geregeld wordt is de toegang tot het afgesloten gedeelte van het UBO-register. Echter, op grond van het EU AML Package, in het bijzonder de voorgestelde anti-witwasverordening, worden de verplichte gegevens voor de identificatie en de verificatie van de identiteit van UBO's naar alle waarschijnlijkheid flink uitgebreid.(373) Het gaat daarbij ook om gegevens die thans niet toegankelijk zijn voor poortwachters in het UBO-register, zoals volledige geboorteplaats en -datum en het woonadres.(374) Tijdens de afronding van dit onderzoek zijn de triloogonderhandelingen over het EU AML Package in volle gang, maar lijken de Commissie, de Raad en het Parlement eensgezind in de uitbreiding van identificatiegegevens voor UBO's. Daarom zouden poortwachters toegang tot het afgesloten gedeelte van het UBO-register moeten krijgen; of dienen het nut en de noodzaak van een afgesloten gedeelte heroverwogen te worden.

1.b. Geef poortwachters toegang tot de BRP voor de uitvoering van hun cliëntenonderzoek

Complexiteit	Impact
	

Poortwachters hebben op grond van de Wwft geen toegang tot de Basisregistratie Persoons-gegevens.(375) In navolging van voorgaande worden naar alle waarschijnlijkheid ook de verplichte gegevens voor de identificatie en de verificatie van de identiteit van klanten uitgebreid met het EU AML Package. Zo zullen poortwachters in het kader van hun cliëntenonderzoek verplicht worden om de nationaliteit(en) en het nationale identificatienummer van natuurlijke personen te identificeren en verifiëren.(376) Bij deze uitbreiding past ook de bevoegdheid voor poortwachters om deze informatie bij de bron te kunnen verifiëren, om een verdere disbalans tussen taken en bevoegdheden te voorkomen.(377)

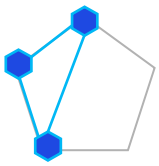
1.c. Maak werk van lopende wetgevingsinitiatieven die poortwachters kunnen helpen effectiever en efficiënter aan hun Wwft-verplichtingen te voldoen

Complexiteit	Impact
	

Een centraal aandeelhoudersregister (CAHR) met actuele en geverifieerde informatie over de aandeelhouders van besloten vennootschappen en niet-beursgenoteerde naamloze vennootschappen kan het cliëntenonderzoek effectiever en efficiënter maken. Ook het mogelijk maken van het 'zoeken op naam' van personen in het Handelsregister stelt poortwachters beter in staat om ongebruikelijke activiteit te identificeren, zoals betrokkenheid van een natuurlijk persoon bij verschillende (ogenschijnlijk niet-gerelateerde) ondernemingen. Initiatieven tot wijziging van wet- en regelgeving, of gesprekken daarover, lopen al lange tijd mede vanwege de impact ervan op de privacy. Het wordt tijd om stappen te zetten op deze dossiers om poortwachters – met inachtneming van privacy voor betrokkenen middels randvoorwaarden en waarborgen ('privacy-by-design') – de middelen te geven hun rol effectiever en efficiënter te vervullen.

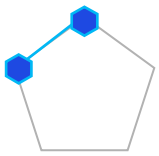
(373) Zie paragraaf 3.2.1.
(374) Artikel 18, tweede lid, jo. artikel 44 sub a AMLR (voorstel). De anti-witwasverordening bevindt zich momenteel in triloogfase tussen de Europese Commissie, de Raad van de Europese Unie en het Europees Parlement. Uit het standpunt van het Europees Parlement wordt duidelijk dat het een aanvullend datapunt voor de identificatie van UBO's wenst, te weten het belastingidentificatienummer. In Nederland is dat het burgerservicenummer (BSN).
(375) Er was even sprake van het ontsluiten van banken en notarissen ten behoeve van de uitvoering van het cliëntenonderzoek onder de Wwft, maar de toezegging van het kabinet om dit te regelen is (nog) niet opgevolgd.
(376) Artikel 18, eerste lid, AMLR (voorstel). Artikel 44, vierde lid, AMLR (voorstel) stelt dat de gegevens voor identificatie en verificatie van natuurlijke personen moeten worden verkregen aan de hand van een identiteitsdocument en informatie uit betrouwbare onafhankelijke bronnen; of door gebruik van digitale identificatiemiddelen.
(377) Zie paragraaf 3.3.1.

1.d. Overweeg poortwachters verder te ondersteunen door registers te creëren waarvoor poortwachters momenteel veelal gebruik moeten maken van commerciële aanbieders

Complexiteit	Impact
	

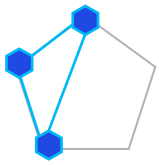
Het gaat bijvoorbeeld om een publiek register van politiek prominente personen (PEP-register) die poortwachters kunnen raadplegen in het kader van hun cliëntenonderzoek of actuele sanctielijsten die door instellingen worden gebruikt bij sanctiescreening.(378) Momenteel gebruiken poortwachters hier vaak commerciële dienstverleners voor, of doen zij handmatige checks tegen de toepasselijke sanctielijsten. Door een volledige, actuele sanctielijst en PEP-register beschikbaar te stellen aan poortwachters, kan de overheid poortwachters ondersteunen in het efficiënter naleven van wet- en regelgeving, omdat zij direct kunnen steunen op de informatie en ze bovendien minder kosten hoeven te dragen.

1.e. Overweeg sanctiechecks tegen publieke registers van overheidswege te verrichten en de onderzoeksinspanning voor bedrijven enigszins te verlichten

Complexiteit	Impact
	

Ieder bedrijf wordt geacht de zeggenschapsstructuur van klanten te onderzoeken om te bepalen of deze niet onder invloed staan van een gesanctioneerde persoon. Om bedrijven, waaronder poortwachters, enigszins te ontlasten in hun onderzoeksplicht, zou de Kamer van Koophandel (KVK) de taak kunnen krijgen om sanctiechecks te verrichten op de informatie zoals opgenomen in het Handelsregister en UBO-register. Wanneer er sprake is van (vermoedens van) sanctionering, zou de KVK hiervoor een aantekening moeten kunnen maken in het register. Hoewel dit partijen niet ontslaat van hun eigen (onderzoeks)plichten – die breder gaat dan de gegevens die in de twee registers zijn opgenomen – kan dit "*bijdragen aan een breder inzicht dat sprake is van sanctionering*".(379) Een stevigere rol voor de KVK past ook bij de ontwikkelingen in het kader van het EU AML Package. In de voorstellen worden beheerders van UBO-registers verplicht om de nauwkeurigheid van de gegevens van UBO's te controleren. Daartoe zouden de beheerders zelfs de bevoegdheid (moeten) krijgen om onderzoek ter plaatse bij bedrijven te verrichten.(380)

2 Creëer een waardevolle feedbackloop

Complexiteit	Impact
	

De roep om een effectieve feedbackloop vanuit de poortwachters bestaat mogelijk al zo lang als de meldplicht zelf bestaat. Geaggregeerde feedback in de vorm van typologieën en casuïstiek aan de hand van meldingen worden al gedeeld.(381) Ook jaaroverzichten van FIU-NL geven enig inzicht in het nut en de waarde van meldingen van ongebruikelijke transacties in generieke zin. Wat thans nog ontbreekt is een individuele terugkoppeling op het niveau van de meldende organisatie of de transactie waarop de melding betrekking heeft. Poortwachters kunnen hiervan leren door de kennis mee te nemen in de organisatie.

(378) In het buitenland worden PEP-registers in enkele gevallen door overheden beschikbaar gesteld aan poortwachters, bijvoorbeeld in Denemarken. Poortwachters mogen daar hun onderzoek op baseren: zie artikel 18(7) jo. artikel 2(8) Hvidvaskloven (Deense equivalent van de Wwft).
(379) Hoff en Hoff 2023, p. 11.
(380) De Europese Commissie en het Europees Parlement stellen zich op het standpunt dat beheerders deze bevoegdheid moeten krijgen, terwijl de Raad van de Europese Unie deze onderzoeksplicht niet (op voorhand) bij de beheerders van de UBO-registers wil plaatsen en de bevoegdheid tot onderzoek ter plaatse een lidstaatoptie wil laten zijn.
(381) Bijvoorbeeld via de Kennisbank en nieuwsbrieven van FIU-NL beschikbaar via de website www.fiu-nederland.nl.

Ook kan het een positief effect hebben op de meldingsbereidheid en kwaliteit van meldingen.[382] Momenteel wordt door FIU-NL enkel in een individuele terugkoppeling voorzien op het moment dat een melding van een ongebruikelijke transactie verdacht verklaard wordt. Dit is een geautomatiseerde mededeling zonder inhoudelijke toelichting.[383]

In de beleidsagenda aanpak witwassen zijn het verbeteren van het inzicht in het gebruik van verdachte transacties en de feedbackloop aangemerkt als een prioriteit. De beleidsagenda geeft echter niet aan hoe invulling wordt gegeven aan de verbetering van de feedbackloop.[384] Eerder in dit onderzoek is ook aangegeven dat het OM samen met de FIOD, FIU-NL en politie binnen de verdachte transactie (VT)-werkgroep hieraan werkt en dat de banken kort geleden zijn aangesloten bij deze werkgroep.

Sectorale feedbackloop

Een start voor het creëren van een waardevolle feedbackloop kan worden gemaakt door het op sectorniveau terugkoppelen van uitkomsten van gedane meldingen vanuit die sector over een bepaalde periode door FIU-NL, eventueel samen met de opsporing, binnen de huidige wettelijke kaders. Voor een waardevolle feedbackloop op individueel niveau zou het FIU-NL en opsporingsautoriteiten juridisch mogelijk moeten worden gemaakt om op individueel niveau een terugkoppeling te geven aan meldende instellingen, zonder de specifieke informatie te delen of verdere opsporing in gevaar te brengen.

Het sectorspecifiek verstrekken van een terugkoppeling over gedane meldingen in een bepaalde periode geeft een sector al wat meer mogelijkheden om inzicht te krijgen in het nut en de waarde van meldingen ten opzichte van de geaggregeerde feedback die nu wordt gedeeld. FIU-NL zou hiervoor periodiek de beroepsorganisaties en/of brancheverenigingen kunnen informeren en daarbij eventuele behoeftes over aard van informatie van de verschillende sectoren mee kunnen nemen. In de sectorspecifieke terugkoppeling zou ook opsporingsinformatie kunnen worden opgenomen; deze kan door opsporingsautoriteiten desgevraagd aan FIU-NL worden verstrekt of opsporing kan de terugkoppeling op sectorniveau samen met FIU-NL geven binnen de mogelijkheden van de wettelijke kaders.

Individuele feedbackloop

Bij het uitwerken van een feedbackloop op individuele meldingen kan FIU-NL mogelijk leren van ervaringen in het buitenland. Voor het inrichten van de feedbackloop kan worden gedacht aan een standaardtermijn voor de terugkoppeling van meldingen van ongebruikelijke transacties die zijn gedaan op basis van subjectieve indicatoren. Ongeacht of verdachtverklaring heeft plaatsgevonden, ontvangt een meldende instelling na een bepaalde periode na het doen van de melding een terugkoppeling met een reden op categorale basis.[385] Daarbij kan ook als reden worden meegenomen dat een melding kwalitatief onvoldoende was; hier kunnen poortwachters dan mee aan de slag. Wanneer ongebruikelijke transacties binnen een periode van vijf jaar alsnog verdacht verklaard kunnen worden, bijvoorbeeld via de koppeling met meldingen die later bij FIU-NL zijn gedaan, een buitenlands FIU-verzoek of door nieuwe opsporingsinformatie, zouden de poortwachters (nog een keer) geïnformeerd kunnen worden over de verdachtverklaring met daarbij een reden op categorale basis.

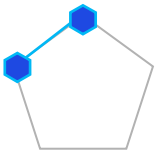
Technologie kan helpen om het proces van de individuele feedbackloop efficiënter te maken. Wanneer poortwachters in staat worden gesteld om bovengenoemde terugkoppelingsmomenten op individueel niveau te 'tracken' in een systeem kunnen zij zelf op elk gewenst moment de stand van zaken nagaan. Deze automatisering kan bovendien een minder grote impact hebben op FIU-NL qua werklast.

(382) Zie paragraaf 3.3.2; DNB 2022, p.6.
(383) FIU-Nederland, *Ik heb een melding gedaan: wat nu?*, beschikbaar via deze link.
(384) Kamerstukken II, 2022/2023, 31 477, nr. 80. De beleidsagenda betreft bijlage 1.
(385) Categorale redenen voor geen verdachtverklaring kunnen bijvoorbeeld zijn dat de melding te weinig informatie bevatte (kwaliteitsindicatie) of dat na analyse geen verdachtverklaring mogelijk was. Categorale redenen voor een verdachtverklaring kunnen bijvoorbeeld de doormeldredenen zijn die FIU-NL thans in generieke zin in haar jaaroverzicht opneemt. Zie FIU 2021, p. 9.

Inzicht in het gebruik van verdachte transacties door opsporing en OM

Met betrekking tot verdacht verklaarde transacties is het waardevol voor poortwachters om (meer) inzicht te krijgen in het gebruik van de door hen gemelde verdachte transacties in het strafrechtelijke opsporingsproces.(386) Opsporingsdiensten en het OM zouden daarom ten minste op een geaggregeerd niveau een terugkoppeling moeten (kunnen) geven, bijvoorbeeld in de vorm van statistieken en het delen van casuïstiek. In de beleidsagenda aanpak witwassen is het opstellen en jaarlijks publiceren van relevante statistieken als actiepunt opgenomen.(387) Daarbij gaat het onder andere om het aantal strafrechtelijke onderzoeken en rechterlijke uitspraken (veroordelingen, vrijspraak).(388) Het publiceren van statistieken is een stap in de goede richting en kan bijdragen aan het verschaffen van het gewenste inzicht, in het bijzonder wanneer de cijfers aangevuld worden met een toelichting vanuit opsporing en/of OM om deze in de juiste context te plaatsen.

3 Reguleer het makelaarsberoep en overweeg een Wwft-registratieplicht in te voeren voor niet-gereguleerde beroepen en instellingen

Complexiteit	Impact
	

Zoals uit hoofdstuk 2 is gebleken is de vastgoedsector kwetsbaar voor witwassen. Dat het makelaarsberoep in Nederland niet gereguleerd is, maakt de sector in potentie nog kwetsbaarder: er worden geen minimumkwaliteitseisen gesteld noch wordt er een verplichte aansluiting bij beroepsorganisaties vereist. Het is daardoor nagenoeg onmogelijk te achterhalen hoeveel makelaars daadwerkelijk actief zijn in Nederland, omdat niet alle makelaars aangesloten zijn bij een van de drie brancheverengingen (NVM, VBO en VastgoedPro). Dit gebrek aan afbakening heeft mogelijk ook impact op het toekennen van bevoegdheden.(389) Reeds eerder is daarom gepleit voor het opnieuw reguleren van het makelaarsberoep.(390)

Gegeven het belang van de poortwachtersrol en daarbij een goede balans tussen taken en bevoegdheden, in samenhang met de oplossingsrichting over de ontwikkeling van waarschuwingssystemen (paragraaf 5.2.2) en de aanbeveling om poortwachters ook toegang te geven tot de BRP eerder in deze paragraaf, is het inderdaad zinvol om regulering van het makelaarsberoep opnieuw te introduceren. Het is daarbij belangrijk om de lessen uit het verleden te betrekken bij de regulering van het beroep; regulering zou niet (uitsluitend) moeten gaan om titelbescherming en beëdiging. Regulering van het makelaarsberoep zou gepaard moeten gaan met doorlopende kwaliteits- en integriteitseisen – zoals thans door brancheorganisaties NVM, VBO en VastgoedPro wordt voorgestaan vis-à-vis hun leden – en een verbod om op te treden als makelaar indien deze niet aan de wettelijke reguleringsvereisten voldoet.

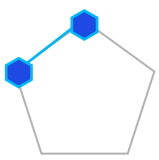
Regulering van het makelaarsberoep kan samengaan met het invoeren van een Wwft-registratieplicht voor niet-gereguleerde beroepen en instellingen.(391) In aanvulling op voorgaande zal ook de toezichthouder baat hebben bij een duidelijk afgebakende groep onder toezicht staande instellingen, omdat de toezichthouder daarmee de beperkte middelen ook daadwerkelijk kan richten op het verrichten van het toezicht in plaats van op het uitzoeken van welke partijen binnen de toezichtpopulatie behoren.(392)

Ook kan regulering van het makelaarsberoep gepaard gaan met een heroverweging van de huidige Wwft-vereisten en -praktijk ten aanzien het cliëntenonderzoek op de wederpartij.

(386) Vgl. DNB 2022, p. 6; Algemene Rekenkamer 2022, p. 30.
(387) Brief van de minister van Financiën over voortgang beleidsagenda aanpak witwassen: Kamerstukken I, 2022/2023, 31 477 en 34 08, D[1] (de letter D heeft alleen betrekking op 31 477), bijlage 2 (Toelichting stand van zaken beleidsagenda aanpak witwassen).
(388) Zie Brief van de minister van Financiën over voortgang beleidsagenda aanpak witwassen: Kamerstukken I, 2022/2023, 31 477 en 34 08, bijlage 4.
(389) Hoogenboom 2021, p. 40.
(390) Hoogenboom 2021, p. 171.
(391) Van den Broek 2015, p. 465-466.
(392) Van den Broek 2015, p. 57.

Zoals aangegeven in hoofdstuk 3 bestaat een verbod op tweezijdige bemiddeling door makelaars. Daardoor kan het voorkomen dat wanneer koper en verkoper allebei gebruikmaken van een makelaar, zij allebei naast de eigen klant ook elkaars klanten (als wederpartij) moeten betrekken bij hun cliëntenonderzoek. Daarmee wordt onderzoek 'dubbelop' gedaan. De toezichthouder heeft in de leidraad aangegeven dat makelaars het cliëntonderzoek van de wederpartij aan elkaar kunnen uitbesteden. Echter, daarmee ligt de verantwoordelijkheid voor het uitgevoerde cliëntenonderzoek op de wederpartij alsnog bij de makelaar van de cliënt. Regulering van het makelaarsberoep met doorlopende kwaliteits- en integriteitseisen zou aanleiding kunnen zijn om in dit geval op elkaars cliëntenonderzoeken te kunnen steunen, waarbij de verantwoordelijkheid voor het uitgevoerde cliëntenonderzoek bij de makelaars van de eigen cliënten blijft liggen. Daarvoor zullen makelaars wel de relevante documentatie over elkaars klanten met elkaar moeten delen en zich er daarbij van moeten vergewissen dat het verrichte onderzoek naar de wederpartij (de cliënt van de andere makelaar) voldoet aan de eigen interne eisen en risicoclassificatie. Indien dat niet het geval is, zal de makelaar alsnog zelf aanvullend onderzoek moeten verrichten. Het creëren van een KYC-taxonomie zoals opgenomen als oplossingsrichting in paragraaf 5.2.1 kan bijdragen aan het harmoniseren van cliëntenonderzoeken door makelaars.

4 Bescherm poortwachters in het geval van angst voor represailles bij het doen van meldingen van ongebruikelijke transacties

Complexiteit	Impact
	

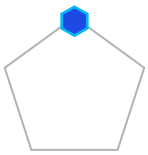
Een knelpunt ervaren door poortwachters betreft de angst voor represailles bij het doen van meldingen van ongebruikelijke transacties bij FIU-NL. Dit geldt in het bijzonder voor 'kleine' poortwachters, omdat de bedrijfs- of kantoornaam soms gelijk is aan de naam van de natuurlijke persoon of omdat vanwege het geringe aantal medewerkers snel duidelijk is wie de melding heeft gemaakt. Echter, ook medewerkers van grote Wwft-instellingen – zoals de medewerkers die het klantcontact onderhouden – krijgen steeds vaker te maken met (concrete) bedreigingen.

Zoals beschreven in paragraaf 3.3.2 zijn de afgelopen jaren al enkele maatregelen genomen en heeft de minister aangekondigd verschillende oplossingen te verkennen om (het gevoel van) veiligheid van melders te versterken. Hierbij past het om te overwegen om de wijze van melden aan te passen. De AMLD staat het toe dat accountants, belastingadviseurs, notarissen, advocaten en makelaars melden via hun beroepsorganisaties; van deze lidstaatoptie is door de Nederlandse wetgever geen gebruik gemaakt.(393)

Als alternatief kan worden gedacht aan het zoeken van aansluiting bij regelingen zoals die voor bijvoorbeeld getuigen in strafprocedures gelden. In dit geval kan overwogen worden om daarbij het belang van de melding in de strafvervolging centraal te stellen: indien de melding voornamelijk als ondersteunend bewijs dient in het strafproces en het dossier naar mening van het OM voldoende overig wettig bewijs bevat om de schuldvaststelling te kunnen dragen, dient ervoor gekozen te worden om de melding buiten het dossier te laten. Indien de melding ondersteunend bewijs is waarbij het OM er niet van overtuigd is dat het strafdossier reeds voldoende wettig bewijs bevat, zou de naam van de poortwachter ten minste moeten worden geanonimiseerd of gepseudonimiseerd. Eveneens dient de melding op niet-herleidbare wijze te worden opgenomen in het strafdossier.

(393) Artikel 34(1) AMLD5. Ook in artikel 51 van de concepttekst (Raadsversie) van de AMLR is deze mogelijkheid opgenomen.

5 Geef publieke voorlichting over de rol en verantwoordelijkheden van poortwachters

Complexiteit	Impact
	

Ondersteuning door de overheid kan ook plaatsvinden in de vorm van voorlichting. Zoals in hoofdstuk 2 beschreven, worden partijen om verschillende redenen als poortwachter aangewezen en bestaan er accentverschillen in de rollen en verantwoordelijkheden. Voor de buitenwereld kan het daarom onduidelijk zijn wat de poortwachtersrol inhoudt, wat poortwachters moeten doen en wat dat in de praktijk betekent voor klanten. Om poortwachters in staat te stellen hun beperkte middelen daadwerkelijk in te zetten voor de vervulling van hun poortwachtersrol, zou de overheid meer publieke voorlichting moeten geven.

De beleidsagenda aanpak witwassen, waar het verbeteren van de voorlichting richting klanten over het doel van de Wwft en de informatie die instellingen nodig hebben voor het cliëntenonderzoek als een van de actiepunten is opgenomen, is een eerste stap in de goede richting.(394) Het actiepunt is echter een uitwerking van het borgen van betalingsverkeer en zodoende beperkt de voorlichting zich tot de bancaire sector.

De overheid zet zich bij voorkeur in voor een bredere oplossing voor alle categorieën poortwachters. Hierbij kan worden gedacht aan het bieden van een (digitale) plek waar voorlichting is te vinden voor klanten van poortwachters over de rollen en verplichtingen van poortwachters bij de naleving van de Wwft en de Sanctiewet. De voorlichting zou wel verder moeten gaan dan het bij elkaar brengen en opsommen van de toepasselijke wet- en regelgeving en de contactgegevens van betrokken publieke en private partijen. Daarnaast zou de overheid een campagne kunnen starten om de samenleving in brede zin kennis te laten maken met het anti-witwasbeleid en de rollen en verantwoordelijkheden van poortwachters. Ook zou de overheid kunnen overwegen een vragen- en/of klachtenloket in te richten, zodat poortwachters bij vragen van of een geschil met klanten hen kunnen doorverwijzen naar de overheid.

5.4.2 Centrale sturing

Het anti-witwasbeleid in Nederland laat zich kenmerken door een hoge mate van fragmentatie. Het is een op zichzelf staand beleidsterrein, maar valt binnen de bredere aanpak van georganiseerde criminaliteit. Dit maakt dat er veel verschillende overheidspartijen betrokken zijn variërend van departementen, toezichthouders, gemeenten, FIU, overheidsdiensten en uitvoeringsorganisaties, opsporingsinstanties tot het OM. Zoals aangegeven in paragraaf 3.3.2. hebben al deze partijen een eigen taak in het kader van de bestrijding van ondermijning en/of financieel-economische criminaliteit en hebben zij hun eigen belangen te behartigen. Uit interviews komt het beeld naar voren dat er veel wordt ‘gepolderd’ tussen deze overheidspartijen.(395) Dit heeft een negatieve impact op de poortwachters.

Een gebrek aan een centrale sturing, inclusief een duidelijke prioritering en belangenafweging, kan ertoe leiden dat de overheid geen duidelijke keuzes maakt en daardoor gaat dralen en verzanden in algemene toezeggingen in plaats van concrete actie te nemen.(396) Daardoor wordt, onder andere, weinig voortgang gemaakt in wetgevingsprocessen. Dat is al het geval bij verschillende wetgevingstrajecten en projecten die het preventieve anti-witwasbeleid raken. Te denken valt aan wetgevingstrajecten rondom de Wet gegevensverwerking samenwerkingsverbanden (WGS) en het Centraal Aandeelhoudersregister (CAHR). Gegeven het spanningsveld in het wetsvoorstel Wet plan van aanpak witwassen tussen het effectief bestrijden van witwassen en terrorismefinancieringen enerzijds en het beschermen van privacy anderzijds bestaat ook hier een groot risico op een moeizaam, langdurig wetgevingstraject.

(394) Brief van de minister van Financiën over voortgang beleidsagenda aanpak witwassen: Kamerstukken I, 2022/2023, 31 477 en 34 08, D[1] (de letter D heeft alleen betrekking op 31 477), bijlage 2 (Toelichting stand van zaken beleidsagenda aanpak witwassen).

(395) Zie paragraaf 3.3.2.

(396) Vgl. Nelen et al. 2023 p. 190-191.

Bovendien is het uitermate onzeker of het wetsvoorstel zoals dat in oktober 2022 naar de Tweede Kamer is verzonden, ook daadwerkelijk in de voorgestelde vorm aangenomen wordt. Verder bevat de beleidsagenda voortgang witwassen veel toezeggingen voor bepaalde inspanningen zonder concrete resultaten. Dit valt op te maken uit de wijze van formuleren: 'bezien', 'versterken', 'onderzoeken', 'inzetten op', 'bevorderen', 'in gesprek met' zijn hier enkele voorbeelden van. Daar komt bij dat de voortgangsrapportage uit mei 2023 meldt dat enkele cruciale inspanningen met betrekking tot samenwerking worden uitgesteld vanwege zorgen op het gebied van privacy.(397)

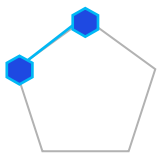
4. Behouden effectieve gegevensdeling en samenwerking	• Bestendigen en doorontwikkelen van samenwerking en gegevensdeling in de aanpak van witwassen, waarbij ook partijen buiten de financiële sector worden betrokken	• Uitgesteld. Naar aanleiding van de zorgen op het gebied van privacy, zie bijvoorbeeld de Wet gegevensverwerking samenwerkingsverbanden (WGS) en het Wetsvoorstel Plan van aanpak witwassen, is het op dit moment niet opportuun om het bestaande stelsel verder uit te werken.
	• Onderzoeken verdere mogelijkheden om huidige samenwerking te verbeteren	• Uitgesteld. Gesprekken met de relevante belanghebbenden zullen wel worden afgerond.
	• Introductie maatregelen uit het wetsvoorstel plan van aanpak witwassen met verbeteringen op het gebied van gegevensdeling	• Loopt. Het wetsvoorstel plan van aanpak witwassen is in oktober 2022 naar de Tweede Kamer verzonden.

Bron: Stand van zaken beleidsagenda aanpak witwassen voortgangsbrief bijlage 1, p.4.

Met een eenduidige visie van de overheid waarbij de verschillende belangen van betrokken overheidspartijen al op voorhand afgewogen zijn en keuzes zijn gemaakt, kan dergelijke 'verlamming' worden voorkomen en tot actie worden overgegaan. Dit geeft bovendien richting en duiding aan poortwachters waar zij zich in het kader van de risicogebaseerde benadering op moeten richten en waar het, in de woorden van de overheid, 'minder kan'.(398) Poortwachters hebben dan geen, of minder, last van de verlammende effecten en onduidelijkheden die een gebrek aan eenduidige sturing en belangenafweging met zich meebrengt. Duidelijkheid draagt bij aan de motivatie van poortwachters, die met de gegeven sturing (nog) gericht(er) aan de slag kunnen gaan.

Concreet leidt het voorgaande tot de volgende aanbevelingen:

1 Wijs een nationale coördinator namens de overheid aan die de regie pakt in de nationale anti-witwasaanpak

Complexiteit	Impact
	

De coördinator acteert idealiter op de hoofdlijnen en treedt op als verbinder tussen de betrokken publieke partijen en hun belangen, als aanjager van een effectief en efficiënt anti-witwasbeleid, en is namens de overheid richting de private sector het gezicht of boegbeeld van deze nationale aanpak. De coördinator wordt daarbij verantwoordelijk gemaakt voor de volgende zaken:

(397) Brief van de minister van Financiën over voortgang beleidsagenda aanpak witwassen: Kamerstukken I, 2022/2023, 31 477 en 34 08, D[1] (de letter D heeft alleen betrekking op 31 477). De brief heeft 6 bijlagen.

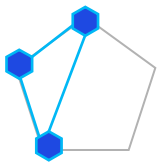
(398) Kamerstukken II, 2022/2023, 31 477, nr. 80. De beleidsagenda betreft bijlage 1.

- Het zorgdragen voor de behartiging van de verschillende (overheids)belangen die de bestrijding van witwassen en terrorismefinanciering raken. Dit betekent dat de coördinator verschillende overheidspartijen op (inter)departementaal niveau, maar ook toezichthouders (Wwft, privacy, mededinging) en andere overheidsdiensten, bij elkaar brengt en dat dit ertoe leidt dat duidelijke keuzes worden gemaakt. Waar verschillende belangen elkaar raken en een wettelijke verankering moet worden gezocht, dient de coördinator de wetgever te adviseren over de (gewenste) afweging van de belangen.
- Het bestendigen van de nationale anti-witwasaanpak in een strategie gebaseerd op de daadwerkelijke risico's voor Nederland (zie ook de aanbeveling 'Versterk, verdiep en breid de nationale risk assessment uit') en waarin keuzes worden gemaakt ten aanzien van de prioriteiten bij de bestrijding van witwassen en terrorisme-financiering (zie ook de aanbeveling 'Prioriteer en stel een risk appetite voor Nederland vast').
- Het binnen het nationale anti-witwasbeleid stimuleren van een duurzame, structurele samenwerking en het afstemmen van de verschillende publiek-private samenwerkingsinitiatieven.
- Het borgen dat de nationale anti-witwasaanpak is afgestemd op andere nationale programma's en beleidsterreinen, zoals de bredere nationale aanpak van ondermijnende (drugs)criminaliteit en (modernisering van) het sanctiestelsel.
- Het monitoren van de nationale anti-witwasaanpak en het adviseren van de overheid waar wijzigingen in de aanpak noodzakelijk zijn om te komen tot een effectiever anti-witwasbeleid met inachtneming van aanpalende belangen.
- Het functioneren als primair aanspreekpunt voor de private sector, waaronder de poortwachters.

De rol kan door een natuurlijke persoon worden vervuld, zoals Stef Blok dat (tijdelijk) deed als Nationaal Coördinator Sanctienaleving en Handhaving, of door een organisatie. In het Verenigd Koninkrijk is bijvoorbeeld het National Economic Crime Centre (NECC) aangewezen als 'system leader' op het gebied van het bestrijden van economische criminaliteit, witwassen, terrorismefinanciering en proliferatiefinanciering.(399)

Waar de poortwachtersrol en de naleving van de Sanctiewet en onderliggende regelgeving elkaar raken, ligt samenwerking met de nationale coördinator, of coördinerende autoriteit, voor de naleving van sancties voor de hand.(400)

2 Versterk, verdiep en breid de nationale risk assessment uit

Complexiteit	Impact
	

Nationale risicobeoordelingen (National Risk Assessments, NRA) zijn het fundament voor een nationale anti-witwasstrategie en de risicogebaseerde benadering in het anti-witwasbeleid. Uit dit onderzoek is naar voren gekomen dat bij poortwachters de behoefte bestaat om een beter begrip te krijgen van de daadwerkelijk grootste bedreigingen voor de integriteit van de financiële sector.(401)

Door de overheid is het beter gebruik en de verdieping van de NRA reeds als een van de prioriteiten opgenomen in de beleidsagenda aanpak witwassen.(402) Een belangrijk aandachtspunt voor verbetering en verdieping van de NRA witwassen zal daarbij het gebruik van diverse databronnen zijn. Momenteel steunt de NRA (bijna) volledig op expertmeningen.(403) In de literatuur wordt echter gesteld dat NRA's uit meerdere informatiebronnen moeten bestaan om geloofwaardig te kunnen zijn.(404)

(399) Zie bijlage B, paragraaf 4.4.
(400) Nationaal coördinator sanctienaleving en handhaving 2022.
(401) Zie paragraaf 3.3.2.
(402) Kamerstukken II, 2022/2023, 31 477, nr. 80. De beleidsagenda betreft bijlage 1.
(403) WODC 2020, p. 21-33.
(404) Ferwerda en Reuter 2022, p. 26.

In de beleidsagenda aanpak witwassen is het opstellen en jaarlijks publiceren van relevante statistieken als actiepunt opgenomen.(405) Daarbij gaat het bijvoorbeeld om toezichtstatistieken (aantal onderzoeken, aantal geconstateerde overtredingen, aantal handhavingsacties) of het aantal strafrechtelijke onderzoeken en rechterlijke uitspraken (veroordelingen, vrijspraak).(406) Het bijhouden van statistieken is een stap in de goede richting en kan op termijn bijdragen aan het versterken van de NRA door deze meer *evidence-based* te maken. Dit vereist overigens niet alleen inzet en commitment van de overheid (toezicht, FIU opsporing), ook poortwachters zullen relevante data moeten bijhouden en delen ten behoeve van de NRA.

Op basis van een analyse van meerdere NRA's in de verkenning komen nog enkele andere punten naar voren die bij kunnen dragen aan een betekenisvolle versterking en verdieping van de NRA en die poortwachters concretere handvatten kunnen geven dan thans het geval is. Uit de verkregen inzichten volgen de volgende suggesties:

1. Overweeg om de NRA in te steken vanuit het perspectief van de onderliggende criminaliteit, de gronddelicten, in plaats van de witwasmethoden.
2. Overweeg om de NRA te richten op inherente risico's.
3. Verbreed de NRA door geografische risico's toe te voegen. Daarbij zouden de voor Nederland belangrijkste economische sectoren en financiële producten in kaart kunnen worden gebracht en kunnen worden gekeken naar de aard en omvang van handelsrelaties, transacties met hoogrisicolanden en de risico's die buurlanden of landen binnen het Koninkrijk der Nederlanden met zich brengen.
4. Verdiep de NRA door in te gaan op regionale verschillen binnen Nederland ('regionale risicobeoordelingen'). De onderliggende criminaliteit en de daarmee gepaarde witwasrisico's kunnen verschillen tussen regio's. Denk bijvoorbeeld aan regio's met luchthavens, havens, grensgebieden, stedelijke gebieden of buitengebieden.
5. Verdiep de NRA door in aanvulling daarop sectorale risicobeoordelingen te verrichten, waarmee de NRA wordt door vertaald en verder wordt uitgewerkt per categorie poortwachter. Dit biedt de verschillende poortwachters meer concrete handvatten, die zij ook weer in hun eigen risicobeoordelingen kunnen meenemen.

3 Prioriteer en stel een risk appetite voor Nederland vast

Als fundament voor de risicogebaseerde benadering is de NRA ook bij uitstek het startpunt voor de nationale anti-witwasaanpak. Voor het kunnen uitoefenen van centrale sturing (zie aanbeveling 'Wijs een nationale coördinator namens de overheid aan die de regie pakt in de nationale anti-witwasaanpak') zijn een strategie en daarop gebaseerd beleid belangrijk. Een goede strategie stelt kaders, geeft richting en stelt in staat om prioriteiten aan te brengen. Prioriteiten helpen bij het aanbrengen van focus in de risicogebaseerde benadering en daarmee ook de inzet van de (beperkte) middelen.

Het is niet realistisch te stellen dat met een effectieve toepassing van het anti-witwasbeleid het witwassen compleet voorkomen kan worden. Het is evenmin realistisch om van poortwachters te verwachten dat zij hun poorten zodanig bewaken dat er helemaal geen crimineel geld het financiële systeem binnenkomt.

(405) Brief van de minister van Financiën over voortgang beleidsagenda aanpak witwassen: Kamerstukken I, 2022/2023, 31 477 en 34 08, D[1] (de letter D heeft alleen betrekking op 31 477), bijlage 2 (Toelichting stand van zaken beleidsagenda aanpak witwassen).

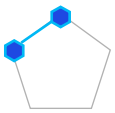
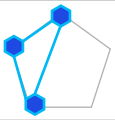
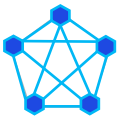
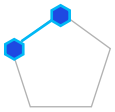
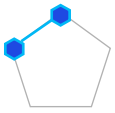
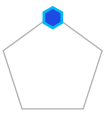
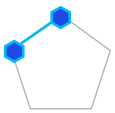
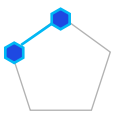
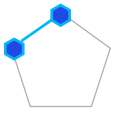
(406) Zie Brief van de minister van Financiën over voortgang beleidsagenda aanpak witwassen: Kamerstukken I, 2022/2023, 31 477 en 34 08, bijlage 4.

Met prioriteitstelling in een nationale anti-witwasstrategie kan de inzet van poortwachters zich vooral richten op de belangrijkste nationale prioriteiten. Omdat niet alles een prioriteit kan zijn of kan blijven, betekent dit uiteraard ook dat de inzet op andere vlakken minder zal zijn. Het is daarom aan te raden dat de Nederlandse overheid met de NRA en bij de vaststelling van haar prioriteiten ook een nationale risk appetite vaststelt die samen met de gestelde prioriteiten als bandbreedte kan dienen voor de risicogebaseerde toepassing van het anti-witwasbeleid, en dus voor de poortwachters bij de uitoefening van hun rol.

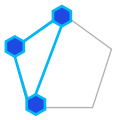
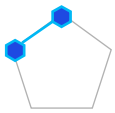
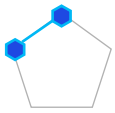
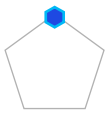
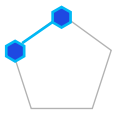
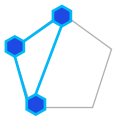
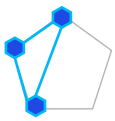
In Nederland heeft de overheid de afgelopen jaren al positieve stappen gezet met onder meer het plan van aanpak witwassen uit 2019 en de beleidsagenda aanpak witwassen uit 2022. De verkregen inzichten uit de verkenning laten echter zien dat de komende jaren verdere stappen gezet moeten worden om (nog) effectiever te worden. Zo zou de NRA idealiter geen onderdeel, maar het startpunt moeten zijn van de ontwikkeling van een nationale anti-witwasstrategie. En binnen die strategie zullen duidelijke prioriteiten moeten worden gesteld die concreet genoeg zijn om sturing te geven aan de (verwachte) inzet van poortwachters. Het recente Economic Crime Plan 2 uit het Verenigd Koninkrijk kan daarbij als voorbeeld dienen voor de Nederlandse overheid: een duidelijke commitment van de private sector bij de totstandkoming van de strategie en duidelijke prioriteiten met een concrete uitwerking, gekoppeld aan heldere tijdlijnen en continue monitoring van de voortgang.

5.5 Van oplossingsrichtingen naar actie

Op basis van het uitgevoerde onderzoek zijn in voorgaande paragrafen enkele oplossingsrichtingen voorgesteld die kunnen bijdragen aan een verbetering van de efficiëntie en effectiviteit van de anti-witwasketen en de naleving van de Sanctiewet, en in het verlengde daarvan de effectiviteit van het anti-witwassysteem in Nederland. Daarbij is een onderscheid gemaakt tussen de verwachte complexiteit en de impact van de oplossingsrichtingen. Tabel 1 zet de oplossingsrichtingen op een rij.

Oplossingsrichting	Complexiteit	Impact
Poortwachters		
KYC-taxonomie		
Waarschuwings-systemen		
Gezamenlijke voorzieningen		
Poortwachters en overheid		
Publiek-private samenwerking		
Digitale identiteit		
Overheid		
Ondersteunende overheid		
Publieke registers • Toegang tot (afgeschermde gedeelte) UBO-register		
• Toegang tot BRP		
• Lopende initiatieven (CAHR, zoekfunctie personen Handelsregister		
• Publiek PEP-register en sanctielijsten		
• Sanctiechecks van overheidswege		

Tabel 1: Complexiteit en impact van voorgestelde oplossingsrichtingen
(vervolg op volgende pagina)

Oplossingsrichting	Complexiteit	Impact
Overheid		
Ondersteunende overheid		
Creatie waardevolle feedbackloop		
Regulering makelaarsberoep en Wwft-registratieplicht		
Bescherming poortwachters bij angst voor represailles		
Publieke voorlichting over de rol en verantwoordelijk-heden van poortwachters		
Centrale sturing		
Nationale coördinator		
Nationaal risico assessment		
Prioritering en vaststellen *risk appetite*		

Tabel 1: Complexiteit en impact van voorgestelde oplossingsrichtingen (vervolg)

De mate waarin de oplossingsrichtingen gerealiseerd gaan worden en hun volle potentieel benut wordt, zal afhangen van de inzet en de commitment van poortwachters en de overheid. Voor de poortwachters is het zaak dat zij de concrete stappen binnen de mogelijkheden die zij daartoe hebben ook (durven) gaan zetten. Voor de overheid is het belangrijk dat zij de poortwachters daartoe in staat stelt. Daarbij gaat het om het geven van bevoegdheden en het wegnemen van (juridische) onduidelijkheden of conflicten. In het licht van de verwachte impact is het toewerken naar sterke centrale sturing van wezenlijk belang. Centrale sturing vereist een heldere nationale anti-witwasaanpak neergelegd in een strategie die is gebaseerd op de daadwerkelijke risico's voor Nederland, en waarin duidelijke keuzes worden gemaakt ten aanzien van de prioriteiten bij de bestrijding van witwassen en terrorismefinanciering.

Veel oplossingsrichtingen worden geraakt door de huidige discussie rondom privacy. Daarom moet de hoogste prioriteit liggen bij het afwegen van het belang van privacy enerzijds, en het voorkomen van witwassen en terrorismefinanciering (en in het verlengde daarvan de bestrijding van criminaliteit) anderzijds. De huidige situatie waarin de twee belangen steeds weer terugkeren op verschillende vlakken – waaronder de toegang tot de Basisregistratie Persoonsgegevens (BRP) en het UBO-register, de mogelijkheid tot gezamenlijke transactiemonitoring, het kunnen of moeten delen van relevante informatie over (gezamenlijke) klanten tussen poortwachters, de feedbackloop en gerichte informatiedeling tussen publiek-private partijen en publieke partijen onderling – is niet houdbaar. De overheid zal moeten accepteren dat het toekennen van een groter belang aan één belang een beperking met zich meebrengt aan het andere belang. Zolang die keuze niet wordt gemaakt, kunnen er geen of slechts beperkte stappen worden gezet in het bestrijden van criminaliteit.

Kortom, het is tijd om goede intenties om te zetten in concrete acties. Dit onderzoek heeft laten zien dat dat vooral kan door in te zetten op samenwerking en het gebruik van technologie. Dat kunnen poortwachters niet alleen. Dat kan de overheid niet alleen. Dat kan alleen met elkaar. Op basis van vertrouwen.

Bijlagen

Literatuur-lijst

A

A. Literatuurlijst

1. Boeken en (tijdschrift)artikelen

Alldridge 2016
P. Alldridge, *What Went Wrong With Money Laundering Law?*, Palgrave Pivot: Londen, 2016

Amicelle 2017
A. Amicelle, 'Policing through misunderstanding: insights from the configuration of financial policing', *Crime Law Soc Change* 2018, vol. 69, p. 207-226

Berkvens 2011
J.M.A. Berkvens, 'Het nieuwe Incidentenwaarschuwingssysteem financiële instellingen in het perspectief van de bestaande jurisprudentie inzake inzage en correctie', *Tijdschrift voor Financieel Recht* 2011, nr. 7/8, p. 205-214

Bökkerink en Ligthart 2014
M.J. Bökkerink en M.C. Ligthart, 'De Wwft en de sanctiewet 1977 – overeenkomsten en verschillen', *Tijdschrift voor Compliance* 2014, nr. 4, p. 212-218

Bökkerink 2022
M. Bökkerink, 'De FATF evaluatie van Nederland: een goed resultaat, maar er moet nog wel iets gedaan worden', in: *Tijdschrift voor Sanctierecht en Onderneming* 2022, nr. 6, p. 169-175

Daalderop 2019
A. Daalderop, 'Straf- en bestuursrechtelijke aansprakelijkheid van poortwachters', *Tijdschrift voor Compliance* 2019, nr. 1, p. 45-51

De Vries en Mourcous 2019
E. de Vries en L. Mourcous, 'Privacyrechtelijke aspecten voor het gebruik van een zwarte lijst', *Privacy & Informatie* 2019, aflevering 6, p. 244-251

Diepenmaat 2021
F. Diepenmaat, '(The Fight Against) Money Laundering: It's All About Networks', in: O.M. Granados en J.R. Nicolás-Carlock (eds), *Corruption Networks. Concepts and Applications*, Springer International Publishing: Cham, 2021, p. 115-130

Ferwerda en Reuter 2022
J. Ferwerda en P. Reuter, *National Assessments of Money Laundering Risks: Learning from Eight Advanced Countries' NRAs*, World Bank Publications: Washington, 2022

Gilmour en Hicks 2023
N. Gilmour en T. Hicks, *The war on dirty money*, Bristol University Press: Bristol, 2023

Groen en Van den Broek 2023
L.G. Groen en M. van den Broek, 'Ontwikkelingen in het Europese anti-witwasbeleid: het EU Single Rulebook', *Tijdschrift voor Sanctierecht & Onderneming* 2023, nr.1, p. 13-20

Hoff en Hoff 2023
R.J. Hoff en J.F. Hoff, 'Sancties in ontwikkeling en modernisering Sanctiewet', *Tijdschrift voor Sanctierecht & Onderneming* 2023, nr.1, p. 3-12

Ipenburg 2023
D. Ipenburg, 'Tussen plan en aanpak. Over het wetsvoorstel Wet plan van aanpak witwassen', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2023, nr. 1, p. 25-31

Kodrzycki en Geertsma 2019
T.J. Kodrzycki en J.G. Geertsma, 'Sanctieregelgeving en Wwft: same same, but different!', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2019, nr.4, p. 230-237

Lagerwaard 2022
P. Lagerwaard, 'Financiële surveillance en de rol van de Financial Intelligence Unit (FIU) in Nederland', *Beleid en Maatschappij* 2022, vol. 49, nr. 2, p. 128-153

Levi, Reuter en Halliday 2017
M. Levi, P. Reuter en T. Halliday, 'Can the AML system be evaluated without better data?', *Crime Law Soc Change* 2017, no. 69, p. 307-328

Nelen et al. 2023
H. Nelen, K. van Wingerde, L. Bisschop & R. Moerland, *Koers bepalen. Over de lessen van de versterking aanpak georganiseerde drugscriminaliteit,* Boomcriminologie: Den Haag, 2023

Nuijten 2023
S.M.C. Nuijten, 'Van poortwachters en witwassers: Ontwikkelingen in het toezicht op de Wwft', *Tijdschrift voor Financieel Recht* 2023, nr. 4, p. 141-148

A. Literatuurlijst

1. Boeken en (tijdschrift)artikelen

Pol 2018
R. Pol, 'Uncomfortable truths? ML=BS and AML=BS^2', *Journal of Money Laundering Control*, vol. 25, nr. 2, p. 294-307

Rainey et al. 2019
D. Rainey, S. Cooper, D. Rawlins, K. Yasuda, Tey Al-Rjula & Manreet Nijjar, 'Digital Identity for Refugees and Disenfranchised Populations The 'Invisibles' and Standards for Sovereign Identity', *International Journal of Online Dispute Resolution* 2019, vol 6, issue 1, p. 20-56

Rakké en Huisman 2020
J.T. Rakké en W. Huisman, 'Motieven voor naleving van de wettelijke anti-witwasmeldplicht', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2023, vol. 1, p. 5-11

Reuter 2013
P. Reuter, 'Are estimates of the volume of money laundering either feasible or useful', in: B. Unger en D. Van der Linde (eds), *Research handbook on money laundering*, Edward Elgar Publishing Ltd: Cheltenham, 2013, p. 224-231

Riekerk 2016
C. Riekerk, 'Integere normen voor trustkantoren', in: *Tijdschrift voor Financieel recht* 2016, nr. 11, p. 433-437

Snijder-Kuipers 2020
B. Snijder-Kuipers, 'Poortwachtersfunctie van de notaris en witwassen', *Tijdschrift voor Compliance* 2020, nr. 1, p. 35-41

Unger en Van Waarden 2013
B. Unger en F. van Waarden, 'How to dodge drowning in data? Rule- and risk-based anti-money laundering policies compared', in: B. Unger en D. Van der Linde (eds), *Research handbook on money laundering*, Edward Elgar Publishing Ltd: Cheltenham, 2013, p. 399-425

Van den Broek 2015
M. van den Broek, *Preventing money laundering: A legal study on the effectiveness of supervision in the European Union*, Eleven International Publishing: Den Haag, 2015

Van den Herik 2022
L. van den Herik, 'De toekomst van VN-sancties', *Ars Aequi* februari 2022, p. 111-117

Verhage 2017
A. Verhage, 'Great expectations but little evidence: policing money laundering', *International Journal of Sociology and Social Policy* 2017, vol. 37, nr. 7/8, p. 477-490

Yeoh 2020
P. Yeoh, 'Banks' vulnerabilities to money laundering activities', *Journal of Money Laundering Control* 2020, vol. 23, nr.1, p. 122-135

Zavoli en King 2021
I. Zavoli en C. King, 'The Challenges of Implementing Anti-Money Laundering Regulation: An Empirical Analysis', *Modern Law Review* 2021, vol. 84, nr. 4, p. 740-771

Zetzsche et al. 2018
D. Zetzsche, D.W. Arner en R. Buckley, 'Digital ID and AML/CDD/KYC utilities for financial inclusion, integrity and competition', *Capco Journal* 2018, vol. 47, p. 133-143

Zwinkels 2020
J.A. Zwinkels, 'Bestraffing van de compliance bij non-compliance trustkantoor – een reëel risico', *Tijdschrift voor Sanctierecht en Onderneming* 2020, nr. 2, p. 60-73

A. Literatuurlijst

2. Rapporten

ABS 2018
Association of Banks in Singapore, *Industry Banking KC Utility Project After-Action Report – Knowledge sharing*, 15 november 2018

Algemene Rekenkamer 2022
Algemene Rekenkamer, *Bestrijden witwassen deel 3: stand van zaken 2021*, juni 2022

Arena Consulting & Pro Facto 2022
Arena Consulting & Pro Facto, *Monitor bestuurlijke aanpak van georganiseerde criminaliteit*, 28 november 2022

ASPI 2018
Australian Strategic Policy Institute, *Preventing another Australia Card fail: Unlocking the potential of digital identity*, 16 oktober 2018

ASPI 2022
Australia Strategic Policy Institute, *The future of digital identity in Australia*, Policy Brief Report No. 66/2022, 17 november 2022

Australia Post 2021
Australia Post, *Annual Report 2021,* 2021

Autoriteit Persoonsgegevens 2019
Autoriteit Persoonsgegevens, *Aanvullend advies wetsvoorstel gegevensverwerking samenwerkingsverbanden*, 19 april 2019

Autoriteit Persoonsgegevens 2019a
Autoriteit Persoonsgegevens, *Advies over het concept voor het Implementatiebesluit registratie uiteindelijk belanghebbenden van vennootschappen en andere juridische entiteiten*, 18 juli 2019

Autoriteit Persoonsgegevens 2019b
Autoriteit Persoonsgegevens, *Advies inzake toegang tot gegevens voor poortwachters bij het voorkomen van witwassen*, 16 december 2019

Autoriteit Persoonsgegevens 2019c
Autoriteit Persoonsgegevens, *Wetgevingsadvies wetsvoorstel gegevensverwerking door samenwerkingsverbanden*, 4 januari 2019

Autoriteit Persoonsgegevens 2023
Autoriteit Persoonsgegevens, *Schriftelijke inbreng Autoriteit Persoonsgegevens Rondetafelgesprek Wetsvoorstel Plan van Aanpak Witwassen,* 24 januari 2023

BIS 2023
Bank for International Settlements Innovation Hub, *Project Aurora: The power of data, technology and collaboration to combat money laundering across institutions and borders*, mei 2023

Bureau Broekhuizen 2022
Bureau Broekhuizen, *De poortwachtersfunctie van Amsterdamse makelaars*, januari 2022

CGAP 2019
Consultative Group to Assist the Poor, *Beyond KYC Utilities: Collaborative Customer Due Diligence for Financial Inclusion*, CGAP Working Paper, augustus 2019

College van toezicht op de bedrijfsrevisoren 2023
College van toezicht op de bedrijfsrevisoren, *Sectorale WG/FT risicoanalyse 2022*, 22 februari 2023

DNB 2017
DNB, *Good Practice: Integrity Risk Appetite*, september 2017

DNB 2019
DNB, *Fiscale integriteitsrisico's voor trustkantoren*, april 2019

DNB 2019a
DNB, *General principles for the use of Artificial Intelligence in the financial sector*, juli 2019

DNB 2022
De Nederlandsche Bank, *Van herstel naar balans*, september 2022

EBA 2020
European Banking Association, *Report on big data and advanced analytics,* januari 2020

EBA 2022
EBA, *Opinion and Report on de-risking and its impact on access to financial services*, EBA/Op/2022/01, 5 januari 2022

A. Literatuurlijst

2. Rapporten

ECORYS 2018
ECORYS, *Monitor anti-witwasbeleid 2014-2016: Eindrapportage*, onderzoek in opdracht van het WODC, september 2018

EDPS 2020
European Data Protection Supervisor, *Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing*, 23 juli 2020

EDPS 2021
European Data Protection Supervisor, *Opinion 12/2021 on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals*, 22 september 2021

EDPS 2023
European Data Protection Supervisor, *EDPB letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations*, Ref: OUT2023-0017, 28 maart 2023

Europees Parlement 2019
Europees Parlement, *Understanding money laundering through real estate transactions*, februari 2019

Europese Commissie 2019
Europese Commissie, *Verslag van de Commissie aan het Europees Parlement en de Raad over de beoordeling van recente vermeende gevallen van het witwassen van geld waarbij EU-kredietinstellingen betrokken zijn*, COM(2019) 373 final, 24 juli 2019

Europese Commissie 2021
Europese Commissie, *Verslag van de Commissie aan het Europees Parlement en de Raad over de evaluatie van Verordening (EU) Nr. 910/2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (eIDAS)*, SEC(2021) 229 final - SWD(2021) 130 final, 3 juni 2021

Europese Commissie 2022
Europese Commissie, *Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities,* COM(2022) 554 final, 27 oktober 2022

Europese Commissie 2022a
Europese Commissie, *Commission staff working document on the use of public-private partnerships in the framework of preventing and fighting money laundering and terrorist financing*, SWD(2022) 347 final, 27 oktober 2022

EY 2021
EY, *Onderzoek effecten Wwft: De effecten van de Implementatiewet vierde anti-witwasrichtlijn op Wwft-instellingen,* onderzoek in opdracht van het Ministerie van Financiën, juli 2021

FATF 2016
FATF, *Mutual Evaluation Report of Italy,* februari 2016

FATF 2017
FATF, *Guidance: Private sector information sharing*, november 2017

FATF 2018
FATF, *Life insurance sector: guidance for a risk-based approach,* oktober 2018

FATF 2019
FATF, *Guidance for a risk-based approach. Trust and company service providers,* juni 2019

FATF 2019a
FATF, *Guidance for a Risk-Based Approach Guidance for Legal Professionals*, juni 2019

FATF 2020
FATF, *Digital Identity*, maart 2020

FATF 2021
FATF, *Opportunities and challenges of new technologies for AML/CFT*, juli 2021

FATF 2021a
FATF, *Stocktake on data pooling, collaborative analytics and data protection*, juli 2021

A. Literatuurlijst

2. Rapporten

FATF 2021b
FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,* oktober 2021

FATF 2022
FATF, *Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing*, juli 2022

FATF 2022a
FATF, *Risk-based Approach Guidance for the Real Estate Sector*, juli 2022

FATF 2022b
FATF, *Mutual Evaluation Report of The Netherlands*, augustus 2022

FATF 2023
FATF, *Money Laundering and Terrorist Financing in the Art and Antiquities Market*, februari 2023

FEC 2021
Financieel Expertise Centrum, *FEC Jaarverslag 2021,* 5 april 2022

FEC 2022
Financieel Expertise Centrum, *FEC Jaarverslag 2022,* 4 april 2023

FEC 2022a
Financieel Expertise Centrum, *FEC Jaarplan 2023,* 20 december 2022

FinCEN 2021
FinCEN, *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities*, 30 juni 2021

FIU 2021
FIU-Nederland, *Jaaroverzicht 2021*, juli 2022

FIU 2023
FIU-Nederland, *Position paper: FIU-Nederland t.b.v. rondetafelgesprek over het Wetsvoorstel plan van aanpak witwassen,* 26 januari 2023

German Federal Ministry of Finance 2020
German Federal Ministry of Finance, *Sicherheit: Sector-specific risk assessment 2020: Risk assessment of possible specific vulnerabilities of legal persons and other legal arrangements that could make them susceptible to being misused for ML/TF purposes*, december 2020

German Federal Ministry of Finance 2019
German Federal Ministry of Finance, *Sicherheit: First National Risk Assessment: Anti-Money Laundering/Countering the Financing of Terrorism 2018/2019*, oktober 2019

Government of Canada 2023
Government of Canada, *Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime Strategy 2023-2026*, maart 2023

Government of Canada 2023a
Government of Canada, *Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada*, maart 2023

Hoogenboom 2021
A. B. Hoogenboom, *Samen: Samenwerking van notarissen, makelaars/taxateurs en overheidsinstellingen om witwassen en fraude bij onroerend goed transacties te voorkomen*, februari 2021

ICAEW 2022
Institute of Chartered Accountants in England and Wales, *Accountancy AML Supervisors Group Risk Outlook*, april 2022

Institute of International Finance 2018
Institute of International Finance, *Machine Learning in Anti-Money Laundering – Summary Report*, oktober 2018

Irish Department of Finance 2019
Irish Department of Finance, *National Risk Assessment Ireland – Money Laundering and Anti-Terrorist Financing 2019*, april 2019

JFSC 2020
Jersey Financial Services Commission, *Exploring smart regulation: An assessment of the options for developing a shared KYC utility for the Jersey financial services sector*, juli 2020

A. Literatuurlijst

2. Rapporten

KPMG 2018
KPMG International, *Could blockchain be the foundation of a viable KYC utility?*, maart 2018

KPMG 2021
KPMG, *Slimme technieken als antwoord op de Financial Economic Crime crisis*, 5 mei 2021

KPMG 2022
KPMG, *De Glazen Leider: Hoe voorkomen we angst voor risico's in een tijd van zero tolerance*, mei 2022

KPMG 2022a
KPMG, *Financial Crime - A Paradigm Shift*, november 2022

KPMG 2023
KPMG, *Trust in Artificial Intelligence. A global study,* februari 2023

KPMG 2023a
KPMG, *Van invoering tot uitvoering. 5 jaar Algemene Verordening Gegevensbescherming (AVG) en het perspectief van de Nederlandse consument,* mei 2023

Leung et al. 2022
D. Leung, B. Nolens, D. Arner en J. Frost, *Corporate digital identity: no silver bullet, but a silver lining*, BIS Papers No 126, juni 2022

Maxwell 2021
N. Maxwell, *Innovation and discussion paper: Case studies of the use of privacy preserving analysis to tackle financial crime,* Future of Financial Intelligence Sharing (FFIS) research programme, 8 januari 2021

MEF 2019
Ministero dell'Economia e delle finanze, *Italy's national money laundering and terrorist financing risks assessment drawn up by the Financial Security Committee,* 2019

MEF 2020
Ministero dell'Economia e delle finanze, *Relazione al Parlamento sullo stato dell'azione di prevenzione del riciclaggio e del finanziamento del terrorismo, elaborata dal Comitato di sicurezza finanziaria*, 2020

Nationaal coördinator sanctienaleving en handhaving 2022
Stef Blok, *Rapport van de nationaal coördinator sanctienaleving en handhaving 2022*, 21 mei 2022

Nationale Bank van België 2020
Nationale Bank van België, *Sectorale beoordeling van de witwasrisico's in de Belgische financiële sector die onder de toezichtsbevoegdheid van de Nationale Bank van België valt*, 8 september 2020

NVB 2019
Nederlandse Vereniging van Banken, *Position paper: Betrouwbaar UBO register essentieel voor aanpak witwassen en terrorismefinanciering*, mei 2019

NVB 2022
Nederlandse Vereniging van Banken, *Position Paper: Information sharing*, juni 2022

NVB 2022a
Nederlandse Vereniging van Banken, *Ongewenste effecten van de-risking voor klanten en banken*, 26 september 2022

NVB 2023
Nederlandse Vereniging van Banken, *Position paper: Wetsvoorstel plan van aanpak witwassen: Waarom banken met deze wetswijziging het misbruik van het financiële stelsel door criminelen beter kunnen voorkomen*, 24 januari 2023

Openbaar Ministerie 2018
Openbaar Ministerie, *Onderzoek Houston: Feitenrelaas en Beoordeling Openbaar Ministerie*, 4 september 2018

Openbaar Ministerie 2021
Openbaar Ministerie, *Onderzoek Guardian: Feitenrelaas en Beoordeling Openbaar Ministerie*, 19 april 2021

Openbaar Ministerie 2022
Openbaar Ministerie, *Jaaroverzicht criminele geldstromen 2022*, 12 april 2023

A. Literatuurlijst

2. Rapporten

RIEC-LIEC 2021
RIEC-LIEC, *Jaarverslag 2021*, 7 juli 2022

RIEC Den Haag 2022
RIEC Den Haag, *Jaarverslag 2022,* 7 april 2023

Rijksuniversiteit Groningen 2023
Rijksuniversiteit Groningen, *Hoofdlijnen van de bestrijding van maffiacriminaliteit in Italië*, april 2023

RUSI 2016
RUSI, *Challenges to Information Sharing: Perceptions and Realities*, RUSI Occasional paper, 8 juli 2016

RUSI 2017
N.J. Maxwell en D. Artingstall, *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime*, RUSI Occasional Paper, oktober 2017

RUSI 2018
RUSI, *Written Evidence to Economic Crime Inquiry: Anti-money laundering supervision and sanctions implementation*, ECR0018, mei 2018

RUSI 2019
RUSI, *Deep impact? Refocusing the Anti-Money Laundering Model on Evidence and outcomes*, RUSI Occasional paper, 11 oktober 2019

RUSI 2022
RUSI, *Lessons in private-private financial information sharing to detect and disrupt crime,* Future of Financial Intelligence Sharing (FFIS), A Survey and Policy Discussion Paper, juli 2022

SEO 2021
Stichting Economisch Onderzoek, *Illegale trustdienstverlening: Een onderzoek naar de aard en omvang van de illegale trustsector in Nederland*, onderzoek in opdracht van het ministerie van Financiën, januari 2021

SEO 2022
Stichting Economisch Onderzoek, *De toekomst van de trustsector*, onderzoek in opdracht van het ministerie van Financiën, 11 oktober 2022

Stichting Maatschappij en Veiligheid 2022
Stichting Maatschappij en Veiligheid, *Poortwachters tegen witwassen: Naar een poortwachters-functie van banken die beter bijdraagt aan voorkoming en bestrijding van witwassen*, 20 juni 2022

Takáts 2007
E. Takáts, *A Theory of "Crying Wolf": The Economics of Money Laundering Enforcement*, IMF Working Paper WP/07/81, april 2007

UIF 2021
Unità di Informazione Finanziaria per l'Italia, *Annual Report 2021,* mei 2022

UK Finance 2018
UK Finance, *Written Evidence to Economic Crime Inquiry: Anti-money laundering supervision and sanctions implementation*, ECR0064, 2018

UK HM Government 2023
UK HM Government, *Economic Crime Plan 2023-2026*, maart 2023

UK HM Treasury en Home Office 2019
UK HM Treasury en Home Office, *Economic Crime Plan 2019-2022*, juli 2019

UK HM Treasury 2020
HM Treasury, *National risk assessment of money laundering and terrorist financing 2020*, 17 december 2020

UK Law Commission 2019
UK Law Commission, *Anti-money laundering: the SARs regime*, HC 2098 / Law Com No 384, 2019

UK Solicitors Regulation Authority 2021
UK Solicitors Regulation Authority, *Sectoral Risk Assessment - Anti-money laundering and terrorist financing*, 28 januari 2021

Unger et al. 2006
B. Unger, G. Rawlings, M. Busuioc, J. Ferwerda, M. Siegel, W. de Kruijf en K. Wokke, *The amounts and the effects of money laundering*, report for the Ministry of Finance, 16 februari 2006

A. Literatuurlijst

2. Rapporten

Unger et al. 2013
B. Unger, H. Addink, J. Walker, J. Ferwerda, M. van den Broek en I. Deleanu, *The Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy*, Project "ECOLEF" funded by the European Commission DG Home Affairs JLS/2009/ISEC/AG/087), februari 2013

US Department of Treasury 2022
US Department of Treasury, *National Strategy for Combating Terrorist and Other Illicit Financing*, mei 2022

US Department of Treasury 2022a
US Department of the Treasury, *National Money Laundering Risk Assessment*, februari 2022

Van Wingerde en Hofman 2022
K. van Wingerde en C. Hofman, *Wachters aan het woord: Dilemma's van accountants, advocaten, belastingadviseurs en notarissen in hun rol als poortwachter*, Politiekunde 116, 2022

Van Wingerde et al. 2023
K. van Wingerde, L. Bisschop en F. Brongers, *Onbedoeld ondermijnen: Verkennend onderzoek naar de wijze waarop de Nederlandse overheid onbedoeld de georganiseerde drugscriminaliteit kan faciliteren,* onderzoek in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC), maart 2023

Wolfsberg Group 2022
Wolfsberg Group, *Effectiveness through Collaboration*, 21 juni 2022

Wolfsberg Group 2022a
Wolfsberg Group, *Wolfsberg Principles for Using Artificial Intelligence and Machine Learning in Financial Crime Compliance*, 1 december 2022

A. Literatuurlijst

3. Media, persberichten en blogs

N. Twomey, 'KYC Utilities: The Second Coming, Learning from Past Failures', *Finextra Blog* 13 november 2017

T. Lyman en L. de Koker, 'KYC Utilities and Beyond: Solutions for an AML/CFT Paradox', *CGAP Blog Series Beyond KYC Utilities* 1 maart 2018

S. Merler, 'Latvia's money laundering scandal', *Bruegel Blog post* 9 april 2018

Openbaar Ministerie, 'Trustkantoor Vistra betaalt 3,5 ton voor niet melden ongebruikelijke transacties', nieuwsbericht 3 september 2019

R. Vaessen, 'Even een rekening openen', *Accountant.nl* 6 september 2019

Isabel Group, '4 grootbanken en Isabel Group bundelen krachten voor vereenvoudiging zakelijke dienstverlening met KUBE', persbericht 22 januari 2020

P. Ooms, 'KUBE: Blockchain voor banken', *FDmagazine.be* 22 januari 2020

Invidem, 'Invidem partners with Encompass and iMeta Technologies to make KYC data handling easier', persbericht 6 april 2020

Cetif Advisory, 'O-KYC, al via il progetto di Cetif Advisory', persbericht 22 juli 2020

S. Wass, 'Nordic banks' agreement on one KYC standard a 'unique advantage' for new utility', *S&P Global market intelligence* 20 augustus 2020

NVB, 'Nieuwe publiek-private samenwerking in Fintell Alliance - "Nieuwe boost voor aanpak witwassen"', nieuwsbericht 11 februari 2021

Cetif Advisory, 'Cetif - UniCatt insieme ad Intesa (Gruppo IBM) e CherryChain nel progetto Onboarding e Know Your Customer (O-KYC) su tecnologia DLT/Blockchain', persbericht 18 februari 2021

Australia Post, 'AusPost's Digital iD linked with DocuSign for e-signatures', persbericht 24 maart 2021

M. Ciobanu, 'Interview Advancing modern financial crime prevention with KYC utilities – interview with Invidem', *ThePaypers* 25 juni 2021

FinCEN, 'FinCEN Issues First National AML/CFT Priorities and Accompanying Statements', persbericht 30 juni 2021

R. Betlem, 'Rabobank sluit kleine autodealers uit vanwege risico op witwassen', *FD* 1 juli 2021

H.W. Smits en H. Rasch, 'Anti-witwasbeleid kost miljarden en levert weinig op', *FTM* 8 juli 2021

Europese Commissie, 'Anti-money laundering and countering the financing of terrorism legislative package', persbericht 20 juli 2021

E. Pastars, 'From zero to hero – a brief overview of AML evolution in Latvia', *Cobalt* 10 september 2021

FD Redactioneel Commentaar, 'Banken voeren eenzame oorlog tegen witwassen', *FD* 25 oktober 2021

Politie, 'Serious Crime Taskforce leidt tot structurele samenwerking', persbericht 25 oktober 2021

FIU-Nederland, 'FIU-Nederland treedt samen met grootbanken op tegen witwassen en terrorismefinanciering', nieuwsbericht 2 november 2021

Autoriteit Persoonsgegevens, 'AP adviseert Eerste Kamer: neem WGS niet aan', persbericht 9 november 2021

Rabobank, 'Rabobank heeft voorgenomen aanwijzing ontvangen van DNB', persbericht 16 november 2021

Invidem, 'Invidem enters into an agreement with the first non-owner client', persbericht 19 april 2022

'Kosten voor bankrekening blijven stijgen, ABN AMRO gooit er in een keer 51,3 procent bovenop', *Volkskrant* 3 mei 2022

A. Literatuurlijst

3. Media, persberichten en blogs

HM Revenue & Customs en HM Treasury, 'Tax crime chiefs summit commits to international action', persbericht 13 mei 2022

CanDeal, 'Canadian Banks Partner with CanDeal to Deliver Industry-wide KYC Solution', persbericht 27 juni 2022

G. Stack, 'Latvian Prosecutors Charge Bankers with Laundering 2.1B Euro', *OCCRP* 29 juli 2022

'ING te druk met witwasonderzoek, weert stichtingen en verenigingen', *NOS.nl* 29 augustus 2022

R. Betlem, 'Zakelijke rekeningen duurder door stijgende kosten witwasonderzoek', *FD* 30 augustus 2022

Intesa, 'Progetto O-KYC, inizia la fase due', persbericht 5 oktober 2022

DNB, 'MiCAR belangrijke stap in regulering van crypto-markten', nieuwsbericht 6 oktober 2022

Autoriteit Persoonsgegevens, 'Nieuwe wet opent deur naar ongekende massasurveillance door banken', persbericht 21 oktober 2022

A. Ploumen, KNB: 'Onderlinge gegevensdeling tegen witwassen nodig en gewenst', *MrOnline* 7 november 2022

'Banken weigeren goede doelen om 'witwasrisico'', *RTL Nieuws* 15 november 2022

DNB, 'Partijen voortvarend van start met gerichte risicogebaseerde witwasaanpak', nieuwsbericht 23 november 2022

N. Boere, 'Online gokken als witwasmethodiek', nieuwsbericht AMLC 28 november 2022

Ministerie van Buitenlandse Zaken | Expertisecentrum Europees recht, 'EU-regeling voor onbeperkte toegang van het publiek tot informatie over de uiteindelijk begunstigden van vennootschappen is ongeldig', nieuwsbericht 2 december 2022

'Bedrijven, stichtingen en kerken moeten van banken meebetalen aan witwasonderzoek', *NOS.nl* 27 december 2022

R. Betlem en M. Rotteveel, 'Machine tegen witwassen werkt niet', *FD* 10 januari 2023
A. Clare, 'Sanctions screening regtech GSS secures $45mn in funding', *Fintech Magazine* 23 januari 2023

Verbond van Verzekeraars, 'Meer duidelijkheid toegang UBO-register', nieuwsbericht 24 januari 2023

C. de Horde, R. Betlem, 'Felle verdeeldheid onder voor- en tegenstanders van nieuwe witwaswet', *FD* 26 januari 2023

Europese Commissie, 'De architectuur en het referentiekader voor de Europese portemonnee voor digitale identiteit', nieuwsbericht 10 februari 2023

'Nederland kent strengste trustwetgeving in EU', *Holland Quaestor* 27 februari 2023

Rijksoverheid, 'Eerste Kamer neemt Wet digitale overheid aan', nieuwsbericht 21 maart 2023

G. de Groot, J. Leupen en S. Motké, 'Russische klanten gaan ondergronds na Nederlands trustverbod', *FD* 24 maart 2023

S. Motké, G. de Groot en J. Leupen, 'Hoe een 'zwart gat' in Amsterdam zich vult met Russen', *FD* 24 maart 2023

FD Redactioneel Commentaar, 'Nederland heeft blinde vlek in trusttoezicht', *FD* 28 maart 2023

College voor de Rechten van de Mens, 'Verzoek geweigerd – Mogen banken klanten afwijzen op grond van nationaliteit?', nieuwsbericht 4 april 2023

K. van Doorne, 'Met knikkende knieën ongebruikelijke transacties melden? Dat kan toch niet', column *VNO-NCW*, 5 april 2023

NVB, 'Openheid en transparantie in uitvoering anti-witwaswet', nieuwsbericht 6 april 2023

A. Literatuurlijst

3. Media, persberichten en blogs

'Racismecoördinator: 'Structurele discriminatie van moslims bij banken', *NOS.nl* 6 april 2023

M. Pols, E. van der Schoot, 'OM-topman: 'Ik mis de verontwaardiging over criminaliteit die het bedrijfsleven ondermijnt'', *FD* 21 april 2023

Raad van de EU, 'Digitaal geld: Raad neemt nieuwe regels aan over markten in cryptoactiva (MiCA)', persbericht 16 mei 2023

Raad van de EU, 'Witwassen: Raad neemt regels aan die overmakingen van cryptoactiva traceerbaar maken', persbericht 16 mei 2023

NVB, 'Minder klantimpact door NVB Standaarden voor risicogebaseerd witwasonderzoek', persbericht 30 mei 2023

'Onderzoek: Italiaanse maffia-aanpak deels bruikbaar voor Nederland', *NOS.nl* 7 juni 2023

I. Withers en K. Ridley, 'BREAKING: Six British banks to share fincrime information in a 'game changer' plan to crack down on money laundering; Lloyds, NatWest already involved in trials', *AMLIntelligence* 22 juni 2023

Raad van de EU, 'Russia's war of aggression against Ukraine: EU adopts 11th package of economic and individual sanctions', persbericht 23 juni 2023

A. Literatuurlijst

4. Kamerstukken

Kamerstukken I, 2022/2023, 31 477 en 34 08, D[1] (de letter D heeft alleen betrekking op 31 477)

Kamerstukken I, 2022/2023, 35 447, K

Kamerstukken II, 2007/2008, 31 237 en 31 238, nr. 6

Kamerstukken II, 2007/2008, 31 238, nr. 3

Kamerstukken II, 2017/2018, 29 911, nr. 180

Kamerstukken II, 2017/2018, 34 808, nr. 3

Kamerstukken II, 2017/2018, 34 910, nr. 3

Kamerstukken II, 2018/2019, 31 477, nr. 41, bijlage plan van aanpak witwassen

Kamerstukken II, 2020/2021, 31 477, nr. 60, bijlage

Kamerstukken II, 2021/2022, 29 911, nr. 348

Kamerstukken II, 2021/2022, 36 085, nr. 2

Kamerstukken II, 2021/2022, 36 102, nr. 3

Kamerstukken II, 2022/2023, 31 477, nr. 80

Kamerstukken II, 2022/2023, 32 545, nr. 180

Kamerstukken II, 2022/2023, 36 200 V, nr. 56

Kamerstukken II, 2022/2023, 36 045, nr. 120

Kamerstukken II, 2022/2023, 36 228, nr. 2.

Kamerstukken II, 2022/2023, 36 228, nr. 3

Kamerstukken II, 2022/2023, Aanhangsel van de Handelingen, 2595

A. Literatuurlijst

5. Handhavingsbesluiten toezichthouders

AFM, *Aanwijzing STX Fixed Income B.V.*, 8 juni 2021, beschikbaar via deze link

AFM, *Bestuurlijke boete FlatexDeGiro*, 23 december 2021, beschikbaar via deze link

AFM, *Aanwijzing Zwaan Finance B.V.*, 25 maart 2022, beschikbaar via deze link

AFM, *Bestuurlijke boete Robeco Institutional Asset Management B.V.*, 31 maart 2022, beschikbaar via deze link

AFM, *Bestuurlijke boetes Revo Capital Management B.V.*, 25 mei 2022, beschikbaar via deze link

Autoriteit Persoonsgegevens, *Boete TikTok vanwege schenden privacy kinderen*, 21 juli 2021, beschikbaar via deze link

Autoriteit Persoonsgegevens, *Boete Belastingdienst voor discriminerende en onrechtmatige werkwijze*, 7 december 2021, beschikbaar via deze link

DNB, *Bestuurlijke boete Suri-Change B.V.*, 25 november 2014, beschikbaar via deze link

DNB, *Aanwijzing MUFG Bank (Europe) N.V.*, 29 juli 2019, beschikbaar via deze link

DNB, *Bestuurlijke boete JTC Institutional Services Netherlands B.V.*, 14 juni 2021, beschikbaar via deze link

DNB, *Bestuurlijke boete Travelex N.V.*, 2 februari 2023, beschikbaar via deze link

A. Literatuurlijst

6. Rechtspraak

Hof van Justitie EU, 22 november 2022, C-37/20 en C-601/20, ECLI:EU:C:2022:912 (*WM v Luxembourg Business Registers* en *Sovim v Luxembourg Business Registers*)

CBb, 3 maart 2020, ECLI:NL:CBB:2020:120

CBb, 18 oktober 2022, ECLI:NL:CBB:2022:707 (Bunq)

Gerechtshof Den Haag 1 februari 2019, ECLI:NL:GHDHA:2019:187

Gerechtshof Amsterdam, 21 januari 2020, ECLI:NL:GHAMS:2020:121

Rb. Amsterdam, 1 december 2020, ECLI:NL:RBAMS:2020:6245

Rb. Amsterdam 22 april 2021, ECLI:NL:RBAMS:2021:2600

Rb. Amsterdam, 5 januari 2022, ECLI:NL:RBAMS:2022:42

Rb. Amsterdam, 15 juni 2022, ECLI:NL:RBAMS:2022:3871

Rb. Amsterdam, 14 september 2022, ECLI:NL:RBAMS:2022:5340

Kamer voor het notariaat Amsterdam 10 maart 2022, ECLI:NL:TNORAMS:2022:8

Kamer voor het notariaat Den Haag 25 mei 2022, ECLI:NL:TNORDHA:2022:10

Kamer voor het notariaat Den Haag 15 juli 2022, ECLI:NL:TNORDHA:2022:14

Kamer voor het notariaat Den Bosch 19 september 2022, ECLI:NL:TNORSHE:2022:31

A. Literatuurlijst

7. Geraadpleegde websites

AMLC, *Strafrechtelijke aanpak via de Wwft*, beschikbaar via deze link

AMLC, *Wat wil het AMLC bereiken*, beschikbaar via deze link

AMLC, *Wie zijn wij en wat doen wij*, beschikbaar via deze link

AUSTRAC, *Reliable and independent documentation and electronic data*, beschikbaar via deze link

Australia Post, *AML solutions: Digital iD AML/KYC offering*, beschikbaar via deze link

Australia Post, *Digital ID*, beschikbaar via deze link

Banca d'Italia, *Regulatory sandbox: admitted projects*, beschikbaar via deze link

Currence, *Collectieve betaalproducten: IDIN*, beschikbaar via deze link

DNB, *Q&A Elektronische identificatiemiddelen en cliëntidentificatie*, beschikbaar via deze link

DNB, *Sanctiescreening*, 16 september 2022, beschikbaar via deze link

Eerste Kamer, *Initiatiefvoorstel-Nijboer en Alkaya Wet centraal aandeelhoudersregister*, beschikbaar via deze link

Europees Parlement, *Artificiële intelligentie: Kansen en gevaren*, beschikbaar via deze link

Europese Commissie, *De prioriteiten van de Europese Commissie*, beschikbaar via deze link

Europese Commissie, *Een digitale identiteit voor alle Europeanen*, beschikbaar via deze link

Europese Commissie, *Europese digitale identiteit*, beschikbaar via deze link

Europol, *European Financial and Economic Crime Centre – EFECC*, beschikbaar via deze link

FIU-Nederland, *Ik heb een melding gedaan: wat nu?*, beschikbaar via deze link

FIU-Nederland, *Nationale samenwerking,* beschikbaar via deze link

iDIN, *iDIN – Een veilig iD*, beschikbaar via deze link

i-Hub, *About i-Hub*, beschikbaar via deze link

Monetary Authority of Singapore, *Digital ID and e-KYC*, beschikbaar via deze link

National Crime Agency, *National Economic Crime Centre*, beschikbaar via deze link

NVB, *IVR/EVR-registratie*, beschikbaar via deze link

Rijksinspectie Digitale Infrastructuur, *Elektronische vertrouwensdiensten*, beschikbaar via deze link

Rijksoverheid, *Digitale Overheid*, beschikbaar via deze link

Singpass, *MyInfo: speed up eKYC processes for individual users with data from government sources*, beschikbaar via deze link

Singpass, *Singpass API Products*, beschikbaar via deze link

Singpass, *Transforming Singapore through technology*, beschikbaar via deze link

TMNL, *Ethische commissie*, beschikbaar via deze link

TMNL, *Over TMNL*, beschikbaar via deze link

TMNL, *TMNL in het kort: Samen financiële criminaliteit bestrijden*, beschikbaar via deze link.

A. Literatuurlijst

8. Overig

Autoriteit Persoonsgegevens, *Besluit inzake de vergunningaanvraag voor de verwerking van [PARTIJ] volgens het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen 2021*, 20 augustus 2021, kenmerk z2021-03355, beschikbaar via deze link

Belastingdienst Bureau Toezicht Wwft, *Leidraad Wwft voor makelaars, bemiddelaars en taxateurs onroerende zaken*, maart 2022, beschikbaar via deze link

Coalitieakkoord 2021-2025*, Omzien naar elkaar, vooruitkijken naar de toekomst*, 15 december 2021, beschikbaar via deze link

Consultatie voor de Wijzigingswet financiële markten 2024, 29 april 2022, beschikbaar via deze link

Consultatie voor het Besluit gegevensverwerking door samenwerkingsverbanden, 20 februari 2023, beschikbaar via deze link

Consultatie voor de Wijzigingswet beperking toegang UBO-registers, 30 mei 2023, beschikbaar via deze link

DNB, *Leidraad Wwft/Sw,* september 2022, beschikbaar via deze link

European Banking Authority, *Richtsnoeren inzake de rol en verantwoordelijkheden van de compliance officer op het gebied van AML/CFT*, EBA/GL/2022/05, 14 juni 2022, beschikbaar via deze link

European Banking Authority, *Richtsnoeren voor onboarding klanten op afstand*, EBA/GL/2022/15, 22 november 2022, beschikbaar via deze link

Goede Doelen Nederland, *Tweede brandbrief aan Kaag over gevolgen de-risking banken*, 21 april 2022, beschikbaar via deze link

Ministerie van Financiën, *Leidraad Financiële Sanctieregelgeving*, 12 augustus 2020, beschikbaar via deze link

Monetary Authority of Singapore, *Circular AMLD 01/2018: Use of MyInfo and CDD Measures for Non Face-to-Face Business Relations*, 8 januari 2018, beschikbaar via deze link

Monetary Authority of Singapore, *Circular ID 26/20: Outsourcing arrangements involving services wholly provided by the Government Technology Agency ("GovTech") or agents appointed by GovTech*, 9 juni 2020, beschikbaar via deze link

Protocol Incidentenwaarschuwingssysteem Financiële Instellingen 2021 (PIFI 2021), beschikbaar via deze link

Reactie van NVM, VBO en VastgoedPro op het wetsvoorstel Wet plan van aanpak witwassen, 2020, beschikbaar via deze link

Wetenschapstoets wetsvoorstel Plan van Aanpak Witwassen, 20 januari 2023, beschikbaar via deze link.

Initiatieven in binnen- en buitenland

B

B. Initiatieven in binnen- en buitenland

1. Informatiedeling tussen poortwachters

1.1. Transactie Monitoring Nederland (TMNL)

Transactie Monitoring Nederland (hierna: 'TMNL') is op 10 juli 2020 opgericht door ABN AMRO Bank, ING Bank, Rabobank, Triodos Bank en de Volksbank.(407) TMNL is opgericht als besloten vennootschap waarin de deelnemende banken aandeelhouder zijn.(408) Het is een voorziening gericht op gemeenschappelijke transactiemonitoring. Momenteel betreft dit uitsluitend de deelnemende banken, maar op termijn is het de bedoeling dat ook andere financiële instellingen kunnen worden bediend door TMNL.(409)

In TMNL brengen de deelnemende banken hun transactiegegevens van zakelijke klanten samen met als doel om ongebruikelijke patronen in het betalingsverkeer te signaleren die niet blootgelegd worden wanneer de transacties individueel door de banken gemonitord worden. Door middel van deze aanpak kunnen netwerken geïdentificeerd worden waarin (mogelijke) witwaspraktijken plaatsvinden en passende maatregelen genomen worden.(410) Met de mogelijkheid om verbanden te kunnen leggen en transactiepatronen in gezamenlijkheid te monitoren, *"kunnen criminelen minder makkelijk gebruik maken van de 'dark space' tussen banken"*.(411)

TMNL bevindt zich in een *minimum viable product*-fase en opereert binnen de huidige juridische grenzen.(412) Om een volgende stap te kunnen maken moet de Wwft op een aantal punten worden aangepast, in het bijzonder door een wettelijke basis voor gezamenlijke transactiemonitoring te creëren.(413) In paragrafen 3.2.1 en 3.2.5 van het onderzoeksrapport is al ingegaan op het wetsvoorstel Wet plan van aanpak witwassen, dat voor deze juridische grondslag moet gaan zorgen.

In de huidige fase worden alle analyseactiviteiten van TMNL verricht in aanvulling op de eigen monitoring activiteiten door banken. TMNL beperkt zich tot transacties waarbij (bankrekeningen van) meerdere banken betrokken zijn en richt zich uitsluitend op de detectie van ongebruikelijke transactiepatronen. TMNL maakt daarbij gebruik van geavanceerde analytische modellen. Wanneer ongebruikelijke patronen worden geïdentificeerd, worden deze als alerts individueel teruggekoppeld naar de betrokken banken. De afhandeling van alerts en eventuele vervolgmaatregelen zoals het melden van een ongebruikelijke transactie wordt verricht door de deelnemende banken zelf.(414)

Met het oog op de bescherming van privacy is ervoor gekozen TMNL enkel transacties van zakelijke klanten te laten monitoren. TMNL ontvangt alleen de strikt noodzakelijke informatie (dataminimalisatie). De transactie- en klantgegevens die TMNL ontvangt worden gepseudonimiseerd door de banken aangeleverd.(415) Dit houdt in dat herleidbare informatie zoals bedrijfsnaam en rekeningnummer wordt omgezet naar een onherleidbare reeks tekens. Ook het verantwoord en ethisch gebruik van de modellen krijgt aandacht binnen TMNL. De organisatie heeft een ethische commissie, bestaande uit academici, die TMNL op objectieve wijze adviseren over ethische vraagstukken bij het gebruik van modellen.(416)

TMNL is een privaat initiatief, maar werkt samen met onder meer FIU-NL en het AMLC.(417) De samenwerking ziet op het opstellen van risico-indicatoren voor witwassen en terrorismefinanciering en het delen van kennis over modus operandi van criminelen. Deze informatie wordt verwerkt in de detectiemodellen van TMNL.(418)

(407) TMNL, *Over TMNL*, beschikbaar via deze link.
(408) FATF 2022, p. 27.
(409) TMNL, *TMNL in het kort: Samen financiële criminaliteit bestrijden*, beschikbaar via deze link.
(410) NVB 2023; Diepenmaat 2021, p. 126.
(411) NVB 2023, p. 5.
(412) FATF 2022, p. 26-27.
(413) Wetsvoorstel Wet plan van aanpak witwassen, Kamerstukken II, 2022/2023, 36 228, nr. 2.
(414) FATF 2022, p. 26-27.
(415) FATF 2022, p. 26-27.
(416) TMNL, *Ethische commissie*, beschikbaar via deze link.
(417) TMNL, *TMNL in het kort: Samen financiële criminaliteit bestrijden*, beschikbaar via deze link; FIU 2023, p. 1-2.
(418) FIU 2023, p. 2.

B. Initiatieven in binnen- en buitenland

Ook hebben TMNL en FIU-Nederland in 2021 samen binnen Fintell Alliance een pilot gedaan. Op basis hiervan heeft FIU-NL geconcludeerd dat gezamenlijke transactiemonitoring onder meer leidt tot betere en completere meldingen van ongebruikelijke transacties bij FIU-NL en dat shopgedrag van (malafide) klanten beter kan worden voorkomen.(419) Ook leiden signalen over modus operandi die FIU-NL deelt en worden opgenomen in de modellen van TMNL sneller tot resultaten dan wanneer individuele banken deze modus operandi en risico-indicatoren moeten verwerken in hun modellen.(420)

1.2. Know Your Customer Utility for Banks and Enterprises (KUBE)

KUBE staat voor 'Know Your Customer Utility for Banks and Enterprises' en is een initiatief van de vier Belgische grootbanken Belfius, BNP Paribas Fortis, ING België en KBC samen met fintechbedrijf Isabel Group.(421) Het initiatief is gestart in januari 2020. Er zijn sinds de start van het initiatief geen nieuwe partijen bij KUBE aangesloten.

KUBE richt zich op het versimpelen van het KYC-proces van gedeelde zakelijke klanten van de banken bij het aangaan van de zakelijke relatie en de voortdurende controle. Een van de doelstellingen is het zorgen voor een efficiënter proces: met toestemming van de klant kunnen gegevens van de organisatie die aan één bank zijn verstrekt in het kader van een cliëntenonderzoek vervolgens ook met andere aangesloten banken gedeeld worden: *"[w]anneer een onderneming een rekening opent bij een andere bank, zal die sneller het KYC-proces doorlopen aangezien de vereiste gegevens al beschikbaar zijn. Hierdoor zal de onderneming rekeningen kunnen openen zonder administratieve rompslomp en vertragingen"*.(422) Hierbij delen betrokken partijen via blockchain gegevens over klanten met elkaar. Dit betekent dat de data niet in een centrale database opgeslagen wordt. De KUBE-blockchaintoepassing wordt door Isabel Group geëxploiteerd.

In de praktijk werkt KUBE als volgt: een zakelijke klant verstrekt de gevraagde KYC-gegevens aan de bank waar de organisatie diensten wil afnemen via de KUBE-toepassing. De gegevens worden door de betreffende bank geverifieerd volgens de tussen de banken afgesproken verificatieregels. Wanneer de zakelijke klant daar toestemming voor geeft, worden de KYC-gegevens en de verificatiestatus van elk afzonderlijk informatiepunt op KUBE geplaatst. Wanneer andere banken een zakelijke relatie met deze zakelijke klant aangaan, kunnen zij de betreffende KYC-gegevens en verificatiestatus ophalen en gebruiken voor hun eigen KYC-onderzoek. De bank die de KYC-gegevens van de zakelijke klant als eerste heeft geverifieerd krijgt van de andere banken die gebruikmaken van de gegevens een compensatie.(423) Alle deelnemers betalen abonnementskosten voor het gebruik van KUBE aan Isabel Group.

Op de website wordt aangegeven dat KUBE volledig AVG-compliant is, vanwege het ontwerpprincipe 'privacy-by-design' en het gebruik van blockchaintechnologie waarbij de data van de zakelijke klant niet in een centrale database wordt opgenomen. Belangrijk is dat toestemming van de klant wordt gevraagd om informatie te delen.(424)

1.3. Invidem Nordic KYC-utility

Invidem AB is in 2019 door zes Scandinavische banken opgericht. Deelnemende banken zijn Danske Bank, DNB, Handelsbanken, Nordea, SEB en Swedbank. De banken zijn gezamenlijk eigenaar van het bedrijf zonder winstoogmerk. In september 2021 werd het KYC-platform van Invidem gelanceerd. In april 2022 breidde Invidem voor het eerst uit met een Zweedse beheerder van een beleggingstelling.(425)

(419) FIU 2023, p. 2.
(420) FIU 2023, p. 2.
(421) Isabel Group, '4 grootbanken en Isabel Group bundelen krachten voor vereenvoudiging zakelijke dienstverlening met KUBE', persbericht 22 januari 2020.
(422) P. Ooms, 'KUBE: Blockchain voor banken', *FDmagazine.be* 22 januari 2020.
(423) Informatie door KPMG verzameld, vertaald en samengevat vanaf de website https://www.kube-kyc.be/en/.
(424) Informatie door KPMG verzameld, vertaald en samengevat vanaf de website https://www.kube-kyc.be/en/.
(425) Invidem, 'Invidem enters into an agreement with the first non-owner client', persbericht 19 april 2022.

B. Initiatieven in binnen- en buitenland

Echter, in april 2023 werd via de website aangekondigd dat Invidem stopt.

De Nordic KYC-utility van Invidem betreft een platform voor zakelijke klanten aan de hand van een door banken vooraf overeengekomen en geharmoniseerde datastandaard. Via het platform worden KYC-gegevens over zakelijke klanten verzameld, geverifieerd en wordt algemene data gevalideerd. Daarmee heeft Invidem zichzelf ook wel een 'clearing house voor KYC-information' genoemd.(426)

De data van de zakelijke klant is opgeslagen op een gecentraliseerde locatie en de klant kan bepalen welke partij tot welke informatie toegang krijgt.(427) De KYC-utiliteit kan worden gebruikt bij het aangaan van een zakelijke relatie en gedurende de relatie.

Voordat het einde van Invidem werd aangekondigd, werden de gemeenschappelijke KYC-datastandaard en de sterke betrokkenheid van de oprichtende banken aangemerkt als belangrijke succesfactoren.(428) In een interview uit 2021 gaf de CEO van Invidem aan dat klanten verschillende voordelen zouden hebben bij het gebruik van de voorziening. Deze betroffen onder meer het niet herhaaldelijk hoeven aanleveren van klantinformatie (mede door de geharmoniseerde datastandaard), betere controle over de eigen KYC-data en het actueel houden van deze data en snellere toegang tot financiële dienstverlening. Voor deelnemende partijen zouden voordelen gelegen zijn in onder meer tijdreductie bij het verrichten van cliëntenonderzoeken (mede door de automatische dataverzameling), het kunnen steunen op de aangeleverde data, en actuele klantdossiers.(429) Bij de aankondiging van het einde van Invidem op de website wordt opgemerkt dat de snelle ontwikkeling van wet- en regelgeving alsook de ontwikkelingen op technologisch gebied hebben geleid tot een hogere complexiteit dan oorspronkelijk beoogd. Ook maakte dit het behalen van de gewenste schaalvoordelen voor zowel klanten als banken lastiger.(430)

1.4. O-KYC

In Italië loopt sinds juni 2020 een project genaamd 'O-KYC'. Na een eerste testfase die afliep in februari 2021 is het project toegelaten tot de regulatory sandbox van de Italiaanse Centrale Bank voor een proeftijd van 18 maanden.(431) Een regulatory sandbox is een gecontroleerde testomgeving waarin innovatieve producten en diensten ontwikkeld en gevalideerd kunnen worden. Vaak zijn de producten en diensten niet (helemaal) toegestaan onder het huidige wettelijke kader, maar omdat de diensten en producten niet aan klanten worden aangeboden, kan tijdelijk worden afgeweken van het wettelijke kader.

Deelnemers aan het O-KYC project zijn Cetif Advisory(432), CherryChain (fintech) en Intesa (IBM Groep), en zes Italiaanse banken: Banca IFIS, Banca Mediolanum, Banca Popolare di Puglia e Basilicata, Cherry Bank, Iccrea Banca en Banca Monte dei Paschi di Siena. Tevens is een advocatenkantoor betrokken om de juridische aspecten van het project te begeleiden.(433)

Het project richt zich op de onboardingfase van het KYC-proces en heeft als belangrijkste doel het vereenvoudigen van het onboardingproces om zo de tijd en kosten te verlagen en de interne processen van poortwachters efficiënter te maken.(434) Ook heeft dit impact op de klantervaring: klanten hoeven niet herhaaldelijk dezelfde of soortgelijke gegevens aan te dragen aan verschillende poortwachters.

(426) S. Wass, 'Nordic banks' agreement on one KYC standard a 'unique advantage' for new utility', *S&P Global market intelligence* 20 augustus 2020.
(427) Invidem, 'Invidem partners with Encompass and iMeta Technologies to make YC data handling easier', persbericht 6 april 2020.
(428) M. Ciobanu, 'Interview Advancing modern financial crime prevention with KYC utilities – interview with Invidem', *ThePaypers* 25 juni 2021.
(429) M. Ciobanu, 'Interview Advancing modern financial crime prevention with KYC utilities – interview with Invidem', *ThePaypers* 25 juni 2021.
(430) www.invidem.com.
(431) Banca d'Italia, *Regulatory sandbox: admitted projects*, beschikbaar via deze link.
(432) Cetif Advisory is een spin-off van Cetif, het onderzoekscentrum van de Università Cattolica del Sacro Cuore.
(433) Cetif Advisory, 'Cetif - UniCatt insieme ad Intesa (Gruppo IBM) e CherryChain nel progetto Onboarding e Know Your Customer (O-KYC) su tecnologia DLT/Blockchain', persbericht 18 februari 2021.
(434) Cetif Advisory, 'O-KYC, al via il progetto di Cetif Advisory', persbericht 22 juli 2020.

B. Initiatieven in binnen- en buitenland

Openbare bronnen maken niet duidelijk of het project zich richt op zakelijke klanten, natuurlijke personen of beide; hoewel de werking via een app impliceert dat het in ieder geval natuurlijke personen betreft. In de praktijk wordt toegewerkt naar het creëren van een 'KYC-portemonnee' van klanten door een van de deelnemers (de 'bewaarder''). Met toestemming van die klant kan de informatie opgenomen in de portemonnee worden gedeeld met andere deelnemers die de informatie opvragen ('de aanvragers'). Distributed Ledger Technologie (DLT) en blockchaintechnologie spelen een belangrijke rol bij het systeem dat wordt opgezet voor de uitwisseling van de gegevens. Binnen het project wordt ook gekeken naar een mogelijke vergoeding voor de bewaarder in de vorm van 'tokens' die binnen het systeem kunnen worden besteed.(435)

Volgens de betrokken partijen is het O-KYC-systeem in lijn met AVG-vereisten. Daarbij worden in het bijzonder de controle van de eindgebruiker (klant) over diens eigen gegevens en de beveiliging van het interne proces genoemd.(436)

1.5. i-Hub KYC Repository for Ongoing Due Diligence

In december 2019 is de KYC Repository for Ongoing Due Diligence uitgerold in Luxemburg. Dit commerciële platform wordt beheerd door i-Hub. i-Hub is een dochteronderneming van Post Luxemburg (een staatsbedrijf) en BGL BNP Paribas.(437) Het heeft een vergunning als ondersteunende financiële instelling ('support PFS') en valt onder het toezicht van de Luxemburgse financieel toezichthouder Commission du Surveillance du Secteur Financier (CSSF).(438) Strikt genomen is de i-Hub KYC Repository geen gezamenlijke KYC-utiliteit; via het gebruik van de KYC Repository for Ongoing Due Diligence besteden aangesloten poortwachters in feite hun cliëntenonderzoek uit aan i-Hub. Het platform is vooralsnog voornamelijk gericht op banken, (beheerders van) beleggingsinstellingen en beleggingsondernemingen.

De KYC Repository betreft een gecentraliseerd platform waarin gegevens van klanten – natuurlijke personen of rechtspersonen – en gerelateerde partijen opgeslagen worden. i-Hub heeft een gestandaardiseerd datamodel en doet namens de aangesloten poortwachters de validatie van gegevens die van de klant zijn ontvangen en van informatie afkomstig uit publieke registers (bijvoorbeeld het Handelsregister en UBO-register). Updates van deze publieke registers worden automatisch opgenomen in de tool en verwerkt in de klantprofielen. Via het platform kan ook PEP- en sanctiescreening worden verricht, inclusief de afhandeling van alerts. Met de tool kan ook de risicoweging en -beoordeling van de klant worden gedaan. Via 'service level agreements' wordt het platform voor elke aangesloten poortwachter afgestemd op individuele behoeften. Transactiemonitoring valt buiten de reikwijdte van het platform.(439)

Informatiedeling tussen aangesloten poortwachters is mogelijk en is gebaseerd op toestemming van de klant, oftewel de eindgebruiker ('opt-in'). Bij updates van klantinformatie ontvangen alle zakelijke relaties van de eindgebruiker deze updates via het platform.(440)

(435) Cetif Advisory, 'O-KYC, al via il progetto di Cetif Advisory', persbericht 22 juli 2020.
(436) Cetif Advisory, 'Cetif - UniCatt insieme ad Intesa (Gruppo IBM) e CherryChain nel progetto Onboarding e Know Your Customer (O-KYC) su tecnologia DLT/Blockchain', persbericht 18 februari 2021.
(437) i-Hub, *About i-Hub*, beschikbaar via deze link.
(438) Een kenmerk van de ondersteunende financiële instelling is dat deze niet zelf een financiële dienst of activiteit verricht, maar bepaalde operationele functies namens andere financiële instellingen en dienstverleners verricht.
(439) Informatie door KPMG verzameld, vertaald en samengevat vanaf de website https://www.i-hub.com/b2b/.
(440) Informatie door KPMG verzameld, vertaald en samengevat vanaf de website https://www.i-hub.com/b2b/.

B. Initiatieven in binnen- en buitenland

1.6. Wetgeving voor KYC-utiliteiten in Letland

In 2022 is in Letland wetgeving geïntroduceerd gericht op de opzet en het gebruik van KYC-utiliteiten.(441) Deze wetgeving is onderdeel van het Letse Actieplan ter voorkoming van witwassen en terrorismefinanciering 2020-2022.(442) Dit actieplan werd ontwikkeld naar aanleiding van een negatieve evaluatie van het Letse anti-witwasbeleid door MONEYVAL, waarna het land onder verscherpte internationale monitoring kwam te staan. Rond dezelfde tijd speelde ook de problematiek bij ABLV Bank, een van de grootste banken van Letland.(443) ABLV werd door Amerikaanse autoriteiten verdacht van witwassen en het helpen van klanten om sancties opgelegd aan Noord-Korea te ontwijken. In de zomer van 2022 kondigden Letse autoriteiten aan het hoger leidinggevend personeel van de inmiddels geliquideerde bank te vervolgen.(444)

De nieuwe wetgeving in Letland staat toe dat poortwachters gebruikmaken van KYC-utiliteiten om hun cliëntenonderzoek effectiever en efficiënter te maken. Het doel van de wetgeving is het bevorderen van informatiedeling tussen poortwachters die niet tot dezelfde juridische groep behoren.(445) De wetgeving bevat bepalingen rondom de mogelijke varianten van een gedeelde KYC-utiliteit en de bevoegdheden van en binnen een dergelijke utiliteit. De wetgeving faciliteert het opzetten van een gezamenlijke KYC-utiliteit en richt daarvoor een vergunningen- en toezichtregime in.

De wetgeving staat twee mogelijke varianten van een gedeelde KYC-utiliteit toe: een gesloten en een open variant. Op het moment van het onderzoeken waren er nog geen KYC-utiliteiten met vergunning actief in Letland.

Gesloten gedeelde KYC-utiliteit

Een gesloten gedeelde KYC-utiliteit betreft een door poortwachters op contractuele basis ingerichte KYC-tool die wordt beheerd door een externe dienstverlener, waaraan bijvoorbeeld een deel van het KYC-proces kan worden uitbesteed mits dit niet in strijd is met de mededingingsregelgeving.(446) Met de inwerkingtreding van de nieuwe wetgeving is het mogelijk dat verschillende categorieën poortwachters die niet tot dezelfde juridische groep behoren (aspecten van) het KYC-proces gezamenlijk uitbesteden.(447) Hiervoor is het wel van belang dat mededingingswetgeving in acht wordt genomen.(448)

Open gedeelde KYC-utiliteit

Een open gedeelde KYC-utiliteit betreft een platform dat wordt beheerd door een onafhankelijke dienstverlener waar poortwachters informatie over klanten en hun UBO's kunnen verkrijgen ten behoeve van hun cliëntenonderzoek. In vergelijking met de gesloten utiliteit wordt veel meer data gedeeld, die uit zowel private als publieke bronnen komt (bijv. overheidsregisters). Om te voorkomen dat poortwachters juridisch aansprakelijk worden gesteld voor het te goeder trouw verstrekken van informatie in een open gedeelde KYC-utiliteit, is in de wet geregeld dat deze verstrekking van informatie niet wordt beschouwd als openbaarmaking van vertrouwelijke informatie.(449)

(441) Zie artikel 17 van de Letse *Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing* (13 juni 2019), beschikbaar via deze link (hierna: Letse AML/CFT-wet); en de Letse *Regulations Regarding the Requirements for Updating Information in the Shared Know-Your-Customer Utility and the Licensing and Supervision of the Shared Know-Your-Customer Utility Service Provider (Cabinet Regulation No. 396)*, beschikbaar via deze link (hierna: Letse KYC utiliteit-voorschriften).

(442) In december 2022 heeft de Letse overheid het Actieplan ter voorkoming van witwassen, terrorismefinanciering en proliferatiefinanciering 2023-2025 aangenomen: ministerie van Binnenlandse Zaken van Letland, *Strengthening Latvia's capacity to combat financial crime*, persebericht 16 december 2022, beschikbaar via deze link.

(443) E. Pastars, 'From zero to hero – a brief overview of AML evolution in Latvia', *Cobalt* 10 september 2021; *Cabinet of Ministers, Order no. 122 On the action plan for the prevention of money laundering, terrorism and proliferation financing for 2022*, beschikbaar in de officiële taal via deze link.

(444) S. Merler, 'Latvia's money laundering scandal', *Bruegel Blog post* 9 april 2018; G. Stack, 'Latvian Prosecutors Charge Bankers with Laundering 2.1B Euro', *OCCRP* 29 juli 2022.

(445) Annotatie bij aanpassing Letse AML/CFT-wet, No. 90/TA-1880 (2020), onderdeel I(2)(10) *Initial Impact Assessment*, beschikbaar via deze link.

(446) Artikel 17.1(1) Letse AML/CFT-wet.

(447) Annotatie bij aanpassing Letse AML/CFT-wet, No. 90/TA-1880 (2020), onderdeel I(2)(10) *Initial Impact Assessment*, beschikbaar via deze link.

(448) Annotatie bij aanpassing Letse AML/CFT-wet, No. 90/TA-1880 (2020), onderdeel I(2)(10) *Initial Impact Assessment* beschikbaar via deze link.

(449) Artikel 17.2(5) Letse AML/CFT-wet.

B. Initiatieven in binnen- en buitenland

De volgende informatie mag worden verwerkt in een open gedeelde KYC-utiliteit:[450]

1. Algemeen beschikbare (openbare) informatie.
2. Klantinformatie betreffende rechtspersonen of UBO's voor zover deze informatie is verkregen uit overheidssystemen die vertrouwelijke gegevens bevatten – met uitzondering van informatie over strafrechtelijke veroordelingen – en poortwachters deze informatie op grond van de anti-witwasregelgeving dienen te vergaren.
3. Informatie die poortwachters delen binnen de reeds bestaande wettelijke kaders in het kader van het introducerend cliëntenonderzoek[451] of het informeren van betrokken poortwachters uit dezelfde categorie dat een melding is gedaan bij de FIU betreffende een gezamenlijke klant en transactie.[452]
4. Informatie over (rechts)personen die onderhevig zijn aan sancties maar die niet direct worden genoemd op internationale sanctielijsten (sectorale sancties), evenals over (rechts)personen die worden ingezet om internationale sancties te omzeilen.
5. Informatie over een natuurlijke persoon die is verzameld in het kader van het cliëntenonderzoek en waarvoor de betreffende persoon toestemming heeft gegeven om de informatie te delen via de open gedeelde KYC-utiliteit.

Informatiedeling binnen de open gedeelde KYC-utiliteit creëert voor klanten de mogelijkheid tot het gebruik van het one-stop principe. Na toestemming te hebben gegeven om zijn of haar gegevens te delen, hoeft de klant deze gegevens niet meer bij iedere poortwachter aan te leveren.[453] Deze toestemming kan desgewenst worden ingetrokken.[454]

De informatie die uitgewisseld wordt via open gedeelde KYC-utiliteiten is direct toegankelijk voor de Letse FIU. Voor andere overheidsorganen dient eventuele toegang bij wet worden geregeld.[455]

Vergunningplicht en toezicht

Voor gesloten gedeelde KYC-utiliteiten waarbij poortwachters niet tot dezelfde financiële of juridische groep behoren, en alle open gedeelde KYC-utiliteiten bestaat een vergunningplicht. De Letse privacytoezichthouder (Datu valsts inspekcija) is aangewezen als toezichthouder op deze KYC-utiliteiten en is verantwoordelijk voor de vergunningverlening. De vergunningen worden afgegeven aan de dienstverleners die de KYC-utiliteit (c.q. het platform) gaan beheren en zijn geldig voor een periode van vijf jaar.[456] Voor het verkrijgen van een vergunning moeten dienstverleners aan verschillende voorwaarden voldoen. Zo mag de dienstverlener bijvoorbeeld geen belastingschuld hebben. Om te borgen dat aan AVG-vereisten wordt voldaan, dient de dienstverlener een privacy officer te hebben aangesteld. Verder dienen de aandeelhouders en bestuurders van de dienstverlener over een goede reputatie en de juiste educatie te beschikken. Een ander voorbeeld is dat de dienstverlener over een passende aansprakelijkheidsverzekering dient te beschikken.[457]

1.7. CanDeal industry-wide KYC Solution

In juni 2022 kondigde CanDeal, een exploitant van Canadese markt- en infrastructuurdiensten, aan met vijf Canadese banken te gaan samenwerken om te komen tot een gecentraliseerde KYC-oplossing voor de kapitaalmarktensector.[458]

(450) Artikel 17.2(3) Letse AML/CFT-wet.
(451) Artikel 29 Letse AML/CFT-wet.
(452) Artikel 38(4) Letse AML/CFT-wet.
(453) Annotatie bij aanpassing Letse AML/CFT-wet, No. 90/TA-1880 (2020), onderdeel I(2)(10) *Initial Impact Assessment* beschikbaar via deze link.
(454) Sectie 6 Letse KYC utiliteit-voorschriften.
(455) Artikel 17.2(6) Letse AML/CFT-wet.
(456) Artikel 17.3 Letse AML/CFT-wet.
(457) Zie voor alle voorwaarden Sectie 8-16 Letse KYC utiliteit-voorschriften.
(458) CanDeal, 'Canadian Banks Partner with CanDeal to Deliver Industry-wide KYC Solution', persbericht 27 juni 2022.

B. Initiatieven in binnen- en buitenland

Deelnemende banken zijn de Bank of Montreal, de Bank of Nova Scotia (Scotiabank), de Canadian Imperial Bank of Commerce, de National Bank of Canada en de Royal Bank of Canada. Het doel is te komen tot gemeenschappelijke data-afspraken, leidend tot meer vertrouwen in het gebruik van data in de risicobeoordelingen en een meer gestroomlijnd KYC-proces voor klanten.

1.8. Incidentenwaarschuwings-systeem Financiële Instellingen (IFI)

Het Incidentenwaarschuwingssysteem Financiële Instellingen (IFI) is het systeem dat het mogelijk maakt voor financiële instellingen om te onderzoeken of iemand – bijvoorbeeld een klant of medewerker – een dreiging is of kan zijn voor de instelling of de financiële sector. Deelnemers zijn banken, verzekeraars, hypotheekverstrekkers en financieringsondernemingen die op grond van de financiële wet- en regelgeving een vergunning hebben om in Nederland diensten te verlenen, en zijn aangesloten bij een van de deelnemende brancheorganisaties.(459)

Het IFI bestaat uit de interne verwijzingsregisters (IVR) en het externe verwijzingsregister (EVR). Dit zijn registers die door de banken en verzekeraars en hun brancheorganisaties worden gehouden en informatie bevatten over klanten en medewerkers die zijn betrokken bij incidenten, zoals fraude, witwassen of valsheid in geschrifte.(460)

Het IVR – ook wel het incidentenregister genoemd – is het interne register binnen een (groep van een) financiële instelling en bevat registraties van personen die betrokken zijn geweest bij een incident binnen die instelling. Interne registers zijn toegankelijk voor het personeel van de financiële instelling en bevatten de naam en geboortedatum van natuurlijke personen of het KVK-nummer van rechtspersonen (eventueel aangevuld met bedrijfsnaam en postcode). Uitsluitend de afdeling Veiligheidszaken kent de aard en achtergrond van het incident.(461) Iedere instelling moet een IVR/incidentenregister hebben en is verwerkingsverantwoordelijke op grond van de privacyregelgeving.

Het EVR is gekoppeld aan het IVR en is het gedeelde register tussen financiële instellingen waarin klanten betrokken bij ernstige(re) incidenten worden opgenomen en banken en verzekeraars dus informatie over klanten van andere financiële instellingen kunnen inzien. Informatie opgenomen in het EVR blijft ook deel uitmaken van het IVR van een instelling. De instelling is de verantwoordelijke partij voor het verwerken van de gegevens (verwerkingsverantwoordelijke).

Voor interne registers is het voldoende dat een gebeurtenis heeft plaatsgevonden die volgens de instelling een risico vormt of aandacht behoeft. Voor externe registers is een zwaardere verdenking nodig en moet het gaan om gebeurtenissen die een bedreiging kunnen vormen voor de instelling, diens medewerkers of de financiële sector. Er moet daarbij in voldoende mate vaststaan dat de betreffende (rechts)persoon betrokken is bij de gebeurtenis c.q. de bedreiging. Dat betekent dat in principe aangifte van strafbare feiten kan worden gedaan en dat er een zwaarder vermoeden moet zijn dan een redelijk vermoeden van schuld.(462)

De registers kunnen worden geraadpleegd via het computersysteem genaamd EVA.(463) Een registercheck heet dan ook wel een 'EVA-toets'. In het geval van natuurlijke personen vullen medewerkers de naam en geboortedatum van de (toekomstige) klant in waarna een melding wordt verkregen of die persoon wel of niet voorkomt in het IVR of EVR ('hit – no hit').

(459) Betrokken brancheorganisaties zijn: Nederlandse Vereniging van Banken (NVB), Verbond van Verzekeraars, Vereniging van Financieringsondernemingen in Nederland (VFN), Stichting Fraudebestrijding Hypotheken (SFH) en Zorgverzekeraars Nederland (ZN). Ook kunnen financiële instellingen die geen lid zijn van de NVB, het Verbond van Verzekeraars, of ZN, onder strikte voorwaarden worden toegelaten als deelnemer.

(460) NVB, *IVR/EVR-registratie*, beschikbaar via deze link.
(461) NVB, *IVR/EVR-registratie*, beschikbaar via deze link.
(462) De Vries en Mourcous 2019, p. 248-249.
(463) Het systeem wordt voor verzekeraars beheerd door Stichting Centraal Informatie Systeem (CIS) en voor banken door Stichting Bureau Krediet Registratie (BKR).

B. Initiatieven in binnen- en buitenland

Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (PIFI)

Door deelnemers van IFI wordt onderkend dat opname in (gedeelde) registers vanwege fraude, witwassen of valsheid in geschrifte ingrijpend is voor de betrokken natuurlijke personen of rechtspersonen. Het IFI wordt daarom gereguleerd door het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen (PIFI) 2021. In het PIFI wordt de rol van financiële instellingen in het voorkomen van misbruik en fraude benoemd en het belang van samenwerking – en daarmee samenhangend de mogelijkheid om informatie uit te wisselen – om misbruik en fraude te voorkomen benadrukt.(464) Vanwege de inbreuk op de privacy van natuurlijke en rechtspersonen gelden strenge registratiecriteria, gebaseerd op strikte proportionaliteits- en subsidiariteitseisen. De Autoriteit Persoonsgegevens heeft dit protocol goedgekeurd en voor de verwerking van strafrechtelijke gegevens overeenkomstig het protocol een vergunning afgegeven.(465) Tevens houdt de AP toezicht op de naleving van het protocol.

Het PIFI bevat voorwaarden voor gegevensuitwisseling en waarborgen tegen ongeautoriseerd gebruik van het stelsel van gegevensuitwisseling, waaronder geheimhouding en bewaartermijnen (hoofdstuk 3 PIFI). Zo regelt paragraaf 3.3 PIFI bijvoorbeeld het toetsingsproces: in beginsel is het antwoord van een bevraagde instelling op een aanvraag over een natuurlijke persoon of rechtspersoon op basis van een 'hit – no hit'-melding richting de aanvragende instelling. Wanneer er sprake is van een hit wordt in beginsel uitsluitend meer informatie over de registratie uitgewisseld tussen de afdeling Veiligheidszaken van de bevraagde instelling en de afdeling Veiligheidszaken van de aanvragende instelling. De afdeling Veiligheidszaken van de aanvragende instelling adviseert vervolgens de medewerker die de aanvraag heeft gedaan. Dit advies kan zijn om de relatie onder voorwaarden aan te gaan, de relatie niet aan te gaan of te beëindigen. Het is voor bevrager verplicht dit advies mee te nemen in de besluitvorming jegens de betreffende natuurlijke persoon of rechtspersoon.(466)

Het PIFI bevat ook vereisten rond de toegang tot de registers, bewaartermijnen en verwijdering van gegevens uit de registers (hoofstukken 4 en 5). Qua governance is op grond van het PIFI een begeleidingscommissie opgezet. Deze adviseert onder andere over de toepassing van de vastleggingscriteria, over de ontvankelijkheid en geschiktheid van banken en verzekeraars die willen toetreden tot het waarschuwingssysteem, dan wel over het uitsluiten van deelnemers in het geval van niet-naleving van het protocol (hoofdstukken 6 en 7). Het PFI bevat nadere rechten en plichten van de deelnemende financiële instellingen, zoals verplichting tot reciprociteit of het vervaardigen van werkinstructies voor personeel (hoofdstuk 8). Tot slot bevat het PIFI ook bepalingen over de rechten en plichten van natuurlijke personen en rechtspersonen die opgenomen worden in de IVR/EVR. Zij hebben in beginsel het recht hierover geïnformeerd te worden, om uitsluitsel te krijgen of de persoonsgegevens in het register zijn opgenomen en daar op verzoek inzage in te krijgen. Indien de gegevens incorrect zijn, heeft betrokkene het recht om de gegevens te laten corrigeren. Betrokkenen hebben ook de mogelijkheid om bezwaar te maken tegen opname in de registers of naar een geschillencommissie te stappen (hoofdstuk 10). Tot slot is van belang op te merken dat een IVR/EVR-registratie niet mag leiden tot uitsluiting van basisproducten, zoals een basisbankrekening of basisverzekering.(467)

(464) Protocol Incidentenwaarschuwingssysteem Financiële Instellingen 2021, p. 6-7. (PIFI 2021).
(465) PIFI 2021, p. 5; Autoriteit Persoonsgegevens, *Besluit inzake de vergunningaanvraag voor de verwerking van [PARTIJ] volgens het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen 2021*, 20 augustus 2021, kenmerk z2021-03355, beschikbaar via deze link. Voor partijen die later deelnemen aan IFI is vereist dat zij een aparte vergunning bij de AP aanvragen, zie De Vries en Mourcous 2019, p. 250.
(466) Paragraaf 3.3.1 PIFI 2021.
(467) PIFI 2021, p. 8.

B. Initiatieven in binnen- en buitenland

2. De ontwikkeling en het gebruik van digitale identiteiten en authenticatiemiddelen

2.1. Australia Post Digital iD

Er wordt in de literatuur wel gezegd dat Australië *"de meest moderne vorm van digitale identificatie"* kent.(468) Tegelijkertijd wordt ook gezegd dat het gebruik van nationale identiteitssystemen voor meerdere doeleinden in Australië een *"poor track record"* heeft.(469)

De Trusted Digital Identity Framework (TDIF) in Australië biedt een (tijdelijk) accreditatiekader voor digitale identiteitsdienstverlening, waaronder zowel overheidspartijen als private partijen digitale identiteiten kunnen ontwikkelen en aanbieden.(470) Het kader bevindt zich nog in een pilotfase, maar de wettelijke verankering is aanstaande met de 2023 Digital Identity draft legislation.(471) Sinds 17 mei 2019 is de Australia Post Digital iD onder dit schema geaccrediteerd; nadien zijn enkele andere (commerciële) dienstverleners ook toegelaten. De Digital iD van Australia Post wordt gezien als de meer commerciële tegenhanger van het door de overheid ontwikkelde GovPass.(472)

De Australia Post Digital iD is een commerciële dienst van Australia Post. Australia Post is een staatsbedrijf, met de overheid als enige aandeelhouder. Echter, het bedrijf ontvangt geen staatsfinanciering en opereert feitelijk als een commercieel bedrijf. Jaarlijks betaalt het bedrijf dividend uit aan de overheid.(473) De Australia Post Digital iD is optioneel voor natuurlijke personen en werkt via een app. De gebruiker downloadt de app, vult enkele persoonsgegevens in en maakt een 'selfie'. Deze gegevens worden vergeleken met gegevens uit overheidsregisters. Vervolgens dient de gebruiker zich fysiek te identificeren met een paspoort of rijbewijs en de telefoon waarop de app staat in een filiaal van Australia Post, waarna de digitale identiteit geactiveerd wordt.(474) Daarna kan een persoon zich via de app identificeren bij partijen die gebruikmaken van de Digital iD van Australia Post. Partijen vragen de gebruiker om toestemming om de digitale identiteit op te halen, wat kan worden bevestigd door de gebruiker via de app. De gegevens behorende bij de Digital iD van Australia Post zijn beperkt tot de standaardgegevens die nodig zijn voor de identificatie en verificatie van personen. Daarbij gaat het om de naam, geboortedatum en -plaats, en woonplaatsgegevens.

Een dienst die gelinkt is aan de Digital iD is Keypass: hiermee kunnen gebruikers bewijzen dat zij ouder zijn dan 18 om alcohol te kopen zonder hun persoonlijke gegevens te delen.(475) Sinds 2021 is de Digital iD te linken aan DocuSign, waarmee documenten digitaal ondertekend kunnen worden.(476)

Digitale identiteiten worden in Australië nog niet (op grote schaal) gebruikt door instellingen in het kader van hun cliëntenonderzoek, hoewel gebruik van elektronische data voor identificatie en verificatie is toegestaan.(477) Australia Post Digital iD wordt wel aangeboden als tool voor de identificatie en verificatie van natuurlijke personen bij het aangaan van zakelijke relaties en gedurende de relatie. Ook geeft Australia Post aan dat de Digital iD in het kader van de AML/KYC-dienstverlening door Australia Post de mogelijkheid biedt voor het verrichten van onder meer PEP-screening, en sanctiescreening.(478)

(468) Rainey et al. 2019, p. 37: *"Australia has the most modern form of digital identification".*
(469) ASPI 2018, p. 3.
(470) Zie ASPI 2022, p. 4-5 voor meer toelichting op de TDIF.
(471) *Digital Identity System: Legislation,* beschikbaar via deze link.
(472) ASPI 2018, p. 7.
(473) Australia Post 2021, p. 4.
(474) Australia Post, *Digital ID,* beschikbaar via deze link; Rainey et al. 2019, p. 37.
(475) Australia Post, *Digital ID,* beschikbaar via deze link.
(476) Australia Post, 'AusPost's Digital iD linked with DocuSign for e-signatures', persbericht 24 maart 2021.
(477) AUSTRAC, *Reliable and independent documentation and electronic data,* beschikbaar via deze link.
(478) Australia Post, AML solutions: Digital iD AML/KYC offering, beschikbaar via deze link.

B. Initiatieven in binnen- en buitenland

2.2. Singapore Personal Access: Singpass

In Singapore hebben de financieel toezichthouder Monetary Authority of Singapore (MAS) samen met de Smart Nation and Digital Government Office (SNDGO) en de Government Technology Agency (GovTech) bijgedragen aan de ontwikkeling van de nationale digitale ID van Singapore: de Singapore Personal Access, kortweg: Singpass.(479) Singpass wordt door overheidsinstanties en (financiële) instellingen gebruikt en bestaat voor zowel natuurlijke personen als rechtspersonen. Singpass is beschikbaar via een app.

Via Singpass kunnen verschillende diensten worden verleend:

- *MyInfo* (persoonlijke informatie voor KYC-doeleinden)
- *Verify* (verifiëren van klanten in fysieke situatie)
- *Login* (toegang tot digitale dienstverlening)
- *Sign* (digitaal ondertekenen van documenten)
- *Biometrics-as-a-service* (biometrie-als-een-dienst)
- *SafeEntry* (in- en uitchecken bij organisaties)
- *SGFinDex* (consolidatie financiële gegevens)
- In de toekomst komt hier nog *Remote Authorisation* (op afstand autoriseren van transacties) bij.(480)

De diensten zijn via API's gelinkt aan het Singpass-systeem. Via de Singpass API-portal website stelt de overheid alle broninformatie over de architectuur, de werking van de API en voorwaarden voor gebruik open voor het brede publiek.(481) De volgende diensten worden door financiële instellingen gebruikt: MyInfo, Sign en SGFinDex.(482)

Gebruik van Singpass-diensten die in het geheel beschikbaar worden gesteld door de overheid via GovTech, worden door de toezichthouder MAS niet beschouwd als vorm van uitbesteding.(483) Financiële instellingen mogen dus gebruikmaken van deze diensten en tools, zonder te moeten voldoen aan bijkomende eisen bij uitbesteding. De reden hiervoor is dat de overheid al controles uitvoert op de diensten en dat de maatschappij in brede zin van deze diensten gebruik kan maken. De drie diensten lichten we hierna verder toe:

1. MyInfo en MyInfo Business

Personen kunnen via een tool genaamd MyInfo – en voor rechtspersonen MyInfo Business – toestemming geven om hun persoonlijke of zakelijke data te gebruiken. Via MyInfo met Singpass kunnen klanten onder meer het KYC-proces doorlopen voor het openen van bankrekeningen en het aanvragen van creditcards en leningen.(484)

Financiële instellingen mogen deze informatie gebruiken voor hun KYC-proces: de MAS accepteert MyInfo als een onafhankelijke en betrouwbare bron voor de volgende gegevens: klantnaam, het nationale ID-nummer, geboortedatum, nationaliteit en woonadres. Financiële instellingen hoeven geen aanvullende identificatie of verificatie te verrichten of (andere) fysieke documentatie, noch een foto van de klant, op te vragen.(485) Via MyInfo wordt deze informatie gecombineerd uit openbare registers: het varieert van persoonlijke informatie (bijv. volledige naam, BSN-nummer, geslacht, geboortedatum, nationaliteit, paspoortnummer) tot financiële informatie, informatie over iemands beroep en opleiding, gezinssamenstelling, auto's en rijbewijs, huisvesting en overheidsprogramma's (bijv. AOW-uitkering).(486)

(479) Monetary Authority of Singapore, *Digital ID and e-KYC*, beschikbaar via deze link.
(480) Singpass, *Transforming Singapore through technology*, beschikbaar via deze link.
(481) Singpass, *Transforming Singapore through technology*, beschikbaar via deze link.
(482) Monetary Authority of Singapore, *Digital ID and e-KYC*, beschikbaar via deze link.
(483) Monetary Authority of Singapore, *Circular ID 26/20: Outsourcing arrangements involving services wholly provided by the Government echnology Agency ("GovTech") or agents appointed by GovTech*, 9 juni 2020, beschikbaar via deze link.
(484) Singpass, *Singpass API Products*, beschikbaar via deze link; Monetary Authority of Singapore, *Circular ID 26/20: Outsourcing arrangements involving services wholly provided by the Government Technology Agency ("GovTech") or agents appointed by GovTech*, 9 juni 2020, beschikbaar via deze link.
(485) Monetary Authority of Singapore, *Circular AMLD 01/2018: Use of MyInfo and CDD Measures for Non Face-to-Face Business Relations*, 8 januari 2018, beschikbaar via deze link.
(486) Singpass, *MyInfo: speed up eKYC processes for individual users with data from government sources*, beschikbaar via deze link.

B. Initiatieven in binnen- en buitenland

MyInfo bevat meer dan 100 verschillende datapunten.(487) Het doel is om alle financiële instellingen te ontsluiten op deze database en om financiële instellingen informatie te laten aanpassen of actualiseren, om zo herhaling van uitvragen richting klanten te voorkomen en de datakwaliteit te verhogen.(488)

Gegeven de werking fungeert de MyInfo-tool op het Singpass-systeem als een soort KYC-utiliteit. Het verschil met de initiatieven die zijn opgenomen in paragraaf 1 van deze bijlage is dat MyInfo door de overheid ontwikkeld en beheerd wordt.

2. Sign

Natuurlijke en rechtspersonen kunnen via een tool genaamd Sign documenten en overeenkomsten digitaal ondertekenen met het gebruik van hun Singpass.

3. SGFinDex

Natuurlijke personen kunnen via de tool SGFinDex (Singapore Financial Data Exchange) met gebruik van hun Singpass al hun financiële gegevens ophalen bij banken, verzekeraars, centrale effectenbewaarinstellingen ('central depositories') en relevante overheidsinstanties (ten behoeve van onder andere belastinginformatie en pensioeninformatie).

De SGFinDex is tot stand gekomen door samenwerking tussen de MAS, SNDGO, met ondersteuning van het Singaporese ministerie van Werkgelegenheid (*Ministry of Manpower*). De tool is gebouwd op Singpass door overheidspartijen, in samenwerking met de Singaporese brancheorganisaties voor banken en levensverzekeraars en deelnemende financiële instellingen. Financiële informatie mag worden gedeeld en geconsolideerd via SGFinDex na toestemming van de betrokken persoon. De toestemming is geldig voor de duur van één jaar.(489)

2.3. Digitale identiteit (e-ID) in Europa en bestaande commerciële oplossingen in Nederland

In Europa biedt de eIDAS-verordening uit 2014 de huidige basis voor het uniforme Europese beleid rondom digitale identiteit.(490) De verordening stelt eisen aan elektronische identificatie en authenticatiemiddelen, zoals elektronische handtekeningen. Zo bevat artikel 8 van de verordening bijvoorbeeld drie betrouwbaarheidsniveaus (laag, substantieel, hoog) die authenticatiemiddelen kunnen hebben. Het vereiste niveau verschilt per dienstverlening: hoe gevoeliger de informatie, des te hoger het betrouwbaarheidsniveau en des te hogere eisen worden gesteld.(491) In de verordening wordt ook de grensoverschrijdende erkenning van e-ID's van overheden vastgelegd en wordt geregeld dat Europese burgers en ondernemingen bij overheidsinstanties, zoals gemeenten, provincies en rijksoverheid, moeten kunnen inloggen met een Europees erkend nationaal inlogmiddel. Voor de authenticatiemiddelen, ook wel vertrouwensdiensten genoemd, wordt een onderscheid gemaakt tussen gekwalificeerde vertrouwensdiensten en niet-gekwalificeerde vertrouwensdiensten. Aan gekwalificeerde vertrouwensdiensten worden hogere eisen gesteld en er wordt toezicht op gehouden. In Nederland wordt dit oor de Rijksinspectie Digitale Infrastructuur (RDI) gedaan.(492)

(487) FATF 2020, p. 76.
(488) JFSC 2020, p. 20.
(489) Monetary Authority of Singapore, *Singapore Financial Data Exchange (SGFinDex)*, beschikbaar via deze link.
(490) Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, *PbEU* L-257, p. 73-11.
(491) Uitvoeringsverordening 2015/1502 van de Commissie van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt, *PbEU* L-253, p. 7 (Uitvoeringsverordening eIDAS) bevat de eisen per betrouwbaarheidsniveau voor de verschillende authenticatiemiddelen.
(492) Rijksinspectie Digitale Infrastructuur, *Elektronische vertrouwensdiensten*, beschikbaar via deze link.

B. Initiatieven in binnen- en buitenland

In 2020 publiceerde de Europese Commissie de strategie rondom de digitale toekomst van de EU en introduceerde *"Een Europa dat klaar is voor het digitale tijdperk"* als een van haar beleidsprioriteiten.(493) Binnen dit plan committeerde de Commissie zich om de eIDAS-verordening te herzien *"om de doeltreffendheid ervan te verbeteren, de toepassing ervan uit te breiden tot de particuliere sector en betrouwbare digitale identiteiten voor alle EU-burgers en -bedrijven te promoten"*.(494)

In juni 2021 publiceerde de Europese Commissie de evaluatie naar de werking van de eIDAS-verordening. Uit de evaluatie komt onder meer naar voren dat eIDAS slechts een beperkte dekkingsgraad heeft, omdat slechts een beperkt aantal e-ID's door lidstaten zijn aangemeld en ontsloten. Verder zijn de kosten hoger gebleken dan de baten en zijn er praktische problemen bij de erkenning van e-ID's.(495) Ook komt de verordening niet tegemoet aan de marktbehoefte: uit de evaluatie bleek dat de meeste meerwaarde werd gezien in het gebruik van e-ID's in de private sector.(496)

Op basis van de evaluatie en in lijn met de eerdergenoemde beleidsprioriteit, heeft de Europese Commissie een voorstel tot wijziging van de eIDAS-verordening ingediend (eIDAS2-verordening).(497) De belangrijkste wijziging is dat de eIDAS-verordening van een kader voor digitale identiteiten binnen verschillende lidstaten naar één overkoepelend kader voor een Europese digitale identiteit beweegt. De Europese Commissie stelt concreet voor dat elke Europese burger en onderneming een eigen Europese digitale ID-portemonnee krijgt, met daarin informatie over de identiteit, maar optioneel ook andere gegevens, zoals diploma's, medische gegevens of volmachten (autorisaties om namens rechtspersonen op te treden).(498) Het voorstel bepaalt dat de digitale identiteit via een app beheerd wordt door de natuurlijke persoon of rechtspersoon zelf; voor natuurlijke personen is de Europese portemonnee voor digitale identiteit gratis (artikel 6bis(6) eIDAS2-verordening). Zij kunnen zelf kiezen welke persoonsgegevens en documenten ze, online en offline, met welke overheidsinstanties en private partijen willen delen. Daarmee heeft de persoon in kwestie dus zelf de controle over het delen van zijn/haar gegevens. De verordening bepaalt dat Europese portemonnees voor digitale identiteit het hoogste beveiligingsniveau voor de voor authenticatie gebruikte persoonsgegevens moeten waarborgen (artikel 6bis(6) eIDAS2-verordening). Private partijen uit een grote groep sectoren (vervoer, energie, financiële dienstverlening, sociale zekerheid, gezondheidszorg, drinkwatervoorziening, postdiensten, digitale infrastructuur, onderwijs of telecommunicatie) worden verplicht de Europese digitale identiteit te waarborgen (artikel 12ter eIDAS2-verordening). Een andere belangrijke wijziging is de uitbreiding van de reikwijdte van de eIDAS2-verordening naar andere vertrouwensdiensten, *"aansluitend op de marktdynamiek en technologische ontwikkelingen"*.(499) Nieuwe diensten die in het voorstel onder de reikwijdte komen te vallen zijn het op afstand beheren van middelen voor het aanmaken van elektronische handtekeningen en elektronische zegels, het aanbieden van elektronische archiefdiensten, het aanbieden van elektronische registers (ledgers) en elektronische attestatie van attributen, oftewel digitaal gewaarmerkte verklaringen van onder meer diploma's.(500)

(493) Europese Commissie, *De prioriteiten van de Europese Commissie*, beschikbaar via deze link.
(494) Europese Commissie 2021, p. 7.
(495) Europese Commissie 2021, p. 3-5.
(496) Europese Commissie 2021, p. 8.
(497) Voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit, COM(2021) 281 final, 2021/0136(COD), 3 juni 2021.
(498) Europese Commissie, *Europese digitale identiteit*, beschikbaar via deze link. Zie ook: DNB 2022, p. 29-30.
(499) Voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit, COM(2021) 281 final, 2021/0136(COD), 3 juni 2021, p. 1 (motivering en doel van het voorstel).
(500) Voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit, COM(2021) 281 final, 2021/0136(COD), 3 juni 2021, p.15.

B. Initiatieven in binnen- en buitenland

Nederland

In aanvulling op de direct van toepassing zijnde eIDAS-verordening en diens opvolger, is in Nederland in maart 2023 ook de Wet digitale overheid (Wdo) goedgekeurd.(501) Deze wet legt de verdere basis voor digitalisering van de overheid, maar gaat ook over de mogelijkheid voor burgers en bedrijven om naast DigiD ook erkende private inlogmiddelen te gebruiken.(502) Wat betreft het gebruik van digitale identiteiten staat de Wwft het, zoals eerder in dit hoofdstuk aangegeven, toe dat poortwachters bij het cliëntenonderzoek gebruikmaken van elektronische identificatiemiddelen om de identiteit van cliënten vast te stellen en te verifiëren, mits deze voldoen aan een substantieel of hoog betrouwbaarheidsniveau. Dit mogen private elektronische identificatiemiddelen zijn. DNB stelt in een Q&A dat instellingen zelf verantwoordelijk blijven voor de naleving van deze eis en dat zij zelf vast moeten stellen dat een e-ID-middel voldoende betrouwbaar is, of dit door een deskundige moeten laten doen.(503)

Specifiek voor het notariaat is het in 2022 ingediende wetsvoorstel inzake het digitaal oprichten van besloten vennootschappen interessant. Dit wetsvoorstel beoogt het oprichten van een besloten vennootschap mogelijk te maken zonder fysieke aanwezigheid van de aanvrager. In het geval geen vermoeden bestaat van identiteitsfraude of twijfel over de handelingsbekwaamheid van de aanvrager, volstaat een verschijning voor de notaris via beeldverbinding en kan de notaris de identiteit van de aanvrager vaststellen aan de hand van een elektronisch identificatiemiddel met betrouwbaarheidsniveau eIDAS-Hoog.(504) De elektronische notariële akte kan digitaal worden ondertekend met een elektronische handtekening.(505) Mede om de digitale oprichting van B.V.'s mogelijk te maken ontwikkelt de Koninklijke Notariële Beroepsorganisatie (KNB) momenteel NotarisID; een combinatie van een elektronisch identificatiemiddel met betrouwbaarheidsniveau eIDAS-Hoog en een gekwalificeerde elektronische handtekening conform de eIDAS-verordening.(506)

In Nederland zijn bovendien verschillende andere private en commerciële initiatieven op het gebied van digitale identiteit, authenticatiemiddelen en digitaal administratiebeheer. Een voorbeeld van een digitale identiteit is iDIN: *"een dienst van de banken waarmee consumenten zich bij andere organisaties met de veilige en vertrouwde inlogmiddelen van hun eigen bank kunnen identificeren, inloggen en leeftijd bevestigen".*(507) Gegevens die binnen iDIN worden gebruikt zijn voorletters, achternaam, geboortedatum, leeftijdsindicatie (18+), woonadres, geslacht, e-mailadres en/of telefoonnummer. Deze gegevens zijn geverifieerd door de bank. Klanten bepalen zelf of en welke informatie mag worden gedeeld.(508) Een ander voorbeeld is Yivi (voorheen IRMA). Net als de plannen voor de Europese ID-portemonnee werkt Yivi via een app op een mobiel apparaat. Informatie die in de Yivi app kan worden geplaatst betreft persoonsgegevens zoals naam, adres en contactgegevens, maar kan ook andere attributen betreffen, zoals financiële gegevens, diploma's en medische gegevens. De persoon kan zelf bepalen welke informatie met wie mag worden gedeeld.(509) Een derde voorbeeld is een van origine Belgische dienst genaamd itsme®. Deze digitale identiteit werkt ook via een app. Bij het aanmaken van de digitale identiteit wordt de ID-kaart of het paspoort gescand door de telefoon en vervolgens wordt de persoon gevraagd met de camera van de telefoon zich te tonen.

(501) Rijksoverheid, 'Eerste Kamer neemt Wet digitale overheid aan', nieuwsbericht 21 maart 2023.
(502) Rijksoverheid, *Digitale Overheid*, beschikbaar via deze link.
(503) DNB, *Q&A Elektronische identificatiemiddelen en cliëntidentificatie*, beschikbaar via deze link.
(504) Zie het voorgestelde artikel 53g in het wetsvoorstel Wet online oprichting besloten vennootschappen, Kamerstukken II, 2021/2022, 36 085, nr. 2.
(505) Zie het voorgestelde artikel 53e in het wetsvoorstel Wet online oprichting besloten vennootschappen, Kamerstukken II, 2021/2022, 36 085, nr. 2.
(506) Informatie door KPMG verzameld op basis van gesprekken met de KNB, evenals de website van KNB, beschikbaar via deze link.
(507) Currence, *Collectieve betaalproducten: IDIN*, beschikbaar via deze link.
(508) iDIN, *iDIN – Een veilig iD*, beschikbaar via deze link.
(509) Informatie door KPMG verzameld, vertaald en samengevat vanaf de website: https://www.yivi.app/.

B. Initiatieven in binnen- en buitenland

Via gezichtsherkenning wordt de persoon vergeleken met de foto op het paspoort. Met itsme® kunnen personen zich identificeren, authentiseren, acties bevestigen en digitaal ondertekenen.(510) Tot slot zijn er al (commerciële) aanbieders van digitaal administratiebeheer of zogenoemde 'digitale datakluizen', vaak gecombineerd met het aanbieden van een digitale handtekening.(511)

3. Publiek-private samenwerking in Nederland

3.1. Fintell Alliance NL

Fintell Alliance NL is formeel opgericht via een Alliantiedocument in februari 2021 en betreft een publiek-private samenwerking van FIU-NL met de banken ABN AMRO Bank, ING Bank, Rabobank, de Volksbank, Triodos en Knab.(512)

Het doel van Fintell Alliance NL is het delen van kennis en operationele informatie tussen de betrokken partijen om criminele netwerken beter in kaart te brengen.(513) Via het delen van rode vlaggen, modus operandi en feedback op meldingen door FIU-NL aan de deelnemende banken wordt een verhoging van de kwaliteit van meldingen aan FIU-NL en opsporingsinstanties beoogd, alsook betere inzichten in trends en fenomenen in relatie tot witwassen en financieren van terrorisme.(514) Wat Fintell Alliance NL onderscheidt van andere PPS-verbanden is dat ook gezamenlijke inhoudelijke analyses worden verricht, voor zover wettelijk toegestaan. Concreet betekent dit dat analisten en onderzoekers van banken en FIU-NL op een fysieke locatie bijeenkomen en samenwerken aan (geanonimiseerde) analyses op een case-by-casebenadering. De uitkomsten van dit werk binnen Fintell Alliance worden ook in andere PPS-verbanden gebruikt, waaronder verschillende FEC-taskforces en -projecten (zie paragraaf 3.2 van deze bijlage).(515)

Doordat de banken en FIU-NL intensief samenwerken zijn de lijnen kort. FIU-NL legt in het Jaaroverzicht 2021 uit wat de successen zijn van Fintell Alliance NL: *"Daarnaast geven deelnemende bankanalisten aan dat de continue feedbackloop vanuit de FIU-Nederland zeer waardevol is voor verdere ontwikkeling en aanscherping. Datzelfde geldt voor de FIU-analisten, die enorme sprongen in hun kennis van het financiële stelsel maken en daardoor ongebruikelijke transacties nog beter kunnen duiden. Dit heeft al geresulteerd in duizenden verdacht verklaarde transacties en meerdere intelligence rapportages over onder andere facilitators, ondergronds bankieren en criminele netwerken die bedrijven opzetten ten behoeve van de smokkel van verdovende middelen. Dit is concrete financial intelligence voor onze opsporingspartners. Tegelijkertijd leidt het ook tot meer kennis die vervolgens gedeeld wordt binnen de banken waardoor een zichzelf versterkende feedbackloop ontstaat. Dit vergroot de effectiviteit van de poortwachtersfunctie die de banken in het kader van het voorkomen van het gebruik van het financiële stelsel voor witwassen en het financieren van terrorisme bekleden."* (516)

3.2. Financieel Expertise Centrum

Het Financieel Expertise Centrum (FEC) is in de eerste plaats een publiek samenwerkingsverband tussen autoriteiten met een toezicht-, controle-, vervolgings- of opsporingstaak in de financiële sector.(517)

(510) Informatie door KPMG verzameld, vertaald en samengevat vanaf de website: https://www.itsme-id.com/nl-NL.
(511) Een willekeurig aantal voorbeelden betreft Doccle, Vidua, Pondres, De Nederlandse Notariskluis, en Digizeker datakluis. Deze zijn niet door KPMG beoordeeld naar opzet, werking en bestaan.
(512) Voorafgaande aan de formalisering van het project heeft een succesvolle pilot tussen FIU-NL en de Volksbank plaatsgevonden: FIU 2021, p. 4.
(513) FIU 2021, p. 16.
(514) FATF 2022b, p. 59; FIU-Nederland, *Nationale samenwerking,* beschikbaar via deze link; FIU-Nederland, FIU-Nederland, 'FIU-Nederland treedt samen met grootbanken op tegen witwassen en terrorismefinanciering', nieuwsbericht 2 november 2021; NVB, 'Nieuwe publiek-private samenwerking in Fintell Alliance - "Nieuwe boost voor aanpak witwassen"', nieuwsbericht 11 februari 2021.
(515) FATF 2022b, p. 59.
(516) FIU 2021, p. 16.
(517) Dit betreffen de AFM, de Belastingdienst, DNB, FIU-NL, de FIOD, het OM en de politie. Zie hiervoor artikel 1 Convenant FEC 2014 (*Stcrt.* 2014, 2351).

B. Initiatieven in binnen- en buitenland

De oprichting van het FEC in 1998 volgde uit het maatschappelijk belang van een integere financiële sector, het belang van adequaat toezicht op de financiële sector en het belang van goede bestuursrechtelijke en strafrechtelijke rechtshandhaving in de financiële sector.(518) Naast de samenwerking tussen de relevante publieke FEC-partners, werken zij op programma- of projectbasis samen met private partijen. Deze publiek-private samenwerking is geïntegreerd in de drie kerntaken van het FEC, zoals hierna wordt toegelicht in de beschrijving van deze kerntaken.

1. Het creëren van structurele informatie-uitwisseling tussen de partners

De eerste kerntaak van het FEC ziet op het faciliteren van structurele informatie-uitwisseling.(519) Het FEC vervult deze taak ten eerste middels het 'FEC-informatieplatform' waarin signalen over (mogelijke) integriteitsissues bij personen of bedrijven kunnen worden uitgewisseld.(520) Door de informatie-uitwisseling kan de informatiepositie van de FEC-partners worden versterkt en kunnen eventueel gezamenlijke interventies worden uitgevoerd.(521) In het Programma FEC-Terrorismefinanciering wordt informatie uitgewisseld tussen de zeven FEC-partners, evenals met zes andere publieke organisaties.(522) Het doel van dit programma is onder meer het op basis van signalen in kaart brengen van financiële netwerken die een mogelijke relatie hebben met terrorisme. Aan de hand van de opgedane kennis worden bovendien typologieën van potentiële vormen van terrorismefinanciering geformuleerd.(523)

Naast de onderlinge informatie-uitwisseling tussen FEC-partners vindt er middels taskforces ook informatie-uitwisseling plaats tussen de FEC-partners en een groep deelnemende private partijen. Dit wordt ook specifiek de FEC-PPS genoemd. Momenteel vindt publiek-private samenwerking plaats binnen de *Serious Crime Taskforce* (SCTF) en de *Taskforce Terrorismefinanciering* (TFTF).

SCTF

De SCTF is in 2019 begonnen als pilot en heeft sinds 2021 een structureel karakter onder het FEC. De taskforce is gebaseerd op een convenant en een besluit op grond van artikel 20 Wet politiegegevens (Wpg), dat is goedgekeurd door betrokken ministeries.(524) Binnen de SCTF werken de politie, het OM, FIU-NL en de FIOD samen met ABN AMRO Bank, ING Bank, Rabobank, De Volksbank, Knab(525) en Triodos(526).

Binnen de SCTF worden door politie en FIOD, in afstemming met het OM, namen van adviseurs of rechtspersonen (tussenpersonen) gedeeld met FIU-NL en banken waarvan vermoed wordt dat zij mogelijk betrokken zijn bij georganiseerde criminaliteit, maar tegen wie nog geen strafrechtelijk onderzoek is gestart. De banken en FIU-NL analyseren deze informatie die mogelijk leidt tot meldingen van ongebruikelijke transacties. Via verdachtverklaring van ongebruikelijke transacties door FIU-NL kan deze informatie weer ter beschikking worden gesteld aan de opsporing. Aan de hand daarvan kan een strafrechtelijk onderzoek worden gestart door politie en FIOD.(527)

Volgens de deelnemers zijn er al meerdere successen behaald, "*zoals het aanpassen van procedures bij banken, strafzaken en honderden verdachte transacties*".(528) Het OM meldt dat het in 2022 ging om *"verschillende onderzoeken met meer dan 700 verdachte transacties, maar ook in aanscherping van procedures in het bankwezen […]"*. (529)

(518) Besluit instelling financieel expertisecentrum van 31 december 1998 (*Stcrt.* 1999, 32).
(519) Artikel 3 Convenant FEC 2014 (*Stcrt.* 2014, 2351).
(520) FEC 2022, p. 20.
(521) FEC 2022, p. 20; FEC 2021, p. 6.
(522) Dit betreffen de Douane, de Koninklijke Marechaussee, de Immigratie- en Naturalisatiedienst, het Bureau Financieel Toezicht, het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en de Belastingdienst afdeling Toeslagen, zie FEC 2022, p. 5.
(523) FEC 2022a, p. 13; FATF 2022b, p. 98.
(524) Convenant Pilot Serious Crime Taskforce, *Stcrt.* 2019, 43629; Politie, 'Serious Crime Taskforce leidt tot structurele samenwerking', persbericht 25 oktober 2021; FEC, *Taskforces*, beschikbaar via deze link.
(525) Addendum bij Convenant Serous Crime Taskforce (pilot): toetreding Knab, *Stcrt.* 2021, 25818.
(526) Addendum bij Convenant Serous Crime Taskforce (pilot): toetreding Triodos, *Stcrt.* 2022, 22003.
(527) Politie, 'Serious Crime Taskforce leidt tot structurele samenwerking', persbericht 25 oktober 2021; FEC, *Taskforces*, beschikbaar via deze link.
(528) Politie, 'Serious Crime Taskforce leidt tot structurele samenwerking', persbericht 25 oktober 2021.
(529) Openbaar Ministerie 2022, p. 18.

B. Initiatieven in binnen- en buitenland

TFTF

De TFTF is in 2017 opgezet als pilot en heeft sinds 2019 een structureel karakter. De taskforce is gebaseerd op het Convenant Terrorismefinanciering Taskforce.(530) Het heeft als doel *"het mogelijk maken van samenwerking tussen publieke en private partners ten behoeve van de preventieve en strafrechtelijke aanpak van terrorismefinanciering".*(531) Binnen de TFTF werken de politie, het OM, FIU-NL en de FIOD samen met Aegon, ABN AMRO Bank, ING, Rabobank, De Volksbank en Triodos.

De werkwijze binnen TFTF is vergelijkbaar met die als hiervoor geschetst voor SCTF. In de TFTF worden in een vroeg stadium door opsporingsdiensten de namen van (rechts)personen die in verband worden gebracht met terrorisme, en de financiering daarvan, gedeeld met de private partijen. Dus binnen de TFTF wordt naar specifieke signalen van terrorisme(financiering) gekeken, terwijl de focus bij de SCTF ligt op transacties die in potentie criminele netwerken of financiële modus operandi, gerelateerd aan de aangedragen adviseur of rechtspersoon, kunnen blootleggen.

2. Het realiseren van een kenniscentrum van, voor en door de partners op de voor het FEC relevante kennisgebieden

De tweede kerntaak van het FEC betreft het realiseren van een kenniscentrum ten behoeve van kennisdeling.(532) Dit 'kenniscentrum' kent meerdere vormen. Zo wordt kennis gedeeld via onderlinge contacten, door samenwerking tussen de FEC-partners, middels kennisbijeenkomsten (zogenaamde FECademy's) of via de diverse gremia en platforms (zoals het 'FEC-privacy platform') van het FEC. Naast dat publieke partijen onderling kennis delen, wordt er ook kennis tussen private en publieke partijen gedeeld binnen het FEC PPS Expertplatform.(533) Ook onderhoudt het FEC contacten met buitenlandse organisaties en neemt zij deel aan internationale bijeenkomsten ten behoeve van internationale kennisdeling.(534)

3. Het uitvoeren van projecten met het oog op concrete, operationeel bruikbare resultaten

De derde kerntaak van het FEC is het gezamenlijk uitvoeren van projecten op verschillende thema's en/of fenomenen, zowel tussen de autoriteiten als op basis van publiek-private samenwerking.(535) Recente projecten zien onder meer op crypto's, de synthetische drugsindustrie en illegale trustdienstverlening.(536) Deze projecten zijn gericht op het delen en vergroten van inzichten, kennis en vaardigheden.(537) In tegenstelling tot de werkwijze bij de taskforces worden binnen projecten geen persoonsgegevens uitgewisseld. Waar het binnen de taskforces momenteel uitsluitend gaat om samenwerking met de bancaire sector, is in 2022 in het kader van een project inzake crypto tevens samengewerkt met cryptodienstverleners.

3.3. AMLC

Het Anti-Money Laundering Centre (AMLC) is opgericht in 2013 op initiatief van de Fiscale inlichtingen- en opsporingsdienst (FIOD) en maakt ook deel uit van deze organisatie. Het AMLC is een kennis- en expertisecentrum waar publieke en private partijen nationaal en internationaal samenwerken om witwassen en financieren van terrorisme te bestrijden.(538)

(530) Convenant Terrorismefinanciering Taskforce, *Stcrt.* 2019, 43628.
(531) FEC, *Taskforces*, beschikbaar via deze link.
(532) Artikel 3 Convenant FEC 2014 (*Stcrt.* 2014, 2351).
(533) FEC 2022, p. 17. De deelnemende private partijen betreffen ABN AMRO, ING Bank, Rabobank, De Volksbank en de NVB.
(534) FEC 2022, p. 23-25.
(535) Artikel 3 Convenant FEC 2014 (*Stcrt.* 2014, 2351); FEC 2022, p. 6.
(536) Zie voor meer informatie, ook over andere projecten: FEC 2022, p. 6-16. Zie meer specifiek over het project gericht op illegale trustdienstverlening bovendien FATF 2022b, p. 148-149. De FATF beschrijft hier het probleem van (voormalig vergunninghoudende) trustdienstverleners die middels het opsplitsen van hun diensten trachten het toezicht van DNB te omzeilen, evenals de aanpak hiervan binnen het genoemde project.
(537) FEC 2022, p. 6.
(538) AMLC, *Wie zijn wij en wat doen wij*, beschikbaar via deze link. Zie ook: Diepenmaat 2021, p. 126.

B. Initiatieven in binnen- en buitenland

Publieke partners van het AMLC zijn onder meer het OM, FIU-NL, de Koninklijke Marechaussee, RIEC-LIEC, verschillende toezichthouders en bijzondere opsporingsdiensten. Private partijen waarmee het AMLC samenwerkt zijn bijvoorbeeld banken, notarissen en accountantsorganisaties.(539)

Kennisontwikkeling en -deling

Als kennis- en expertisecentrum richt het AMLC zich – veelal op projectmatige en thematische basis(540) – op het vergroten van de kennis over witwassen en financieren van terrorisme op basis van data en informatie. Voorbeelden zijn het (her)formuleren van witwastypologieën, het signaleren van nieuwe fenomenen en het ontwikkelen van nieuwe meldindicatoren.(541) Op de website publiceert het AMLC jurisprudentie, verdiepende artikelen, literatuur en bronnen met betrekking tot de strategische thema's. Ook publiceert het AMLC regelmatig podcasts, waarin AMLC-experts en gasten (uit de publieke en private sector, alsook uit de wetenschap) dieper ingaan op bepaalde witwasthematiek. Tevens ontwikkelt het AMLC trainingsmateriaal voor zowel de publieke als private partners.(542)

Ondersteunen strafrechtelijke onderzoeken

Naast deze actieve rol in het ontwikkelen en het delen van kennis met een breed publiek, ondersteunt het AMLC de FIOD en andere publieke partners bij strafrechtelijke (voor)onderzoeken. Het AMLC verricht de opsporingsonderzoeken niet zelf, maar kan aangedragen signalen beoordelen en verrijken.(543) Het AMLC heeft als onderdeel van de FIOD toegang tot strafvorderlijke informatie uit verschillende bronnen en heeft ook toegang tot de FIU-database met meldingen van ongebruikelijke transacties. De FATF-evaluatie over Nederland roemt de *"unique data availability"* en maakt melding van de 'AMLC Suite' als voorbeeld van een datahub. De AMLC Suite is een browser waarmee geautoriseerde personen van opsporingsdiensten gecombineerde informatie kunnen zoeken in verschillende bronnen: FIU-meldingen, politiële en strafvorderlijke gegevens en informatie uit openbare bronnen (zoals verschillende Leaks en Papers).(544)

3.4. Landelijke en Regionale Informatie- en Expertise Centra (LIEC/RIEC)

Het Landelijk Informatie- en Expertise Centrum (LIEC) en de tien Regionale Informatie- en Expertise Centra (RIEC's) zijn sinds 2008 opgerichte samenwerkingsverbanden die zich richten op het ondersteunen van de samenwerkende overheidspartners in de bestrijding van georganiseerde en ondermijnende criminaliteit in brede zin.(545) Het RIEC-LIEC-bestel doet dit door het vergroten van bewustwording over het probleem inzake georganiseerde en ondermijnende criminaliteit bij de overheid en private partijen, het ondersteunen en versterken van samenwerking zowel binnen de overheid als met private partijen, en het delen van kennis en expertise op het gebied van de bestuurlijke en integrale aanpak van ondermijnende criminaliteit.

(539) AMLC, *Wie zijn wij en wat doen wij*, beschikbaar via deze link; FATF 2022b, p. 60.
(540) De huidige strategische thema's van het AMLC betreffen de veiligheid van het financiële stelsel ('financial safety'), witwassen door middel van handelstransacties ('trade-based money laundering) en verborgen vermogen in binnen- en buitenland ('concealed assets'). Zie: www.amlc.nl.
(541) AMLC, *Wat wil het AMLC bereiken*, beschikbaar via deze link. Zie ook FATF 2022b, p. 41; Diepenmaat 2021, p. 126.
(542) FATF 2022b, p. 43.
(543) ECORYS 2018, p. 155.
(544) FATF 2022b, p. 41 en 51.
(545) Artikel 2 Convenant ten behoeve van Bestuurlijke en Geïntegreerde Aanpak Georganiseerde Criminaliteit, Bestrijding Handhavingsknelpunten en Bevordering Integriteitsbeoordelingen (hierna: RIEC-LIEC-convenant); RIEC-LIEC 2021, p. 8. De volgende overheidspartners nemen deel aan het RIEC-LIEC-convenant: Gemeenten, Provincies, Belastingdienst, FIOD, Douane, Nederlandse Arbeidsinspectie, Politie, Koninklijke Marechaussee, Openbaar Ministerie, Immigratie- en Naturalisatiedienst, Uitvoeringsinstituut Werknemersverzekeringen, Nederlandse Voedsel- en Warenautoriteit.

B. Initiatieven in binnen- en buitenland

Het RIEC-LIEC kenmerkt zich door een aanpak die regionaal, landelijk en internationaal van aard is. De regionale aanpak via de RIEC's volgt uit de gedachte dat georganiseerde ondermijnende criminaliteit doorgaans een regionale oorsprong en verankering kent.(546) Het LIEC ondersteunt de RIEC's waar taken alle RIECs raken maar te duur of specialistisch zijn om ze bij elke RIEC te beleggen.(547) Ook deelt het LIEC best practices en ervaringen met RIEC's.(548) Op internationaal vlak werkt het LIEC-RIEC samen met België en Duitsland binnen het EURIEC.(549)

RIEC-LIEC richt zich in de bestrijding van georganiseerde en ondermijnende criminaliteit op verschillende thema's. Een van deze thema's betreft witwassen en daaraan gerelateerde vormen van financieel-economische criminaliteit. Andere thema's zijn onder andere mensenhandel en -smokkel en georganiseerde hennepteelt.(550) In 2021 zagen de meeste RIEC-casussen op het thema witwassen.(551)

Samenwerking met de private sector

In de samenwerking met private partijen zijn bedrijven die kunnen worden gebruikt als facilitators van criminele activiteiten de voornaamste doelgroep. Dit kunnen poortwachters zijn, maar ook andere partijen zoals scholen, vliegvelden, havens of de bloemenveiling. De publiek-private samenwerking is niet primair gericht op het opsporen en vervolgen van criminelen, *"maar op het voorkomen en/of het verstoren van ondermijnende criminaliteit enerzijds en het gestructureerd opbouwen van duurzame samenwerkingsverbanden anderzijds"*.(552)

Er wordt binnen de publiek-private samenwerking ingezet op het delen van kennis en expertise. In dit kader organiseren RIEC's onder meer bewustwordingsbijeenkomsten en gesprekken met de branches. Op landelijk niveau organiseert het LIEC zogenaamde 'landelijke fenomeentafels'. Het eerste fenomeen dat behandeld is, betreft ondermijning in de vastgoedketen. Zodoende zijn notarissen en makelaars-taxateurs relevante private partijen in de PPS-context van het RIEC-LIEC.

PPS vindt ook plaats via (gezamenlijke) projecten. Projecten die worden geïnitieerd in het kader van PPS zijn gericht op het voorkomen en verstoren van criminaliteit, en het gestructureerd opbouwen van duurzame samenwerkingsverbanden. Enkele voorbeelden van projecten in het kader van witwassen zijn:

- Een onderzoek dat RIEC Amsterdam-Amstelland samen met de Makelaarsvereniging Amsterdam heeft laten uitvoeren naar de vraag in hoeverre Amsterdamse makelaars middels de uitoefening van hun poortwachtersfunctie barrières opwerpen om criminele activiteiten te belemmeren;(553)
- Een onderzoek 'Witwassen via vastgoed' dat RIEC Den Haag laat uitvoeren. Het doel van dit onderzoek is het door gemeenten leren herkennen en voorkomen van witwassen via vastgoed, en het achterhalen welke partners binnen het RIEC-convenant dan wel private partners nodig zijn voor deze aanpak;(554)
- Het project 'notariaat', gericht op het tegengaan van witwassen van criminele gelden, dat binnen RIEC Noord-Nederland wordt uitgevoerd.(555)

(546) Artikel 3 RIEC-LIEC-Convenant; RIEC-LIEC 2021, p. 8.
(547) Artikel 4 RIEC-LIEC-Convenant; RIEC-LIEC 2021, p. 8.
(548) RIEC-LIEC 2021, p. 29.
(549) Zie voor meer informatie deze link.
(550) Artikel 2 RIEC-LIEC-Convenant; RIEC-LIEC 2021, p. 12.
(551) RIEC-LIEC 2021, p. 15.
(552) RIEC-LIEC 2021, p. 29.
(553) Bureau Broekhuizen 2022.
(554) RIEC Den Haag 2022, p. 6.
(555) RIEC-LIEC 2021, p. 29.

B. Initiatieven in binnen- en buitenland

4. Centrale sturing overheid

4.1. Nationale risicobeoordelingen

Vergelijkend onderzoek naar NRA's uit acht landen, waaronder Nederland, toont een grote diversiteit in de opzet, uitvoering en rapportage.(556) Ook de kwaliteit lijkt beperkt: geen van de onderzochte NRA's voorziet in een goed onderbouwde en uitgebreide risicobeoordeling. Ferwerda en Reuter constateren dat alle NRA's fundamentele problemen kennen en maken daarin een onderscheid naar het gebruikte conceptuele kader ('conceptual confusion'), de gebruikte informatiebronnen en analysemethodiek, en de bruikbaarheid van de resultaten.(557)

Voornoemde maakt een verkenning uitdagend. Desalniettemin biedt een eigen analyse van verschillende NRA's uit het buitenland de mogelijkheid om inspiratie op te doen voor een verbetering van de NRA in Nederland. Uit de verrichte verkenning komen drie punten naar voren die mogelijk interessant zijn voor de Nederlandse overheid bij het versterken en verdiepen van de NRA. Dit betreft de toegepaste analysemethoden, sectorale risico's en geografische risico's.

Analysemethoden

Voor Nederland wordt in het eerder aangehaalde onderzoek gewezen op het feit dat de NRA (vrijwel) uitsluitend steunt op expertopinies: *"[a]t an extreme, the Dutch NRA made use only of expert opinion; it presented no data of any other kind"*.(558) Wel wordt door de onderzoekers opgemerkt dat de analysemethode in Nederland in vergelijking met die in andere landen kan worden gezien als het meest geavanceerd.(559) Andere informatiebronnen die in andere NRA's worden gebruikt betreffen onder meer meldingen van ongebruikelijke (verdachte) transacties, strafrechtonderzoeken, statistieken, literatuur en rapporten.(560) De Italiaanse NRA bevat de grootste diversiteit aan informatiebronnen.(561)

In de Nederlandse NRA witwassen wordt de analyse van de dreiging ingestoken vanuit de toegepaste witwasmethoden.(562) Aangezien witwassen een secundair crimineel feit is en volgt op gronddelicten, zou mogelijk een meer genuanceerde risicoschets kunnen worden gemaakt. De insteek vanuit gronddelicten is bijvoorbeeld te vinden in de Amerikaanse NRA.(563) Ook de Ierse NRA benadert het aspect van dreiging via gronddelicten en koppelt deze vervolgens aan veelgebruikte witwastypologieën.(564) De Canadese NRA categoriseert de gronddelicten in verschillende risicogroepen op basis van de mate van *"sophistication, capability, scope, and proceeds of crime"*.(565) Het valt te overwegen om de NRA te onderzoeken vanuit het perspectief van de onderliggende criminaliteit, de gronddelicten en in het verlengde daarvan de daarbij gebruikte witwasmethoden.

In de Nederlandse NRA wordt het residuele risico op witwassen geanalyseerd, dus het risico dat overblijft na inzet van het beleidsinstrumentarium. In de literatuur wordt gesuggereerd dat wanneer andere analysemethoden dan het (voornamelijk) steunen op expertmeningen worden toegepast, het meten van inherente risico's mogelijk waardevoller wordt.(566) Enkele andere NRA's richten zich momenteel al meer op de inherente risico's. De Canadese NRA is hier een duidelijk voorbeeld van en ook in de NRA van het Verenigd Koninkrijk lijkt dit het geval te zijn.(567)

(556) Ferwerda en Reuter 2022, p. 7 en 19.
(557) Ferwerda en Reuter 2022, p. 19.
(558) Ferwerda en Reuter 2022, p. 21.
(559) Ferwerda en Reuter 2022, p. 16.
(560) Ferwerda en Reuter 2022, p. 15-16.
(561) Ferwerda en Reuter 2022, p. 21.
(562) WODC 2020, p. 46.
(563) US Department of Treasury 2022a.
(564) Irish Department of Finance 2019, p. 28-38.
(565) Government of Canada 2023a, p. 17.
(566) Ferwerda en Reuter 2022, p. 36.
(567) UK HM Treasury 2020.

B. Initiatieven in binnen- en buitenland

Sectorale risico's

Buitenlandse NRA's gaan in vergelijking met de NRA witwassen verder waar het de analyse van sectorale risico's betreft, maar doen dat op verschillende manieren. Zo zijn de toezichthouders in België op grond van de anti-witwaswet verplicht hun toezicht uit te oefenen op grond van een risicobeoordeling.(568)

Gebaseerd op de supranationale NRA van de Europese Commissie en de NRA, aangevuld met eigen toezichtobservaties en data verkregen bij de uitoefening van het toezicht, publiceren de Belgische toezichthouders hun sectorale risicobeoordelingen.(569) Daarmee is de risicobeoordeling niet uitsluitend het startpunt voor het risicogebaseerde toezicht, maar kunnen poortwachters ook kennisnemen van deze aanvullende analyse toegespitst op hun sector en dienstverlening. Ook in het Verenigd Koninkrijk publiceren de toezichthouders sectorale risicobeoordelingen in aanvulling op de NRA *"in order to help firms to better estimate the risks they are exposed to"*.(570) De Ierse overheid heeft ervoor gekozen om naast de NRA ook op verschillende momenten sectorale c.q. thematische risicoanalyses te publiceren. Momenteel zijn er vier van dit soort risicoanalyses: de kansspelsector (2018), nieuwe technologieën(571) (2019), rechtspersonen en juridische structuren (2020), en aanbieders van trust- en bedrijfsdiensten (2022).(572) De Duitse overheid gaat in haar NRA uitgebreid in op specifieke risico's voor de verschillende categorieën poortwachters.(573) In aanvulling daarop heeft zij ook een sectorale risicoanalyse gepubliceerd, waarin wordt ingegaan op de specifieke kwetsbaarheden van rechtspersonen en andere juridische entiteiten voor witwassen en terrorismefinanciering.(574) De Ierse NRA bevat ook een meer gedetailleerde uiteenzetting van de specifieke witwasdreigingen per categorie poortwachter.(575) Tot slot is de analyse van de mate van kwetsbaarheid in de Italiaanse NRA ingestoken vanuit sectoraal perspectief, waarmee voor elke categorie poortwachters de relatieve kwetsbaarheid wordt bepaald.(576)

Geografische risico's

Enkele NRA's gaan ook in op geografische risico's voor het land, of verschillen tussen regio's wat betreft de witwasrisico's binnen het land. De Duitse NRA bevat bijvoorbeeld een uitgebreide analyse van mogelijke witwasrisico's voor Duitsland vanuit geografisch perspectief. Daarbij worden buurlanden, landen waar veel Duitsers wonen en vice versa, landen waar Duitsland een sterke economische relatie mee heeft en hoogrisicolanden in de analyse meegenomen.(577) De Italiaanse NRA gaat in op regionale verschillen wat betreft het gebruik van cash, waarbij ervan wordt uitgegaan dat cash een indicator is voor witwasrisico.(578)

4.2. Canada

In maart 2023 heeft Canada de eerste nationale strategie gepubliceerd: Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime Strategy 2023-2026.(579) De strategie is gebaseerd op de Canadese nationale inherente risicobeoordeling (National Inherent Risk Assessment) en op meerdere evaluaties van het Canadese anti-witwasbeleid. De strategie bevat vier prioriteiten:

1. Het verhogen van de operationele effectiviteit.
2. Het dichten van mazen in wet- en regelgeving.
3. Het verbeteren van de governance en coördinatie van het beleid.

(568) Artikel 87 van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten.
(569) Zie bijvoorbeeld: College van toezicht op de bedrijfsrevisoren 2023; Nationale Bank van België 2020.
(570) Zie bijvoorbeeld: UK Solicitors Regulation Authority 2021, p. 1-2; ICAEW 2022.
(571) Hierbij wordt gekeken naar cryptovaluta, crowdfunding en elektronisch geld.
(572) Irish Department of Finance, *National Risk Assessment - Money laundering and Terrorist Financing*, beschikbaar via deze link.
(573) German Federal Ministry of Finance 2019, p. 55-107.
(574) German Federal Ministry of Finance 2020.
(575) Irish Department of Finance 2019, p. 39-76.
(576) MEF 2019, p. 28-31.
(577) German Federal Ministry of Finance 2019, p. 31-33.
(578) MEF 2019, p. 8-11.
(579) Government of Canada 2023.

4. Het bijdragen aan de internationale initiatieven voor de bestrijding van witwassen en terrorismefinanciering.

Uit de vier prioriteiten volgen in totaal 13 activiteiten. De activiteiten betreffen in het algemeen toezeggingen om bepaalde inspanning te leveren, en in beperkte mate concrete resultaten of uitkomsten. Behalve dat de looptijd van de strategie van 2023-2026 is, bevat de strategie geen planning.

In de strategie is publiek-private samenwerking een van de belangrijkste speerpunten. De Canadese regering onderschrijft het belang van samenwerking met de private sector omdat het haar in staat stelt mogelijke witwas- en terrorismefinancieringsrisico's te identificeren, bredere financiële connecties te ontwaren, en intelligentie te verschaffen om bepaalde onderzoeken verder te brengen.(580) Wat betreft het verbeteren van de governance en coördinatie van het beleid zet de Canadese overheid bijvoorbeeld in op het uitbreiden van publiek-private samenwerking. Relevante overheidspartijen "*will continue to build on these partnerships and work with businesses (…) to improve information-sharing, increase value-added intelligence products, and implement relevant technology to continue to mitigate money laundering and terrorist financing activities*".(581) Een nadere specificering is niet opgenomen in de strategie.

4.3. Verenigde Staten

De nationale strategie tegen witwassen en terrorismefinanciering in de Verenigde Staten is neergelegd in de National Strategy for Combatting Terrorist and Other Illicit Financing, ontwikkeld door de US Department of Treasury.(582) De meest recente versie dateert uit mei 2022 en kent een looptijd van twee jaar. De strategie is gebaseerd op de risico's die zijn geïdentificeerd in de nationale risicobeoordelingen op het gebied van witwassen, terrorismefinanciering en proliferatiefinanciering. De strategie uit 2022 bevat vier prioriteiten:

1. Het vergroten van transparantie en het dichten van mazen in het regelgevend kader op het gebied van de bestrijding van witwassen en terrorismefinanciering.
2. Het voor financiële instellingen effectiever en efficiënter maken van het regelgevend kader op het gebied van de bestrijding van witwassen en terrorismefinanciering.
3. Het versterken van de operationele effectiviteit van de bestrijding van witwassen, terrorismefinanciering en proliferatiefinanciering.
4. Het ondersteunen en gebruiken van technologische innovaties om risico's van witwassen, terrorismefinanciering en proliferatiefinanciering te beperken.

De vier prioriteiten worden uitgewerkt in 14 actiepunten en voor elk actiepunt worden meerdere concrete uitkomsten benoemd. Deze betreffen zowel harde resultaten als inspanningsverplichtingen.

De strategie zet in het bijzonder in op de risicogebaseerde benadering, samenwerking (waaronder publiek-private samenwerking) en technologische innovatie. Wat betreft de risicogebaseerde benadering is het goed te wijzen op de FinCEN National AML/CTF Priorities uit 2021.(583) Deze prioriteiten, gebaseerd op de vorige nationale strategie, betreffen de grootste bedreigingen voor de Verenigde Staten. Instellingen worden geacht deze prioriteiten in hun interne beleid te verwerken. De prioriteiten betreffen acht gronddelicten voor witwassen: corruptie, cybercrime (inclusief cryptovaluta), binnen- en buitenlandse financiering van terrorisme, fraude, grensoverschrijdende georganiseerde criminaliteit, georganiseerde drugssmokkel, mensenhandel en mensensmokkel, en proliferatiefinanciering.(584)

(580) Government of Canada 2023, p. 10.
(581) Government of Canada 2023, p. 19.
(582) US Department of Treasury 2022.
(583) FinCEN staat voor Financial Crimes Enforcement Network en is de Amerikaanse tegenhanger van FIU-NL: FinCEN, 'FinCEN Issues First National AML/CFT Priorities and Accompanying Statements', persbericht 30 juni 2021.
(584) FinCEN 2021, p. 1-2.

B. Initiatieven in binnen- en buitenland

FinCEN heeft met de publicatie van de nationale prioriteiten aangekondigd met regelgeving en guidance te komen voor hoe instellingen deze prioriteiten dienen te integreren in hun risicogebaseerde aanpak. Op basis van publieke informatie lijkt hier echter nog geen opvolging aan te zijn gegeven.

In de 2022 strategie wordt wel nog vermeld dat de nationale prioriteiten op het gebied van witwassen en terrorismefinanciering regelmatig worden geactualiseerd en worden gedeeld met de private sector.(585) Voor technologische innovatie ten behoeve van een verhoogde compliance met de wet- en regelgeving door poortwachters geeft de Amerikaanse regering bijvoorbeeld aan in te zetten op de ontwikkeling en invoering van digitale identiteit-oplossingen, zowel voor gebruik door de overheid als door financiële instellingen. Ook is in de strategie opgenomen dat overwogen wordt een 'regulatory sandbox' te creëren.(586)

4.4. Verenigd Koninkrijk

In het Verenigd Koninkrijk werd in maart 2023 het tweede Economic Crime Plan 2023-2026 (hierna ook ECP2) gepubliceerd.(587) Het volgt op het eerste plan dat liep van 2019-2022, dat weer voortvloeide uit een Actieplan tegen witwassen en terrorismefinanciering uit 2016, het Actieplan tegen corruptie uit 2017 en de Strategie ernstige en georganiseerde criminaliteit uit 2018.(588)

Het ECP2 is een gezamenlijk actieplan van de publieke en private sector. De betrokken private sectoren zijn de bankensector, de verzekeringssector, de accountancy, en advocatuur.(589) De naleving en voortgang van het plan worden bewaakt door de Economic Crime Strategic Board, met vertegenwoordigers uit de publieke en private sectoren.

Het ECP2 richt zich op drie strategische prioriteiten:

1. Het verminderen van witwassen en het verhogen van inbeslagname c.q. ontneming.
2. Het bestrijden van kleptocratie en het terugdringen van het ontwijken van sancties.
3. Het terugdringen van fraude.

Binnen elk van de geselecteerde strategische prioriteiten zijn enkele nadere thema's vastgesteld. Voor het eerste thema (verminderen van witwassen) gaat het om het verminderen van het misbruik van Britse juridische structuren; het versterken van het toezicht en regelgevend kader; het tegengaan van crimineel gebruik van crypto's; het verbeteren van data, feedback en analyse door een hervorming van het meldsysteem; het verhogen van inbeslagnames c.q. ontneming; het verder brengen van het cross-sectorale operationele antwoord op witwassen in het licht van risico's en kwetsbaarheden. Deze thema's worden vervolgens uitgewerkt in concrete acties, met daaraan verbonden verantwoordelijke organisaties (zowel publiek als privaat), concrete uitkomsten en daarbij horende uitkomsten. In totaal bevat het plan 43 acties.(590)

Onderkennend dat publiek-private samenwerking van cruciaal belang is, wordt in het ECP2 gesteld dat *"directing public-private resource towards priority areas will enable us to maximise our collective impact against the threat"*.(591) Daarom committeert de overheid zich in het plan om samen met de private sector 'één versie van de waarheid' te ontwikkelen, waarin een gedeeld begrip van de risico's en kwetsbaarheden bestaat en waarbinnen prioriteiten kunnen worden aangebracht. Dit houdt, volgens het plan, in dat de overheid samen met de private sector onderzoekt hoe de overheid de private sector kan ondersteunen om meer risicogebaseerd haar rol te vervullen.(592)

(585) US Department of Treasury 2022, p. 15.
(586) US Department of Treasury 2022, p. 25.
(587) UK HM Government 2023.
(588) UK HM Treasury en Home Office 2019.
(589) De betrokken beroepsorganisaties zijn: UK Finance, Association of British Insurers, alle accountancy beroepsorganisaties verenigd in de Accountancy AML Supervisors' Group (AASG) , en The Law Society of England and Wales.
(590) UK HM Government 2023.
(591) UK HM Government 2023, p. 68.
(592) UK HM Government 2023, p. 68.

B. Initiatieven in binnen- en buitenland

Daaruit vloeit actiepunt 33 voort. Dit actiepunt richt zich op het versterken van de rol van het National Economic Crime Centre (NECC)[593] als 'system leader' verantwoordelijk voor de samenwerking met toezichthouders en bredere overheid om de prioriteiten en eenduidige visie voor het systeem ter bestrijding van economische criminaliteit te bepalen, alsook te identificeren waar 'het wat minder kan' om middelen vrij te maken voor nuttigere werkzaamheden.[594] Aan het actiepunt worden per kwartaal concrete mijlpalen verbonden.

Het plan onderkent het belang van informatiedeling, data en technologie. Het stelt vast dat informatie op dit moment niet optimaal gedeeld kan worden. Er zijn juridische en technologische uitdagingen, en waar informatiedeling mogelijk is speelt onder andere het gebrek aan standaardisatie een beperkende rol.[595] In dit kader wordt in het ECP2 een 'public-private economic crime data strategy' aangekondigd.[596] In aanvulling daarop geeft het plan aan dat de overheid in nauw contact zal staan met de private sector en de maatschappij over de mogelijkheden om met gebruik van nieuwe technologieën de strijd tegen economische criminaliteit te versterken.[597]

4.5. Italië

De Italiaanse overheid wordt geroemd om haar strijd tegen de Italiaanse maffia. In het Coalitieakkoord 2021-2025 *Omzien naar elkaar, vooruitkijken naar de toekomst* van 15 december 2021 hebben de coalitiepartijen opgenomen dat zij de geleerde lessen uit Italië willen betrekken bij het versterken van de aanpak van ondermijning.[598] Hoewel in het bijzonder relevant vanuit strafrechtelijk oogpunt gegeven de geïntegreerde anti-maffiawetgeving en de bevoegdheden voor opsporings- en justitiële instanties, hangt het preventieve anti-witwasbeleid hier ook nauw mee samen. De FATF merkt daarbij op dat Italië een sterke coördinatie kent.[599]

Centraal in deze coördinatie staat het *Comitato di Sicurezza Finanziaria (*CSF). Dit comité dat in 2001 werd opgericht[600], opereert binnen het Italiaanse ministerie van Economie en Financiën (MEF) en wordt voorgezeten door de directeur-generaal van het MEF.[601] Het CSF bestaat in beginsel uit vertegenwoordigers van verschillende departementen (naast MEF ook van Binnenlandse Zaken, Justitie, Buitenlandse Zaken en Internationale Samenwerking, en Economische Zaken), de Italiaanse Centrale Bank, de financieel toezichthouders op de kapitaalmarkten (CONSOB) en verzekeringssector (IVASS), de Italiaanse FIU, en verschillende opsporingsautoriteiten waaronder de Guardia di Finanza, de Carabinieri, verschillende anti-maffia en -terrorisme diensten, en een vertegenwoordiger van de Italiaanse douane.[602] Het CSF heeft onder meer de volgende taken:[603]

- Het coördineren van de aanpak van witwassen en terrorismefinanciering.
- Het adviseren van het ministerie van Economie en Financiën over het voorkomen van witwassen en terrorismefinanciering.
- Het opstellen van de NRA.[604]
- Het implementeren en handhaven van internationale sancties.

(593) Het NECC is een publiek orgaan dat in oktober 2018 speciaal is opgericht om een coördinerende rol te spelen in het beleid gericht op het tegengaan van economische criminaliteit, waaronder witwassen. Het NECC opereert onder de auspiciën van de National Crime Agency (NCA) – de opsporingsautoriteit verantwoordelijk voor de bestrijding van ernstige en georganiseerde criminaliteit. Zie: National Crime Agency, *National Economic Crime Centre*, beschikbaar via deze link.
(594) UK HM Government 2023, p. 69: *"Strengthen the role of the NECC as the system leader responsible in collaboration with regulators and wider public sector for informing priorities for the economic crime system and defining a single view of economic crime threats, and in tandem identify and agree activity which can be de-prioritised to enable an increased focus on high-utility activity."*
(595) UK HM Government 2023, p. 71.
(596) UK HM Government 2023, p. 72-73.
(597) UK HM Government 2023, p. 71.
(598) Zie 'Onderzoek: Italiaanse maffia-aanpak deels bruikbaar voor Nederland', *NOS.nl* 7 juni 2023. Zie voor het volledige onderzoek waar in dit artikel naar wordt verwezen Rijksuniversiteit Groningen 2023.
(599) Rijksuniversiteit Groningen 2023; FATF 2016, p. 22.
(600) Het comité is oorspronkelijk opgericht via wetsdecreet 369/2001 van 12 oktober 2001. Artikel 5 van wetsdecreet 90/2017 van 25 mei 2017 regelt de taken en verantwoordelijkheden van het CSF. Thans zijn de compositie en het functioneren van het CSF neergelegd in artikel 3 wetsdecreet 109/2007 van 22 juni 2007 met nadere regels omtrent het functioneren van het comité in het MEF decreet 59/2022 van 22 april 2022.
(601) MEF 2020, p. 13.
(602) MEF 2020, p 13; FATF 2016, p. 126. Het CSF wordt aangevuld met het agentschap staatseigendom in de context van bevriezen van tegoeden en andere sanctieregelgeving.
(603) MEF 2020, p. 13.
(604) MEF 2019.

B. Initiatieven in binnen- en buitenland

Relevant voor deze verkenning is in het bijzonder de coördinerende rol van het CSF. Met de vertegenwoordiging in het comité heeft een grote, diverse groep overheidspartijen een gedeelde taak bij de preventie van witwassen en terrorismefinanciering. Binnen het comité kunnen de verschillende autoriteiten samenwerken en informatie uitwisselen waarbij kan worden afgeweken van eventuele geheimhoudingsplichten die van toepassing zijn.(605) De FATF zegt hierover dat *"[d]etailed rules for the exchange of information and collaboration among the concerned agencies are established under article 9 of the AML Law. These agencies are required to cooperate and coordinate, and a Memoranda of Understanding (MOUs) must be signed between them"*.(606)

Elk jaar dient het CSF aan de minister van Economie en Financiën, met het oog op doorzending aan het parlement, te rapporteren over de verrichte inspanningen op het gebied van de preventie van witwassen en het financieren van terrorisme, waarbij het comité voorstellen moet doen voor het verbeteren van de anti-witwasaanpak.(607)

Het overkoepelende regelgevende kader en de gezamenlijke verantwoordelijkheid van betreffende overheidspartijen voor de coördinatie van het anti-witwasbeleid leidt ertoe dat deze partijen effectief en efficiënt met elkaar kunnen samenwerken om de gezamenlijke wettelijke doelstellingen te bereiken.

(605) Informatie door KPMG verzameld en vertaald van de website van het Italiaanse ministerie van Economie en Financiën, beschikbaar via deze link. Zie voor meer informatie bovendien FATF 2016, p. 22 en p. 149; UIF 2021, p. 128.
(606) FATF 2016, p. 129.
(607) Artikel 5, zevende lid, wetsdecreet 90/2017.

Lijst van geïnterviewde partijen

C

C. Lijst van geïnterviewde partijen

Organisaties

In alfabetische volgorde:

1. Autoriteit Financiële Markten (AFM)
2. Belastingdienst – Bureau Toezicht Wwft
3. Bureau Financieel Toezicht (BFT)
4. De Nederlandsche Bank (DNB)
5. Financial Intelligence Unit Nederland (FIU-NL)
6. Holland Quaestor
7. Koninklijke Notariële Beroepsorganisatie (KNB)
8. MKB-Nederland
9. Nederlandse Vereniging van Banken (NVB)
10. Vereniging van Makelaars en Taxateurs in onroerende goederen NVM U.A. (NVM)
11. Openbaar Ministerie (OM)
12. Vereniging VBO - Vereniging van Makelaars & Taxateurs
13. Verbond van Verzekeraars
14. VNO-NCW

Experts

15. Universiteit Utrecht (1)
16. Vrije Universiteit Amsterdam
17. Offshore Kenniscentrum
18. Universiteit Utrecht (2)