NUMMER 28 / MAART 2018 / JAARGANG 8

DE COMPLIANCE OFFICER

INTERVIEW:
ANITA VAN DIS
LANDELIJK OFFICIER
BESTRIJDING WITWASSEN

SPEAKERS' CORNER
DE PARADISE PAPERS:
INCIDENT OF TREND?

CDD

COLOFON

De Compliance Officer is het vakblad voor compliance officers en andere betrokkenen bij het complianceproces. De doelgroep bestaat uit compliance officers, bestuurders, toezichthouders, secretarissen van de vennootschap en bedrijfsjuristen die betrokken zijn bij het uitvoeren van compliancetaken.

REDACTIE:
Sharon Karsten (bureauredactie) en Cora Wielenga (eindredactie)
Tel 088 99 88 100 E-mail: redactie@complianceofficer.nl
AAN DEZE EDITIE WERKTEN VERDER MEE: Jan van Koningsveld, Judy van der Graaf, Harry Kerklaan, Mara Wesseling, Musa Elmas, Thai-Ha Vu
FOTOGRAFIE: Wilco van Dijen
VORMGEVING: Tangram Studio
DRUK: Platform P, Rotterdam
UITGEVER: Nederlands Compliance Instituut, Postbus 5111, Capelle aan den IJssel

Nieuwsfeiten, ingezonden artikelen en personeelsmutaties kunt u per e-mail doorgeven aan redactie@complianceofficer.nl.

Het abonnement is gratis voor de doelgroep. Abonnees buiten de doelgroep: € 50 per jaar.

Oplage 3.500 exemplaren
ISSN 1878-7991

INHOUD

25 JAAR WITWASBESTRIJDING

Hoewel compliance in Nederland eind jaren tachtig begonnen is met het voorkomen van marktmisbruik, komt de witwasbestrijding op een goede tweede plaats. Vlak nadat banken de eerste regelingen privébeleggingstransacties op orde hadden, diende zich een nieuw dossier aan: witwasbestrijding. Al vanaf 1993 hebben we in Nederland wetgeving ter voorkoming van witwasbestrijding. Destijds hadden financiële ondernemingen te maken met de Wet identificatie bij financiële dienstverlening en de Wet melding ongebruikelijke transacties. Deze wetten zijn na een aantal wetswijzigingen in 2008 vervangen door de huidige anti-witwaswet, de Wwft, oftewel de Wet ter voorkoming van witwassen en financieren van terrorisme. Als ik de sanctiewetgeving uit 1977 niet meereken, hebben we dit jaar een jubileum te vieren van vijfentwintig jaar wetgeving voor het bestrijden van witwassen in Nederland. Nu weet ik dat veel mensen dit niet zo'n feestje waard vinden. Deze regels worden namelijk gezien als een ballast die eerder zwaarder dan lichter wordt. Mede door de steeds veranderende en strengere wetgeving, maar evenzeer door de toezichthouders die de regels strikter interpreteren dan voorheen. Nu zal ik ook niet ontkennen dat de wetgeving van nu nog veel lijkt op die uit 1993. Ondanks dat de Wwft nog steeds gestoeld is op de twee klassieke pijlers van ken-uw-klant en de meldplicht, is er veel gewijzigd, en daarmee verzwaard. Ik zal evenmin ontkennen dat al deze regels daadwerkelijk bijdragen aan het voorkomen van witwassen dan wel het voorkomen van terrorismefinanciering. Het schiet wel eens zijn doel voorbij en dat maakt het lastig om deze regels vol enthousiasme te blijven opvolgen.

Toch zou ik willen voorstellen om, in het kader van laten-we-het-maar-omdenken-noemen, het juk van deze regels om te turnen in iets moois. Toen ik in 2004 zelf met begon met compliance en witwasbestrijding in het bijzonder, waren er op dat moment al mooie voorbeelden van banken die het gehele verplichte ken-uw-klant-principe commercieel benutten. Hoe mooi zou het zijn als we het merendeel van de CDD-verplichtingen vanuit commercieel oogpunt zouden kunnen vragen? De meeste medewerkers uit de eerste lijn hebben immers het vak gekozen vanuit het oogpunt om klanten te helpen, of wellicht vanuit een commerciële ambitie. Het lijkt me wat onwaarschijnlijk dat er iemand het vak van financieel adviseur, bankier, of vermogensbeheerder heeft gekozen vanwege de ambitie om te voldoen aan CDD-regelgeving. Hoe mooi zou het dan ook zijn om alle ken-uw-klant-informatie op te vragen vanuit dienstbaarheid naar de klant, en als dat wat te vaag klinkt, dan tenminste vanuit commercieel oogpunt. Hoe beter je de klant kent, des te eerder de klant zich gezien en gehoord voelt, en des te beter de dienstverlening daar weer op aansluit. Ik weet dat er al een aantal jaar verschillende instellingen zijn die proberen om deze slag te maken. We hebben zelfs een aantal jaar geleden een radiocommercial gehad waarin werd aangegeven dat deze bank heel veel vragen aan de klant stelde om zo de klant beter te kunnen bedienen. Alle vragen die in die commercial gesteld werden, kwamen voort uit toezichtwetgeving, maar waren nu anders verpakt. Tot nu toe is het de meerderheid van de instellingen die aan de Wwft moeten voldoen nog niet gelukt om de Wwft om te turnen in iets positiefs. Ik zou het mooi vinden als we bij het dertigjarig jubileum de ken-uw-klant-principes als een vanzelfsprekend commercieel onderdeel van de dienstverlening kunnen zien. Ik zou me kunnen voorstellen dat het financieel advieswerk daar een stuk leuker van wordt. Wat mij betreft dopen we CDD daarom om in Commercial Due Diligence.

Cora Wielenga

ANITA VAN DIS:

"COMPLIANCE OFFICERS. ZORG ERVOOR DAT ZE WETEN WIE JE BENT EN WAT JE DOET!"

Anita van Dis is Landelijk Officier Bestrijding Witwassen. Ze ontvangt ons op het Parket Generaal van het Openbaar Ministerie recht boven de Utrechtsebaan, de enige weg die rechtstreeks toegang biedt tot het centrum van Den Haag. Je zou deze locatie als symbool kunnen zien voor haar functie als bewaker van de wet bij het onderzoek naar witwassen. Maar natuurlijk doet een landelijk officier veel meer dan dat. Harry Kerklaan ging op bezoek en belandde niet in een prachtig grote werkkamer met een eikenhouten bureau, maar in een kaal bespreekkamertje met een whiteboard. De landelijk officier zou dit tijdens het gesprek veelvuldig gebruiken.

U BENT SINDS 2010 LANDELIJK OFFICIER BESTRIJDING WITWASSEN EN TERRORISMEFINANCIERING. WAT IS UW JURIDISCHE ACHTERGROND? "Ik ben hier in Den Haag in 1999 als zaaksofficier begonnen. Later kwam het Functioneel Parket, dat min of meer al was ontstaan tijdens de beroemde Clickfondszaak. Daar heb ik ook aan gewerkt. In 2009 werd ik de nieuwe landelijk officier. Ook zit ik in het managementteam van de FIU, de Financial Intelligence Unit. Ik zet de grote lijnen uit, ik coördineer de witwasbestrijding en selecteer de witwaszaken die we in het strafrecht op gaan pakken. Ik doe nog wel zaken, maar niet zo veel meer. Het gros van de witwaszaken wordt door de zaaksofficieren in het land gedaan."

WELKE TAKEN, VERANTWOORDELIJKHEDEN EN BEVOEGDHEDEN HEEFT U ALS OFFICIER VAN JUSTITIE? "De officier van justitie is belast met de strafrechtelijke handhaving van de rechtsorde. Het OM zorgt ervoor dat strafbare feiten, waaronder witwassen, worden opgespoord en vervolgd en werkt daarbij samen met het Landelijk Parket, de politie, het Anti-Money Laundering Centre (AMLC) van de FIOD en andere opsporingsdiensten. Daarnaast bewaakt een officier of de opsporing volgens de wet gebeurt. Als men bijvoorbeeld bijzondere opsporingsmiddelen wil toepassen, dan bepaalt een officier van justitie of dit proportioneel is. Dat doe je, al naar gelang inbreuk op de privacy, samen met een rechter. En we beslissen of de zaak in het strafrecht opgepakt wordt. Soms is bestuursrecht beter. Of je doet beide een deel. Het OM streeft naar de inzet van strafrecht op die plekken waar de meerwaarde het grootst is. Wat je wil is dat strafbare feiten in de toekomst niet, of in ieder geval minder gebeuren. Het strafrecht kan ook signaleren en problemen agenderen. Als een rechter dan uiteindelijk een straf oplegt, dan zijn wij er verantwoordelijk voor dat deze ook wordt uitgevoerd."

WAT MAAKT HET VAK VAN LANDELIJK OFFICIER VOOR U BETEKENISVOL? "Dat het belangrijk is voor de maatschappij. Ik ben ooit belastingadviseur in de internationale adviespraktijk geweest en dat was vanuit juridisch oogpunt mooi werk. Maar ik vond het op een gegeven moment niet bevredigend meer. Ik vind dat we de laatste jaren echt zaken doen die er toe doen. We zoeken hierbij altijd naar afdoeningen die het meeste effect sorteren. Een transactie kan bijvoorbeeld effectiever zijn dan dagvaarden, omdat je dan als voorwaarde kan stellen dat een bedrijf eerst de compliance op orde stelt.

Je ziet het ook in de Wwft-aanpak (HK: Wet ter voorkoming van witwassen en financieren van terrorisme).

Sinds 2012 proberen we samen met de FIU en toezichthouders, poortwachters en bedrijven te bewegen om hun verplichtingen op grond van de Wwft na te komen. Alle signalen die we krijgen over het niet of niet op tijd melden van transacties of het niet doen van het verplichte cliëntenonderzoek, pakken we op. In het strafrecht of in het toezicht. We voeren samen de druk op. Naleving van de bestaande wet- en regelgeving is echt belangrijk voor de strijd tegen witwassen. En met resultaat. Het bedrijfsleven neemt haar compliancetaak steeds serieuzer."

DIT IS GOED NIEUWS VOOR NEDERLAND. MAAR GELD KENT GEEN GRENZEN. IS COMPLIANCE IN HET BUITENLAND EEN TOPIC? "Zeker, in 1989 ontstond de Financial Action Task Force. Amerika was toen volop bezig met haar 'war on drugs' en wilde het witwassen aanpakken. Dit kon niet zonder een internationale samenwerking en zo ontstond de FATF. Heel veel landen zijn hier lid van. Nederland ook. Landen beoordelen elkaar middels peer review op het invoeren van wetgeving die toeziet op compliance en witwasbestrijding. En dat niet alleen: ze beoordelen elkaar ook op effectiviteit van die wetgeving. Mocht je als land op een strafbankje terecht komen, dan is dat buitengewoon vervelend. In het ergste geval kunnen allerlei maatregelen worden opgelegd die het betalingsverkeer van en naar dat land kunnen belemmeren."

KUNT U UITLEGGEN HOE HET OPSPOREN IN DE PRAKTIJK WERKT? "Neem bijvoorbeeld de aanpak van verborgen vermogen in het buitenland. De opsporingsdiensten, het Openbaar Ministerie en de belastingdiensten hebben hierbij de handen ineen geslagen. De kans dat de belastingdienst verborgen buitenlands vermogen op het spoor komt, wordt daarom steeds groter. Dit komt door het structureel uitwisselen van data met buitenlandse overheden, door de gegevens die we via tipgevers en groepsverzoeken krijgen en door slimme gegevenskoppeling. Ook internationale samenwerking en de opheffing van het bankgeheim helpen ons hierbij. De Nederlandse belastingdienst beschikt ook over gegevens van betalingen die zijn gedaan met buitenlandse betaalkaarten. De belastingdienst controleert in het project Debet- en creditcards of de kaarten zijn gekoppeld aan vermogen in het buitenland en kijkt of belastingplichtigen dat vermogen ook hebben opgegeven bij de belastingdienst. Als ze dat niet hebben gedaan, kunnen ze bestuurlijk worden aangepakt. Maar ze maken ook kans om onderwerp te worden van een strafrechtelijk onderzoek."

HET OM WERKT SAMEN MET DE FIOD, DE FIU, EN TOEZICHTHOUDERS ALS BFT EN DNB AAN HET PROJECT NIET-MELDERS. WAT HOUDT DIT PROJECT IN? "In de Wwft zit een bepaling die de commissie Meldplicht instelt. Hier zitten Justitie en Financiën in, de toezichthouders, het OM, de FIOD en alle brancheorganisaties. Vanuit de laatste groep kwam het signaal dat ze hun leden wel voorlichten en opleiden, en hierbij soms zelfs tuchtrecht toepassen, maar dat er nog altijd beroepsbeoefenaars zijn die niet al hun verplichtingen nakomen. Dat levert concurrentievervalsing op. Bovendien doet het schade aan de integriteit van het financiële stelsel. We besloten daarop meer branchegericht te gaan werken. Denk hierbij aan autobedrijven, accountants of notarissen. Als deze mensen een loopje met de wet nemen, worden ze aantrekkelijk voor een bepaald soort klanten en dit wil je niet. Dus we hebben binnen het project afgesproken een keer per half jaar te vegen. Dit doen we dan met veel lawaai. Iedereen waarvan we weten dat die zijn verplichtingen niet is nagekomen, krijgt een bezoek van een toezichthouder of de belastingdienst. Hoe we daar achter komen? Laten we een vastgoedtransactie als voorbeeld nemen. De bank meldt bij de FIU dat het pand is betaald met een sporttas vol 500 eurobiljetten. En de notaris meldt helemaal niets. Als we in dat geval een aanwijzing hebben dat de Wwft niet goed is toegepast, dan zouden we wel eens een strafrechtelijk onderzoek kunnen openen.

Ik denk niet dat er altijd boze opzet in het spel is. De gemiddelde dienstverlener stapt 's ochtends niet op zijn fiets met de gedachte eens lekker te gaan witwassen of daarbij te helpen. Maar wat er wel gebeurt, is dat een meldplichtige zijn compliance niet goed op orde heeft, zijn klant niet goed wil kennen of een transactie niet goed of op tijd bij de FIU meldt. We hebben eens tientallen aanwijzingen van zaken waarin de Wwft niet goed was nageleefd, beetgepakt en ons hierbij afgevraagd: 'Wat zit er achter?'. Dan zie je dat bij circa 10% sprake is van iets groters en bij een derde van deze gevallen zelfs sprake is zware criminaliteit, zoals corruptie of vastgoedfraude."

NAAST HET PROJECT NIET-MELDERS ZIJN ER DE LAATSTE JAREN STEEDS MEER SPECIFIEK MULTIDISCIPLINAIRE ANTI-WITWASPROJECTEN? BIJVOORBEELD HET INTEGRALE AFPAKTEAM. WAT IS DAT? "Je kunt niet witwassen zonder, wat ik noem, het gronddelict. Bijvoorbeeld drugshandel, corruptie, beleggingsfraude. Dit levert geld op. Daar is het criminelen

vaak om te doen. Dat geld moeten ze ergens laten. Het Integrale Afpakteam is onderdeel van de teams die het gronddelict onderzoeken. Al in die eerste fase van onderzoek moeten zij onderzoeken waar het verdiende geld is gebleven. Er was natuurlijk al de Plukze-wetgeving, maar de laatste jaren hebben we er echt gas op gegeven. Je moet er zo snel bij zijn, want het geld is met één druk op de knop drie keer de wereld rond. Wij zitten samen met het AMLC van de FIOD vooral op projecten van onverklaarbaar vermogen, trade based money laundering en bijvoorbeeld internationale structuren waarbij de beneficial owner wordt verhuld. Er zijn mensen zonder inkomsten, maar wel met de mooiste huizen en de grootste auto's. Dan vragen we aan zo'n persoon: 'Hoe kan dat dan?' En als ze geen goede verklaring hebben, hebben wij een vermoeden van witwassen. Je ziet dan bijvoorbeeld dat dit soort mensen een onderneming hebben die feitelijk niets doet, maar waar ze wel inkomen uithalen, bijvoorbeeld een nagelstudio. Of ze krijgen een hypotheek uit een risicoland. Hier zie je ook dat mensen heel veel geld buiten Nederland hebben staan."

WERKEN DE PRIVATE SECTOR EN HET OM HIERBIJ MET ELKAAR SAMEN? EN KAN DIT BETER? "Het kan altijd beter. In Nederland doen we al veel maar we lopen tegen grenzen aan. Als je kijkt naar wat in het buitenland gebeurt, bijvoorbeeld in de UK, dan zie je dat daar meer initiatieven zijn die ook wat verder gaan. In Rotterdam liep het Finpro-project onder leiding van een hoogleraar van Nyenrode. In dat project werden de gegevens van private partijen op elkaar gelegd. Je ziet dan heel interessante patronen en veel fraude. De pilot was bedoeld om het debat aan te zwengelen over de vraag of het gebruik van big data bij criminaliteitsbestrijding verder ontwikkeld mag worden. We mogen in Nederland namelijk niet zomaar informatie plussen en delen. Er zijn veel wettelijke barrières. We gebruiken overheidsinformatie binnen de wettelijke mogelijkheden die er zijn. Ook banken mogen hun gegevens niet zomaar met elkaar koppelen. Ja, we leren wel van elkaar, maar echt in zaken samenwerken? Nee, dat gaat niet zomaar. Privacy- en geheimhoudingswetgeving verbieden veel. Je hoort regelmatig dat de compliance officer hier ook mee te maken heeft. Bank A weigert een klant en Bank B neemt hem bijvoorbeeld wel. Dat had voorkomen kunnen worden als Bank A de klantgegevens had mogen delen. Maar dat mag niet altijd. Privacy is natuurlijk belangrijk, het is een groot goed. Het is altijd zoeken naar de balans tussen twee belangrijke principes: recht op privacy en de waarheidsvinding. Er zitten een hoop kanten aan en ik denk ook dat het een politiek heet hangijzer is."

IS ER IN DE LOOP DER TIJD VEEL VERANDERD? "Er is, ook in het buitenland, meer aandacht voor compliance en er zijn nu veel meer meldplichtigen. Ook krijgen instellingen veel eerder te maken met een strafrechtelijke vervolging. Ook zie je dat instellingen beter en vaker melden. Onze wetgever zet er dan ook meer druk op. Iemand die in zijn beroep meewerkt aan witwassen kan acht jaar krijgen. En we hebben de Wwft. Als je vaker niet goed naar je klant kijkt, kan je maximaal vier jaar krijgen. En bedrijven kunnen boetes krijgen tot 10% van hun omzet."

EEN TRANSACTIE KAN EFFECTIEVER ZIJN DAN DAGVAARDEN, OMDAT JE DAN ALS VOORWAARDE KAN STELLEN DAT EEN BEDRIJF EERST DE COMPLIANCE OP ORDE STELT.

DIT GELDT VOOR DE STRAFMAAT. IS ER OP HET GEBIED OP OPSPORING VEEL VERANDERD? "Ja, er kan technisch meer. Op dit moment kunnen dataspecialisten met bits-en-bytes bepaalde processen in kaart brengen om te zien waar fraude plaatsvindt. We werken met indicatoren die duiden op witwassen. En dan krijgen we personen in beeld waarvan we het vermoeden hebben dat ze geld buiten het zicht van de autoriteiten houden. Door bijvoorbeeld onze goede samenwerking met de belastingdienst hebben we al veel zwartspaarders kunnen aanpakken."

BIJ HET PUBLIEK LEEFT HET GEVOEL DAT DE GEORGANISEERDE CRIMINALITEIT EN WITTEBOORDENCRIMINALITEIT VERDER TOENEMEN. IS DEZE PERCEPTIE TERECHT? "Ik weet niet of dit klopt. Het is ook een populair onderwerp in de media, dit versterkt het gevoel ook. In het NRA, National Risk Assesment, staat bijvoorbeeld dat georganiseerde misdaad in Nederland relatief weinig voorkomt. Maar aan de andere kant zien we in Zuid-Nederland wel een heel ander beeld. Wat we wel zien, en dat is omdat we minder naïef zijn geworden, is corruptie. We hebben lang gedacht dat dit in Nederland niet voorkwam. Dit is helaas niet zo."

ZIET U ANDERE TRENDS IN DE WITWASPRAKTIJK? "Nee, het zijn veelal dezelfde constante. Contant geld blijft er een. Het schuiven, over de grens brengen, wisselen of 'smurfen'. Dat is het bedragen opnemen waarmee je net onder de meldlimiet blijft. Wat je ook altijd ziet is de trustsector, die met ingewikkelde structuren de beneficial owner probeert te verhullen. Offshore-vennootschappen, dat is ook zo'n cluster dat er al jaren is. Net als Trade Based Money Laundering. Dat is omzet bijplussen of geld verschuiven in internationale handelstransacties. Maar denk hierbij ook aan de nagelstudio's in de stad waar je bijna nooit een klant ziet, maar wel voor inkomsten van de eigenaar zorgen. En de virtuele currencies moet ik ook noemen. Die zijn er al heel lang, maar je kan er nu veel meer mee doen. Er zijn nu ATM's waar je bitcoins kan omwisselen in contanten en andersom. In tegenstelling tot het buitenland is er in Nederland niet veel toezicht. Dat zie ik graag veranderd. We maken met de laatste Europese richtlijnen wel stappen in de goede richting. Ja, virtuele munten is nu een hot-topic, maar het is een kleine markt als je het vergelijkt met de trustsector. De trustsector in Nederland is goed voor 4000 miljard en voert voor circa 14.000 rechtspersonen het bestuur. Als je kijkt naar de Panama Papers, het grote geld zit echt in de hoek van de trustsector. Het is ook duidelijk een sector die hoog scoort op de risico's genoemd in het NRA."

WELKE BOODSCHAP ZOU U WILLEN MEEGEVEN AAN DE COMPLIANCE OFFICERS? "Ik geef wel eens presentaties en dan eindig ik altijd met een beeld van mannen in pak die hun hoofd in het zand steken. Het is de taak van de compliance officer ervoor te zorgen dat de mensen hun hoofd niet in het zand steken en het witwassen gewoon melden. De risico's voor de bedrijven zijn veel te groot. Zeker internationaal. Het tweede wat ik de compliance officer wil meegeven: zorg ervoor dat de mensen weten dat je er bent. Laat jezelf zien. Niet in een kamertje achteraf braaf je werk doen, maar iedereen in het bedrijf duidelijk maken dat het niet-melden van witwassen een criminele daad is en daarom echt niet kan."

DE LAATSTE JAREN HEBBEN WE ER ECHT GAS OP GEGEVEN. JE MOET ER ZO SNEL BIJ ZIJN, WANT HET GELD IS MET ÉÉN DRUK OP DE KNOP DRIE KEER DE WERELD ROND.

TECHNOLOGIE, CDD EN FINANCIEEL-ECONOMISCHE CRIMINALITEIT

JUDY VAN DER GRAAF

WAAR HET GAAT OM VOORKOMEN DAT MISBRUIK WORDT GEMAAKT VAN HET FINANCIËLE STELSEL IN DE VORM VAN FINANCIEEL-ECONOMISCHE CRIMINALITEIT (FEC), SPELEN TECHNOLOGISCHE TOEPASSINGEN EEN STEEDS GROTERE ROL.[1] OOK FINANCIËLE INSTELLINGEN PASSEN TECHNOLOGIE, ONDER DE NOEMER VAN REGULATORY TECHNOLOGY (REGTECH), IN TOENEMENDE MATE TOE IN PROCESSEN, GERICHT OM TE VOORKOMEN DAT ZIJ BETROKKEN RAKEN BIJ FEC.

In dit artikel wordt stilgestaan bij de voorwaarden waaronder RegTech op een zinvolle wijze door financiële instellingen kan worden toegepast in relatie tot de preventie van FEC.

AANTREKKINGSKRACHT VAN REGTECH

Het waarborgen van de integriteit van het financiële stelsel, met daarbij de aanpak van FEC mede via financiële instellingen, is de afgelopen decennia een belangrijk onderdeel geworden van een omvangrijk regelgevings- en toezichtklimaat. Financiële instellingen hebben een wettelijk verankerde poortwachtersfunctie om te voorkomen dat zij betrokken raken bij FEC. Onder andere de Wet op het financieel toezicht (Wft), de Pensioenwet, de Wet toezicht trustkantoren (Wtt), de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) en de Sanctiewet 1977 (Sw) bevatten verplichtingen voor financiële instellingen ten aanzien van het identificeren van risico's die zij lopen op het begaan of faciliteren van FEC en het nemen van maatregelen om deze risico's te mitigeren.

Het huidige regelgevings- en toezichtklimaat nodigt instellingen uit om initiatieven te ontplooien en te implementeren, om op efficiëntere en meer kostenbesparende wijze te voldoen aan regels. Met behulp van RegTech zien instellingen kansen om voortgang te boeken wat betreft mogelijkheden, snelheid en efficiëntie in het detecteren van FEC en om hierover te rapporteren. Daarnaast vormt de behoefte om nalevingskosten beter beheersbaar te maken een belangrijke reden voor de huidige aandacht voor RegTech.

Instellingen kunnen RegTech op verschillende terreinen toepassen. RegTech wordt in algemene zin gebruikt om te verwijzen naar technologische toepassingen voor het bewerkstelligen van compliance. Het is geenszins een nieuwe ontwikkeling, maar wel een die in de financiële sector een impuls heeft gekregen na de financiële crisis van 2007-2008, die geresulteerd heeft in toegenomen uitgaven aan compliance, waaronder aan de bestrijding van FEC. Zo zijn er RegTech-oplossingen die gericht zijn op het op zichzelf en geautomatiseerd identificeren van veranderingen

1 In dit artikel wordt de term financieel-economische criminaliteit gebruikt om te refereren aan vormen van criminaliteit die raken aan het financiële systeem doordat zij deze misbruiken voor oneigenlijke doelen en het plegen van een strafbaar feit. Te denken valt aan witwassen, corruptie (omkoping), financiering van terrorisme, handel met voorwetenschap, niet-naleven van sancties, verduistering, oplichting en valsheid in geschrifte (zie ook het factsheet van De Nederlandsche Bank 'De aanpak van financieel-economische criminaliteit').

in het regelgevend landschap. Of die gericht zijn op het voldoen aan rapportagevereisten uit prudentiële wet- en regelgeving, bijvoorbeeld ten behoeve van kapitaal- en liquiditeitseisen. In dit artikel ligt de nadruk echter op technologische toepassingen in de bestrijding van FEC. In het bijzonder wordt ingegaan op RegTech-initiatieven gericht op het beperken van kosten en kwetsbaarheden, in twee kernprocessen die cruciaal zijn in de bestrijding van FEC, namelijk het klantacceptatie- en transactie-monitoringsproces.

DE TOEKOMST VAN HET KLANTACCEPTATIE-PROCES

Het kennen van de klant is een cruciaal onderdeel van financiële dienstverlening. Waar dit voor instellingen lange tijd relatief eenvoudig was met veel persoonlijk contact, is dit onder invloed van economische, maatschappelijke én technologische ontwikkelingen in enkele decennia sterk veranderd. Consumenten verwachten steeds meer op afstand te kunnen doen. Naast het belang van het kennen van de klant voor de integere bedrijfsvoering van instellingen, is het specifieke belang voor het bestrijden van FEC, steeds meer op de voorgrond gekomen en geformaliseerd als vereiste in financiële wet- en regelgeving.

In het klantacceptatieproces is het noodzakelijk om informatie uit verschillende bronnen te raadplegen en te analyseren, om onder andere de identiteit van een zakelijke relatie en uiteindelijk belanghebbende vast te stellen, en de identiteit van een relatie en uiteindelijk belanghebbende te verifiëren. Met name in complexe gevallen, bijvoorbeeld bij potentiële klanten die actief zijn in meerdere jurisdicties, vormt klantacceptatie een intensief proces. Het opvragen van documenten, gegevens of informatie, het controleren van de juistheid hiervan en het vastleggen van verkregen gegevens, kost veel tijd. Dit is dan ook de reden dat instellingen inventariseren welke technologische vernieuwingen er zijn in het klantacceptatieproces en hiermee experimenteren.

Instellingen, al dan niet individueel of gezamenlijk, zijn in toenemende mate op zoek naar efficiëntere manieren van datavergaring en verificatie van deze data door deze naast data uit andere bronnen te leggen. Externe partijen die data uit verschillende bronnen aggregeren en deze op een centrale plek aanbieden voor het uitvoeren van klantonderzoeken, worden daarbij steeds vaker gezien als de weg vooruit. Op de langere termijn kan distributed ledger-technologie, met blockchain als belangrijkste verschijningsvorm, een belangrijke rol gaan spelen in het samenbrengen van zogenaamde ‘know-your-customer’-

data. Met behulp van distributed ledger-technologie kan data in een gezamenlijk netwerk worden bijgehouden door verschillende partijen, waaronder mogelijkerwijs publieke instanties als belastingautoriteiten en toezichthouders.

Belangrijke vragen bij het gebruiken van een uniforme infrastructuur met decentrale opslag van data zijn wel hoe data wordt gevalideerd en wie de toegang tot bepaalde data bepaalt, bijvoorbeeld in geval van het klantacceptatie-proces. Andere technieken die in het klantacceptatieproces worden onderzocht hebben betrekking op biometrische technieken. Deze technieken kunnen in het bijzonder een rol gaan spelen bij identificatie en verificatie, doordat dit gemakkelijker op afstand kan plaatsvinden met methoden die in andere domeinen, zoals binnenlandse veiligheid, reeds worden toegepast in de vorm van gezichts-, stem-, vingerafdruk- en irisherkenning.

Huidige klantacceptatieprocessen leunen sterk op documentatie voor identificatie en verificatie, maar met de toepassing van biometrie zou het klantacceptatieproces kunnen opschuiven naar identificatie en verificatie (mede) op basis van unieke biologische kenmerken die meer betrouwbaar en minder fraudegevoelig zijn. Naar aanleiding van identificatie en verificatie met biometrie, zou ook het gebruik van digitale identiteit een rol kunnen gaan spelen. Door het ontstaan van een digitale identiteit is het proces van identificatie en verificatie op termijn wellicht slechts eenmalig noodzakelijk. De eerste eenmalige identificatie en verificatie weegt daarbij nog zwaarder en de vraag is ook welke partij hiervoor dan verantwoordelijk is en de kosten en risico's zal dragen.

TRANSACTIEMONITORING EN KUNSTMATIGE INTELLIGENTIE

Zodra een klantrelatie tot stand is gekomen, vormt het monitoren van de activiteiten en transacties van de klant en het melden van ongebruikelijke transacties bij de Financial Intelligence Unit (FIU) een cruciaal proces in het voorkomen van FEC. Monitoring kan op verschillende wijzen worden ingericht, bijvoorbeeld in de vorm van gerichte controles op bepaalde rekeningen of bij bepaalde transacties, of in de vorm van handmatige monitoring. Een belangrijke plek binnen financiële instellingen wordt echter ingenomen door transactiemonitoringssystemen. Deze systemen genereren automatisch een alert indien er bepaalde, ongebruikelijke transacties of patronen in transacties plaatsvinden. Detectieregels, of business rules, met daarin scenario's en grenswaarden, filteren in een transactiemonitorings-systeem ongebruikelijke transacties uit de miljoenen transacties die dagelijks plaatsvinden bij de grotere instellingen. Instellingen worden daarbij nog veelvuldig geconfronteerd met 'false positives' en blijven kwetsbaar voor 'false negatives'.

Om het proces van transactiemonitoring efficiënter te maken, hebben instellingen de afgelopen jaren steeds meer werk gemaakt van intelligente transactiemonitoring, waarbij een transactieprofiel van een klant wordt opgesteld waartegen iedere nieuwe transactie wordt getoetst. Transacties die buiten het verwachte patroon vallen, worden nader onderzocht om na te gaan of deze als ongebruikelijk dienen te worden aangemerkt en te worden gemeld aan de FIU. In een intelligent transactiemonitoringssysteem wordt door instellingen ook geëxperimenteerd met kunstmatige intelligentie, met als doel de aanscherping van detectie-regels. Op allerlei terreinen wordt kunstmatige intelligentie toegepast, waarbij innovatieve, (zelf)lerende computers in staat zijn te reageren op allerlei data en gedragingen. Op basis daarvan kunnen deze computers taken zelfstandig uitvoeren en beslissingen nemen.

Toegepast in de wereld van transactiemonitoring kan met behulp van kunstmatige intelligentie een detectiesysteem worden ingericht dat zelf kan leren bepaalde afwijkende alsook nieuwe, ongebruikelijke patronen te ontdekken en voorspellen. Daarmee kan met kunstmatige intelligentie in een veel grotere dataset worden gezocht naar verbanden die niet direct of helemaal niet duidelijk zichtbaar zouden worden wanneer enkel onderzoek plaatsvindt vanuit een menselijk oog. Transactiemonitoring met behulp van kunstmatige intelligentie is voor nu vooral nog iets waarmee financiele instellingen experimenteren.

MET NAME IN COMPLEXE GEVALLEN VORMT KLANTACCEPTATIE EEN INTENSIEF PROCES.

Bovendien zal het ook niet direct voor alle instellingen een relevante ontwikkeling zijn. Afhankelijk van de dienstverlening, de omvang van het aantal transacties en het type cliënten, zal de rol van geavanceerde transactiemonitoring-technieken meer of minder relevant zijn.

RISICO'S ROND DE TOEPASSING VAN REGTECH IN DE BESTRIJDING VAN FEC

Onbedoelde neveneffecten zijn, waar het gaat om risico's en de beheersing ervan, veelbesproken onderwerpen. Voor wat betreft de mogelijkheden van RegTech om verbeteringen te bewerkstellingen in de beheersing van risico's op FEC, geldt eveneens dat technologische toepassingen in zichzelf ook weer risico's met zich meebrengen. Eén van deze risico's betreft het risico dat het toenemende gebruik van technologie, instellingen juist ook weer kwetsbaar maakt voor misbruik. Het gebruik van RegTech-toepassingen kan FEC uitlokken, bijvoorbeeld waar oplossingen gericht zijn op het bij elkaar brengen en opslaan van grote hoeveelheden klantdata, zoals hierboven besproken. Deze, veelal privacygevoelige, bij elkaar gebrachte data zal eveneens een aantrekkelijke bron zijn voor misbruik voor criminele doeleinden.

Een ander risico van RegTech is gelegen in de mate waarin instellingen zich tot op zekere hoogte afhankelijk maken van derde partijen voor de beheersing van risico's op FEC. Waar instellingen er regelmatig voor kiezen zelf onderzoek te doen naar RegTech-oplossingen en het bouwen van applicaties en toepassingen, is het voor instellingen ook aantrekkelijk om een beroep te doen op een externe partij met reeds aanwezige, gespecialiseerde technologische kennis en middelen. RegTech-ontwikkelingen hebben inmiddels geleid tot een hele industrie van dienstverleners gespecialiseerd op dit terrein. Daarbij krijgen deze dienstverleners toegang tot gevoelige data, zowel van de instellingen zelf als die van hun klanten. Hoe hierbij wordt omgegaan met privacy is een cruciaal punt.

Het beheersen van risico's komt met het gebruiken van een externe partij meer op afstand van de instelling te staan. Ook bij uitbesteding aan een gespecialiseerd RegTech-bedrijf, blijft de verantwoordelijkheid voor het beheersen van aan FEC gerelateerde risico's bij de instelling zelf. Wanneer het almaar wenselijker wordt geacht om technologie toe te passen, zullen instellingen zich moeten afvragen of dit ook niet tevens gepaard dient te gaan met de nodige investeringen om zelf kennis over technologische toepassingen in huis te halen. Of om ten minste de technologie en de processen van de geboden oplossingen van RegTech-dienstverleners te begrijpen en te toetsen met een belangrijke rol voor compliance en audit.

Daarnaast zullen vraagstukken aangaande verantwoordelijkheid en aansprakelijkheid met het gebruik van technologie de komende jaren steeds prominenter worden daar waar instellingen ervoor kiezen gezamenlijk op te trekken in het vergaren en delen van data. Vooral wanneer hierbij op termijn distributed ledger-technologie een rol zou gaan spelen en geen centrale partij meer de controle heeft, rijst de vraag wie verantwoordelijk is voor waarborgen omtrent de vergaring, kwaliteit en opslag van data en bij bijvoorbeeld misbruik door criminelen.

Vragen over verantwoordelijkheid en aansprakelijkheid spelen ook ten aanzien van kunstmatige intelligentie, zoals bijvoorbeeld toegepast in het hiervoor beschreven voorbeeld van transactiemonitoringsystemen. Het uitvoeren van transactiemonitoring met behulp van lerende algoritmes kan naast efficiëntie ook grote risico's met zich meebrengen. Bij een verkeerd algoritme – bijvoorbeeld een algoritme opgesteld met een bepaalde 'bias', waardoor ongebruikelijke transacties niet worden gedetecteerd ('false negatives') – zijn de gevolgen vele malen groter dan in een systeem zonder zelflerende algoritmes. De effectiviteit, functionaliteit

HET HUIDIGE REGELGEVINGS- EN TOEZICHTKLIMAAT NODIGT INSTELLINGEN UIT OM OP EFFICIËNTE EN KOSTENBESPARENDE WIJZE TE VOLDOEN AAN REGELS.

en betrouwbaarheid van algoritmes zal constant aandacht vragen.

Hierbij zal ook meer en meer de vraag naar voren komen hoe instellingen om zullen gaan met het veiligstellen van de integriteit van technologische toepassingen. Waakzaamheid voor mogelijke onbedoelde neveneffecten zal van groot belang zijn bij de ontwikkelingen op het terrein van RegTech. Uit deze korte schets van mogelijke risico's, wordt evident dat mensen nodig blijven voor monitoring en daarmee mensen met kennis van technologische ontwikkelingen. De compliance officer zal hierbij binnen instellingen een essentiële rol moeten vervullen door het stellen van kritische vragen bij de ontwikkeling van nieuwe initiatieven.

VOORWAARDEN VOOR DE TOEPASSING VAN REGTECH

Om de risico's rond het gebruiken van technologische oplossingen naar de toekomst toe zoveel mogelijk te beperken, kan er gedacht worden over een aantal voorwaarden waaraan moet worden voldaan alvorens de toepassing van RegTech kan plaatsvinden. Vanzelfsprekend zal voor instellingen voorop staan dat RegTech-oplossingen daadwerkelijk efficiënt zijn en zoveel mogelijk kostenbesparend in het voorkomen van betrokkenheid bij FEC. Daarnaast valt echter te denken aan een aantal andere elementen. Nieuwe technologieën zullen bijvoorbeeld uitgebreid getest moeten worden voordat deze worden ingebed in processen, waarbij deze tests niet alleen zien op de effectiviteit, maar ook op het beperken van mogelijke onbedoelde neveneffecten van technologische toepassingen.

Tevens zal bij gebruik van gespecialiseerde RegTech-dienstverleners, due diligence op deze bedrijven in het bijzonder van belang zijn, alsmede het inregelen van zekerheden – onder andere op het gebied van data-veiligheid. Een andere kernvoorwaarde voor het gebruiken van RegTech-toepassingen, of deze nu door instellingen zelf worden ontwikkeld of door externe partijen, is dat er transparantie dient te bestaan over de keuzes die worden gemaakt in het ontwikkelen van de achterliggende technologie van RegTech-oplossingen. Instellingen zullen moeten waken over de integriteit van de door hun gebruikte technologie. Zo moet technologie dat doel dienen waar het ook voor is bedoeld. Al met al gaat het gebruiken van technologie verder dan weten of het betrouwbaar is en werkt, het gaat ook over integriteit. In dit vroege stadium van verkenningen in de mogelijkheden van RegTech is daarom vereist dat medewerkers, waaronder compliance professionals, kennis hebben van technologie.

CONCLUSIE

De mate waarin technologische ontwikkelingen impact zullen hebben op het terrein van de beheersing van risico's ten aanzien van FEC, zal de komende jaren steeds duidelijker worden. De vraag is niet zozeer of, maar veel meer hoe en in welke mate RegTech een verschil zal kunnen maken in risicobeheersing en compliance. In combinatie met betrokkenheid van compliance professionals kan RegTech ertoe leiden dat technologische oplossingen bijdragen aan een efficiënte bestrijding van FEC, zonder dat hierbij de veiligheid, betrouwbaarheid, effectiviteit en integriteit van het financiële systeem wordt geschaad.

Dr. J.S. (Judy) van der Graaf is werkzaam bij De Nederlandsche Bank (DNB) in het toezicht op financieel-economische criminaliteit. In haar rol bij DNB is Judy betrokken bij cross-sectorale onderzoeken op uiteenlopende terreinen van de financiële toezichtwetgeving rond integriteit.

Dit artikel is afgeleid van het artikel 'De toepassing van technologie in het klantacceptatie- en transactiemonitorings-proces ter bestrijding van financieel-economische criminaliteit' uit het Jaarboek Compliance 2018, Nederlands Compliance Instituut, Capelle aan den IJssel, ISBN 978-94-91252-28-0.

Aanvullende leestip: 'De invloed van FinTech en de verwerking in de systematische integriteitrisicoanalyse', drs. R.M.L. (Roderick) Noordhoek, Jaarboek Compliance 2018.

DE HOOFDPUNTEN VAN HET WETSVOORSTEL WWFT 2018

THAI HA VU

Voor de Vierde Europese Anti-witwasrichtlijn, die op 26 juni 2017 in nationale wet- en regelgeving geïmplementeerd diende te zijn, is op 13 oktober 2017 het wetsvoorstel ter implementatie in de Wet ter voorkoming van witwassen en financiering van terrorisme (Wwft) bij de Tweede Kamer ingediend. Uit de Vierde Anti-witwasrichtlijn blijven twee kernverplichtingen staan, namelijk de verplichting om een cliëntonderzoek te verrichten en de verplichting om ongebruikelijke transacties te melden bij de FIU. Hieronder hebben we de belangrijkste aandachtspunten voor u op een rij gezet.

HET WETSVOORSTEL BRENGT DE VOLGENDE WIJZIGINGEN VOOR DE WWFT MEE:

1. Uitbreiding reikwijdte

Het toepassingsbereik van de Wwft wordt uitgebreid en zal ook van toepassing zijn op aanbieders van kansspelen[1] en grootwaardehandelaren[2].

2. Risicogebaseerde aanpak

Zowel de Europese Commissie als lidstaten zijn verplicht tot het opstellen van een risicobeoordeling, welke als basis zal worden gebruikt voor beleid en wetgeving inzake voorkoming van witwassen en financiering van terrorisme. Instellingen en meldingsplichtige entiteiten zijn verplicht om hun risicobeoordeling op witwassen en financiering van terrorisme op te stellen en vast te leggen, in lijn met de hun interne gedragslijn en procedures. Tevens dienen de risicobeoordelingen actueel te worden gehouden en op verzoek te kunnen worden verstrekt aan de toezicht houdende autoriteiten.

3. Cliëntenonderzoek

Meldingsplichtige instellingen moeten een cliëntenonderzoek verrichten dat gebaseerd is op het risiconiveau. Er dient een onderzoek te worden verricht naar de cliënt, de achtergrond en het doel van de beoogde zakelijke relatie of transactie. De risico's die hieruit voortvloeien, bepalen de intensiteit van de onderzoeksmaatregelen. Een meldingsplichtige instelling is vrij om zelf de intensiteit van de maatregelen te bepalen.

Een vereenvoudigd cliëntenonderzoek volstaat in geval van een bewezen laag risico. Een verscherpt cliëntenonderzoek is vereist in een hoogrisicogeval. Bij een hoog risico dient een meldingsplichtige instelling meer gegevens te verzamelen en te controleren, bijvoorbeeld in de situatie waarbij een cliënt woonachtig of gevestigd is in een hoogrisicojurisdictie of waarbij sprake is van een correspondentrelatie.[3] Daarnaast dient de instelling de identiteit van de UBO vast te stellen en dient zij na te gaan of er sprake is van een PEP. Verscherpte onderzoeksmaatregelen zijn vereist:

- in gevallen van transacties of zakelijke relaties met een cliënt die als PEP kwalificeert; of
- wanneer de UBO van een cliënt als een PEP kwalificeert; of
- waarbij de begunstigde van een levensverzekering of waarbij de UBO van de begunstigde een PEP is.

1 Speelcasino's en overige kansspelaanbieders, waaronder loterijen, aanbieders van sportweddenschappen en speelautomatenhallen.

2 Personen die beroeps- of bedrijfsmatig in goederen handelen in het geval daarbij contante betalingen worden gedaan of ontvangen van EUR 10.000 of meer en kopers van goederen (naast de verkopers).

3 In geval van een correspondentrelatie treedt een bank of andere financiële onderneming in feite op als agent voor een andere bank of financiële onderneming (de respondentinstelling). In deze gevallen worden diensten verleend ten behoeve van een cliënt van de respondentinstelling.

Met het nieuwe wetsvoorstel wordt de definitie van UBO aangepast in lijn met de FATF-aanbevelingen. De instelling dient in ieder geval in het cliëntenonderzoek de UBO vast te stellen en te verifiëren.
Daarnaast wordt met het nieuwe wetsvoorstel geen onderscheid meer gemaakt tussen binnenlandse en buitenlandse PEP's. Dit heeft als gevolg dat hierdoor meer verscherpt cliëntenonderzoek moet worden verricht.

4. UBO-definitie

De UBO-definitie gaat beter aansluiten bij die van de FATF. Zo kan er sprake zijn van een UBO wanneer deze een percentage van de aandelen of stemrechten houdt. Daarnaast kan een natuurlijke persoon ook een UBO zijn via indirect eigendom. Tevens kan een of meerdere personen tot hoger leidinggevend personeel als UBO aan te wijzen zijn. De definitie voor UBO in de trustsector is eveneens opgenomen.

5. Centraal register voor lidstaten – internationale aanpak

Met de Vierde Anti-witwasrichtlijn wordt er een internationale aanpak gestreefd, waardoor lidstaten verplicht worden gesteld om een centraal register bij te houden. Via dit register kan informatie en kunnen gegevens worden gedeeld tussen financiële inlichtingeneenheden uit verschillende lidstaten. De informatie kan betrekking hebben op UBO's en andere juridische entiteiten. Het ziet ook toe op express trusts, juridische constructies, bijkantoren, meerderheidsdochterondernemingen, etc.

6. Handhavingsinstrumentarium toezicht houdende autoriteiten

Lidstaten dienen ervoor te zorgen dat de bepalingen van de Vierde Anti-witwasrichtlijn worden nageleefd. Toezicht houdende autoriteiten krijgen de bevoegdheid toegekend in doeltreffende, evenredige en afschrikkende bestuurlijke sancties en maatregelen. De toezicht houdende autoriteit heeft een boetebevoegdheid om voldoende af te schrikken. De hoogte van de boete is afhankelijk van de ernst en duur van de overtreding, de verwijtbaarheid van de overtreder, het evenredigheidsbeginsel en de draagkracht van de overtreder. Naast een omzet gerelateerde boete opleggen, heeft de toezicht houdende autoriteit ook de bevoegdheid om een vergunning van de instelling in te trekken.

7. Publicatiebevoegdheden toezicht houdende autoriteiten

Met het wetsvoorstel is het vereist voor toezicht houdende autoriteiten dat zij alle besluiten openbaar maken in geval een bestuurlijke boete of maatregel is opgelegd bij overtreding van de Wwft. De toezicht houdende autoriteit heeft ook de bevoegdheid om een waarschuwing of een publieke verklaring uit te vaardigen in geval van een overtreding. Dit zal gaan om overtredingen in de tweede en derde categorie. Het publiek kan kennis nemen van overtreding en de gronden daarvoor. Een ander effect van openbaarmaking kan zijn dat andere instellingen de verklaringen lezen en hieruit gedragingen afleiden waardoor overtreding van de Wwft wordt ontmoedigd. Zelfs wanneer een bestuurlijke boete nog niet onherroepelijk is geworden, kan de toezicht houdende autoriteit deze informatie openbaar maken. Hierbij dient het opleggen van een last onder dwangsom wel verbeurd te zijn.

8. Gegevensbescherming

In het kader van het cliëntenonderzoek onder de Wwft worden er persoonsgegevens verwerkt. Zonder verwerking van persoonsgegevens zou het niet effectief zijn om witwassen en financiering van terrorisme te bestrijden. Zo wordt er o.a. informatie verwerkt over de identiteit van de cliënt, het doel en de aard van de zakelijke relatie, incidentele transacties dan wel dienst van de UBO. Ondanks dat het voorkomen van witwassen en financiering van terrorisme een zwaarwegend belang is, mogen er niet meer persoonsgegevens verwerkt worden dan noodzakelijk is voor de naleving van de verplichtingen van Vierde Anti-witwasrichtlijn. Instellingen worden verplicht om informatie die zij verzamelen en verwerven uit een cliëntenonderzoek en monitoringsonderzoek, voor opsporing- en onderzoeksdoeleinden voor een periode van vijf jaar te bewaren na beëindiging van de zakelijke relatie of het uitvoeren van een transactie.
De FIU krijgt de bevoegdheid om gegevens en inlichtingen over een bepaalde cliënt of transactie op te vragen aan alle instellingen in verband met de taakuitoefening van de FIU. Dit gaat nog breder dan enkel de instellingen die zelf een melding hebben gedaan.
De toezicht houdende autoriteit moet bij publicatiebevoegdheden ook rekening houden of het geen onevenredige gevolgen heeft voor de overtreder. In dat geval kan een bestuurlijke sanctie geanonimiseerd worden gepubliceerd of op een ander moment worden gepubliceerd.
Een toezicht houdende autoriteit is in ieder geval gehouden aan dat inmenging in de persoonlijke levenssfeer dient te worden beperkt en ongerechtvaardigde inmenging moet worden voorkomen. In geval van publicatie van een besluit, dient de toezicht houdende autoriteit alvorens betrokkene daarvan op de hoogte te stellen.

Thai Ha Vu is compliance officer bij het Nederlands Compliance Instituut.

EEN EFFECTIEF BELEID TEGEN TERRORISME-FINANCIERING: TIJD VOOR EEN EERLIJK GESPREK

MARA WESSELING

Afgelopen zomer verscheen in het blad *Foreign Affairs* een veel besproken artikel over de falende strijd tegen terrorisme-financiering. De auteur, Peter Neumann, stelt dat er meer dan vijftien jaar na 9/11 meer terroristische organisaties zijn en dat terroristische organisaties over meer geld beschikken dan ooit tevoren.

Ook al zouden de genomen maatregelen het terroristen moeilijker hebben gemaakt om toegang te verkrijgen tot de internationale financiële sector, een terroristische aanslag is er, in zijn woorden, niet mee voorkomen. Soortgelijke geluiden klonken er in november op een conferentie van het *Centre for Financial Crime and Security Studies* in Londen. Vertegenwoordigers van zowel grootbanken als internationale opsporingsdiensten leken het eens te zijn dat de huidige aanpak onvoldoende effectief was en het tijd was voor Combatting the Financing of Terrorism (CFT) 2.0. Hoewel deze geluiden zeker niet nieuw zijn, lijkt er momenteel meer oor voor te zijn en klinkt de roep om verandering luider. Dit artikel zal ingaan op de effectiviteit van de strijd tegen terrorismefinanciering. Waarom is het detecteren van terrorismefinanciering zo complex? Waarom is de effectiviteit van de maatregelen zo moeilijk vast te stellen? En hebben we wel de juiste verwachtingen van wat de strijd tegen terrorismefinanciering kan en zou moeten opleveren?

DETECTEREN IN HET DUISTER

Na de aanslagen van 9/11 is de bestrijding van terrorisme-financiering in het anti-witwasraamwerk opgenomen. De tegoeden van de van terrorisme verdachte individuen en organisaties moesten worden bevroren, de KYC- en CDD-verplichtingen alsmede het aantal meldplichtige instellingen zijn uitgebreid en nieuwe opsporingsmethoden zijn ontwikkeld. Er bleek echter al vrij snel dat de logica achter de aanpak van witwassen niet zondermeer toepasbaar is op het fenomeen terrorismefinanciering. Bij het bestrijden van witwassen is het hoofddoel het detecteren van transacties die de herkomst van de winst uit al gepleegde misdaden dient te verhullen. Bij het preventief detecteren van terrorismefinanciering zoekt men daarentegen naar aanwijzingen voor de intentie van het plegen van een misdaad in de toekomst. Hoewel er voorbeelden zijn van terroristische organisaties die ook zijn betrokken bij witwaspraktijken, is het voor de financiering van een aanslag niet nodig om veel kapitaal te verwerven middels ingewikkelde financiële constructies. In de praktijk bleek het lastig om typologieën en profielen te ontwerpen om terrorismefinanciering preventief te detecteren en deze leverden nauwelijks relevante hits op. Hier zijn verschillende redenen voor.

De eerste is methodologisch van aard. Een van de centrale aannames van het CFT-beleid is dat terrorismefinanciering gepaard gaat met afwijkend financieel gedrag dat als 'ongebruikelijk' of 'verdacht' kan worden aangemerkt. Het is echter lastig patronen te ontdekken met betrekking tot de financiering van terroristische groepen en aanslagen. Statistisch gezien is (gelukkig) het aantal aan terrorisme-

financiering gerelateerde transacties op het totaal van alle transacties heel erg laag. Daarnaast financieren terroristen zich vaker zelf met beperkte, en op het oog legale middelen (salaris, uitkeringen, spaargeld, krediet). Als er geen specifieke verdenking is, zal dit soort transacties niet opvallen als ongebruikelijk en detecteert men in het duister. Verder financieren terroristen zich veelal op opportunistische wijze met de middelen die zij voor handen hebben. De bestudering van recente terroristische aanslagen laat zien dat er een breed palet aan inkomstenbronnen is gebruikt en transacties zowel binnen, maar zeker ook buiten de formele financiële sector plaatsvinden. Het is voor banken en andere meldplichtige instellingen dus lastig om volledig beeld van een transactie of klant te krijgen. Het behoeft hier overigens te zeggen dat er de afgelopen jaren wel enig succes is bereikt met het detecteren van zogenaamde uitreizigers naar Syrië en Irak. Ook zijn er nationaal en internationaal nieuwe initiatieven gestart waarbij publieke en private partijen samenkomen en meer specifieke informatie en ook namen delen om terrorismefinanciering effectiever op te sporen. Een Nederlands voorbeeld is de Task Force Terrorisme Financiering, een pilot waarin vijf private en vier publieke partijen samenwerken. Vergelijkbare initiatieven zijn 'the Consortium' in de Verenigde Staten en de 'Joint Money Laundering Intelligence Taskforce' (JMLIT) in het Verenigd Koninkrijk.

Ten tweede is het maken van typologieën zo lastig omdat de terroristische dreiging en de financieringsmethoden continue veranderen, zowel als reactie op ingevoerde regelgeving als door de geopolitieke realiteit en financieel technische innovaties. Terroristische aanslagen zijn goedkoop en door de jaren heen steeds goedkoper geworden. De afgelopen vijftien jaar lagen de geschatte kosten van aanslagen in Europa onder de € 10.000. De enige uitzonderingen waren de aanslagen van 13 november 2015 in Parijs. Afhankelijk van wat men wel en niet meetelt, zijn de kosten van deze aanslagen geschat tussen € 30.000 en € 82.000. Kijkt men naar de recente aanslagen met messen, vuurwapens en/of voertuigen – zoals op de kerstmarkt van Berlijn, op de Promenade des Anglais in Nice of op de Ramblas in Barcelona – dan zijn de kosten nagenoeg verwaarloosbaar.

Wat betreft financieringsmethoden ziet men bijvoorbeeld een verschuiving in het belang van internationale giften. In 2001 werden deze als een van de belangrijkste geldbronnen achter Al Qaida en de aanslagen van 9/11 gezien, terwijl

HOEWEL ER SINDS 9/11 WERELDWIJD TEGOEDEN ZIJN BEVROREN, BLEEK HET NIET HET EINDE VAN HET TERRORISME.

HET BEVRIEZEN VAN TEGOEDEN, NOCH HET PREVENTIEF DETECTEREN VAN VERDACHTE KLANTEN EN TRANSACTIES BLEEK HET ULTIEME PANACEE.

deze maar een klein percentage van het totale budget van IS vormden. Nu IS een groot deel van haar territorium en de daaruit voortkomende inkomsten kwijt is, zullen de overgebleven strijders nieuwe manieren zoeken om geld te stallen en nieuwe inkomsten te genereren. Het vermoeden is dat de organisatie mobieler en meer verspreid zal gaan opereren en dat het delen van haar (cash)vermogen investeert op verschillende aandelenmarkten in het Midden-Oosten en in de aankoop van ondernemingen.[1]

MET WELK MEETLINT METEN?

In 2016 stelde DNB als toezichthouder naar aanleiding van haar themaonderzoek inzake transactiemonitoring vast dat de uitvoering van de Wwft bij veel banken zorgelijk is en de nodige verbetering behoeft.[2] Daarna heeft de sector door een verhoogd bewustzijn en het aanscherpen van haar compliancebeleid, significant meer meldingen met de verdenking van terrorismefinanciering gedaan aan de FIU-NL.[3] In andere woorden: het toezicht van DNB heeft geleid tot een meer specifieke en op maat gemaakte uitvoering van de Wwft op het gebied van terrorismefinanciering. De bredere vraag of de Wwft (of het FATF-raamwerk) effect heeft op de financiering van terroristische aanslagen en organisaties, is moeilijk eenduidig vast te stellen. Om deze vraag te bestuderen helpt het om onderscheid te maken tussen 'output effectiveness', 'outcome effectiveness' en 'impact effectiveness'.

Output effectiveness heeft betrekking op het ontwikkelen van beleidsinstrumenten en compliancemechanismes en op het implementeren van beleid. Met andere woorden: de vraag of er uitvoering wordt gegeven aan de wettelijke vereisten. Het beoordelen van output effectiveness wordt vaak gezien als het beoordelen van een papieren werkelijkheid en een 'tick the box'-oefening. Het beleid, de procedures en de tools kunnen immers op papier bestaan, maar dit zegt weinig over de uitvoering. Wordt het beleid actief, volledig en doordacht uitgevoerd? Is de risicoanalyse bijvoorbeeld goed toegespitst op het profiel van de klanten, de aangeboden diensten en producten en de landen waarmee de meldplichtige entiteit zakendoet?

In eerste instantie beoordeelden toezichthouders en internationale organisaties zoals de FATF in hun evaluaties vooral de output effectiveness. De laatste jaren is er echter veel meer aandacht gekomen voor *outcome effectiveness*. Dit houdt in dat er ook gekeken wordt naar de uitvoering van beleid in de dagelijkse praktijk. Indicatoren voor outcome effectiveness zijn bijvoorbeeld aantallen gemelde ongebruikelijke transacties, aantallen hits op de terroristenlijst, bevroren tegoeden, aantallen vervolgingen voor terrorismefinanciering. Ook kan men steekproefsgewijs nagaan waarom in specifieke gevallen bepaalde besluiten genomen zijn en of dit in overeenstemming is met het interne beleid en de geldende wetgeving. Hoewel deze aanpak probeert om de papieren werkelijkheid te ontstijgen, is het vaak een uitdaging om relevante indicatoren te vinden en deze goed te interpreteren. Is het melden van veel ongebruikelijke transacties teken van een robuust beleid of van defensief rapporteren? Komt het niet-melden van hits op de verschillende terrorismelijsten doordat men niet goed checkt of doordat er geen matches zijn? En welk verband is er tussen de aantallen gemelde, ongebruikelijke transacties of geweigerde klanten en de mate waarin terrorismefinanciering plaatsvindt?

Deze laatste vraag is waar *impact effectiveness* zich op richt: de effecten van het CFT-beleid in relatie tot de langetermijn-

1 Europees Parlement (2017) The Financing of the 'Islamic State' in Irak and Syria (ISIS), in-depth analysis for the Directorate-General for External Policies, september 2017, zie: www.europarl.europa.eu/RegData/etudes/IDAN/2017/603835/EXPO_IDA(2017)603835_EN.pdf.

2 DNB (2016) Nieuwsbericht: Transactiemonitoring behoeft verbetering, 31 Augustus 2016, zie: www.dnb.nl/nieuws/dnb-nieuwsbrieven/nieuwsbrief-banken/nieuwsbrief-banken-augustus-2016/dnb345504.jsp.

3 FIU-Nederland (2017) Nieuws: 4,6 miljard aan verdachte transacties: banken en geldkantoren melden steeds meer ongebruikelijke geldstromen, 26 mei 2017, zie: www.fiu-nederland.nl/nl/46-miljard-aan-verdachte-transacties.

doelstellingen van het CFT en het CT-beleid. Het aantonen van causaliteit tussen enerzijds specifiek beleid en anderzijds het stoppen of inperken van terrorismefinanciering is echter complex en problematisch. Wat is bijvoorbeeld de maatstaf voor succes in het terugdringen van terrorismefinanciering: minder aanslagen, minder slachtoffers, meer vervolgingen of bevroren tegoeden? Het wordt nog lastiger – maar zeker niet minder relevant – als men ook de negatieve effecten van CFT-wetgeving op de private sector (o.a. de kosten), bepaalde internationale goede doelen, bedrijfssectoren en migranten (de-risking, de-banking) in de evaluatie mee wil nemen.

GEPASTE VERWACHTINGEN

Uit het bovenstaande zou men kunnen concluderen dat de opsporing van terrorismefinanciering door banken en andere meldergroepen veel inzet vraagt en de opbrengst daarvan grotendeels beperkt is of onmeetbaar blijft. Dit beeld ontstaat doordat – zoals ook Neumann doet – geprobeerd wordt een direct verband aan te tonen tussen de geleverde inspanningen en het effect daarvan op terrorisme(financiering). De vraag of het bestrijden van terrorismefinanciering effectief is, kan echter ook op een andere manier worden beantwoord: de verwachtingen van het beleid duidelijker te definiëren.

In eerste instantie zette de internationale gemeenschap na 9/11 in op het bevriezen van tegoeden. In de VS en in Europa bestond het idee dat terroristen van hun levensbloed werden beroofd als men de geldstromen zou afsnijden. Hoewel er sinds 9/11 wereldwijd tegoeden zijn bevroren, bleek het niet het einde van het terrorisme. In de loop der tijd is dit beleid wel verder uitgewerkt. Daarbij is het zwaartepunt verschoven van het bevriezen van grote geldtegoeden naar het op lijsten plaatsen van verdachte terroristen. Het doel hiervan is hun mogelijkheden om tot actie over te gaan te verstoren of te bemoeilijken en hun supportnetwerk af te schrikken om nog zaken met hen te doen.

Parallel aan het bevriezen van tegoeden werd er ingezet op het preventief detecteren van terroristen. Enerzijds door private bedrijven te verplichten risicogerichte analyses te maken en verdachte transacties op te sporen. Anderzijds door het maken van netwerkanalyses op basis van databases met uitgevoerde transacties. De resultaten van deze aanpak zijn niet eenduidig weer te geven. Waar sommigen (bescheiden) resultaat zien, klagen anderen (nog altijd) over het zoeken van een speld in een hooiberg. Meer algemeen bestaat de overtuiging dat grotere aandacht voor de identiteit van de klant en de context waarin transacties plaatsvinden, op terroristen (en andere misdadigers) een afschrikkende werking heeft en terroristen dwingt om zich op andere manieren te financieren of hun ambities aan te passen aan meer beperkte financiële middelen. Bovendien is een betere vaststelling van de identiteit van klanten, transacties en netwerken waardevol gebleken nadat een aanslag heeft plaatsgevonden.

De laatste jaren wordt er steeds meer aangedrongen op het feit dat financiële gegevens met name nuttig zijn als onderdeel van het inlichtingenwerk. Er wordt gesteld dat financiële informatie soms net het missende puzzelstuk kan zijn binnen een groter plaatje. Ook helpen financiële inlichtingen bij het lokaliseren van individuen en delen van netwerken, waardoor het in kaart brengen van verdachten en financiële stromen op een meer doelgerichte manier kan gebeuren. Om de waarde van financiële inlichtingen goed te begrijpen, stellen sommigen dat ze als één onderdeel van de bredere strijd tegen terrorisme en financiële criminaliteit moeten worden geplaatst.

Sinds de aanslagen van 9/11 hebben de ideeën zich ontwikkeld over wat de bestrijding van terrorismefinanciering kan en zou moeten opleveren. Het bevriezen van tegoeden van terrorismeverdachten, noch het preventief detecteren van verdachte klanten en transacties en het in kaart brengen van netwerken bleek het ultieme panacee. Dit neemt niet weg dat, in specifieke situaties, het plaatsen van iemand op een terrorismelijst of het gebruik van een typologie om onbekende (vermeende) terroristen in beeld te brengen, bij kan dragen aan de strijd tegen terrorisme. Ook kunnen financiële inlichtingen net dat cruciale inzicht geven in een breder terrorismeonderzoek. In Nederland lijkt sinds de opkomst van IS en de aanslagen in Europa een nieuwe sprong te zijn gemaakt voor wat betreft bewustwording en initiatieven met betrekking tot het belang van CFT binnen compliance. De toekomst van dit beleid, of CFT 2.0, ligt niet alleen in het herijken van het beleid en nieuwe initiatieven waar nodig. Er zou ook een eerlijk en genuanceerd gesprek moeten komen met betrekking tot de verwachtingen, de (neven)effecten, en daarbij passende middelen in de strijd tegen terrorismefinanciering. Zowel publieke als private actoren maar ook de wetenschap kunnen bijdragen aan een frisse en kritische blik.

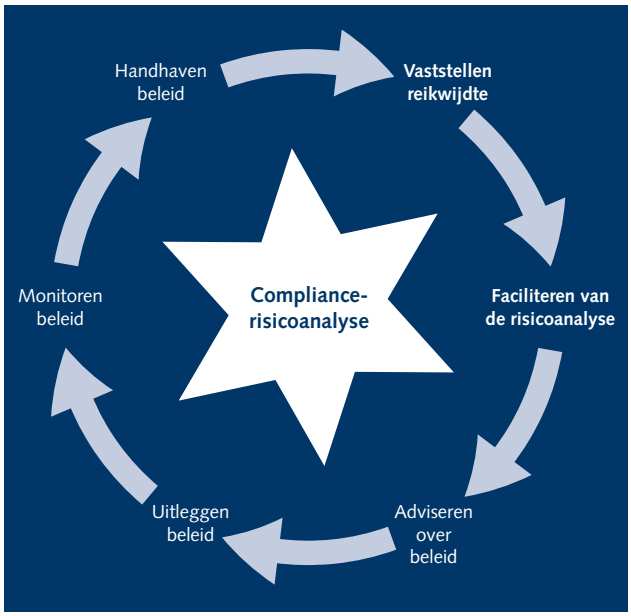
Dr. M. (Mara) Wesseling is onafhankelijk consultant en docent op het gebied van de bestrijding van terrorismefinanciering (CFT). In 2013 promoveerde zij aan de Universiteit van Amsterdam op de Europese strijd tegen terrorisme financiering.

WWFT 2018: ROADMAP VOOR COMPLIANCE OFFICERS

MUSA ELMAS

IN 2018 ZAL NAAR VERWACHTING DE AANGEPASTE WET TER VOORKOMING VAN WITWASSEN EN FINANCIEREN VAN TERRORISME (WWFT) IN WERKING TREDEN. IN EEN VAN DE ANDERE BIJDRAGEN IN DEZE EDITIE VAN DE COMPLIANCE OFFICER HEEFT THAI-HA VU DE CONTOUREN VAN DE WWFT 2018 UITEENGEZET, GEBASEERD OP DE VIERDE EUROPESE ANTI-WITWASRICHTLIJN (VIERDE AWWR) EN DE TOT OP HEDEN VERSCHENEN PUBLICATIES VANUIT DE RIJKSOVERHEID OMTRENT DE VOORGENOMEN IMPLEMENTATIE DAARVAN IN DE WWFT. ALS COMPLIANCE OFFICERS KUNNEN WE ONS ALVAST VOORBEREIDEN OP DE WWFT 2018. IN DEZE BIJDRAGE WORDT VOOR COMPLIANCE OFFICERS AAN DE HAND VAN DE COMPLIANCECYCLUS EEN ROADMAP UITEENGEZET VOOR DE OMGANG MET DE WWFT 2018.

De compliancecyclus[1] ziet er als volgt uit:



ONTWIKKELINGEN IN WET- EN REGELGEVING

Lees u alvast in en blijf op de hoogte van de actualiteit

Allereerst is het zaak om als compliance officer de ontwikkelingen in de aanstaande Wwft 2018 bij te houden. Van daaruit zal de vertaalslag plaatsvinden naar interne regelgeving. Op het moment van schrijven zijn de volgende publicaties verschenen rondom de implementatie van de richtlijn in de Wwft:

- 5 juli 2016: Concept wetsvoorstel voor de Implementatiewet Vierde AWWR
- 5 juli 2016: Bijbehorend Concept Memorie van toelichting Vierde AWWR
- 31 maart 2017: Consultatie Implementatiewet registratie uiteindelijk belanghebbenden
- 13 oktober 2017: Wetsvoorstel Implementatiewet Vierde AWWR
- 13 oktober 2017: Bijbehorend Concept Memorie van toelichting Vierde AWWR
- 31 januari 2018: Ontwerp Uitvoeringbesluit Wwft 2018[2]

1 *Handboek Compliance Professional 2017*, Capelle aan den IJssel, Uitgever: Nederlands Compliance Instituut, p. 53, 2017.

2 Primair gericht op de nieuwe PEP- en UBO-definitie.

Na het lezen van de genoemde publicaties zullen de contouren van de Wwft 2018 voor u duidelijker worden.

Houdt u zichzelf verder op de hoogte van de actualiteit. Abonneer u bijvoorbeeld op de nieuwsbrieven van het ministerie van Financiën en de nieuwsbrieven van de toezichthouders, zoals DNB en de AFM.

VASTELLEN REIKWIJDTE

Bepaal of en welke bepalingen van de Wwft 2018 van toepassing zullen zijn op uw organisatie. Bij banken zal de reikwijdte bijvoorbeeld anders zijn dan bij gokinstellingen. Bij gokinstellingen kunnen er vrijstellingen worden toegepast. De conceptwetgeving van de Wwft 2018 loopt daarop vooruit, maar hoe het e.e.a. gestalte zal gaan krijgen met betrekking tot de mogelijke vrijstellingen voor gokinstellingen is nog niet duidelijk.

Nadat je de nieuwe wettelijke verplichtingen in het vizier hebt en de gevolgen voor je organisatie hebt beoordeeld, kun je werken aan een plan van een aanpak. Benoem daarin welke thema's onder het nieuwe CDD-beheersingsraamwerk zullen vallen. Neem je bijvoorbeeld de sanctieregelgeving of internationale regelgeving mee of adresseer je die separaat, ontwikkel je een internationaal groepsbeleid of juist niet, specificeer je het voor bepaalde afdelingen of niet, et cetera.

FACILITEREN VAN DE RISICOANALYSE

De Vierde AWWR introduceert een versterkte risicobenadering, tevens van toepassing op private instellingen die vallen onder de reikwijdte van de Wwft. Instellingen behoren zelf factoren te identificeren die duiden op een lager of hoger risico. Artikel 6 van de huidige Wwft, met een lijst van instellingen die nu standaard in aanmerking komen voor vereenvoudigd cliëntenonderzoek, komt als gevolg daarvan te vervallen.

De risicoanalyse behoort een uitdieping te zijn van de cliëntintegriteitsrisico's, voortkomende uit cliënt-, product-, dienst- of leveringskanaalgebonden[3] en geografisch gebonden risicofactoren. De Vierde AWWR voorziet in de bijlagen met voorbeelden van lagere en hogere risico's. De Wwft en de leidraden van de toezichthouders bieden ook generieke aanknopingspunten, maar wees erop bedacht dat het profiel van de organisatie juist tot uiting hoort te komen in de risicoanalyse, het centrale thema in de compliancecyclus.

Een organisatie is dan ook zelf aan zet om na te denken over de risicomethodologie en over de risico-indicatoren die blijk geven van het (risico)profiel van de organisatie. Dit behoort goed onderbouwd te worden.

Overleg in deze fase als compliance officer met de beleidsbepalers over de strategie van de organisatie. Daaruit komen namelijk de cliëntintegriteitsrisico's voort. Vervolgens kan de blauwdruk van de risicoanalyse worden ontwikkeld ter voorbereiding van de daadwerkelijke risicoanalyse. Leg daarbij het accent op kwalitatieve criteria (risicoindicatoren) in plaats van kwantitatieve criteria. De resultaten van de risiconanalyse behoren integraal door te werken in de beheersmaatregelen die de instelling neemt in de klantrelatiecyclus (identificatie, verificatie, risicoclassificatie, acceptatie, monitoring en review).[4] De risico-indicatoren en daarbij behorende beheersmaatregelen in de klantrelatiecyclus kunnen als uitvloeisel van de risicoanalyse het beste worden vervat in een risico-matrix. Een dergelijke matrix kan in de praktijk eenvoudig door medewerkers worden toegepast.

Bij de cliëntintegriteitsrisicoanalyse is betrokkenheid van diverse geledingen in de organisatie gewenst, bovenal beleidsbepalers, het managementteam en de business (in de lead). Compliance kan als sparringspartner betrokken zijn vanuit zijn/haar adviserende (gevraagd en ongevraagd), initiërende, faciliterende, coördinerende en monitorende rol.

ADVISEREN OVER BELEID

De Wwft 2018 maakt het noodzakelijk om het CDD-beheersingsraamwerk van een instelling te reviseren. Na de risicoanalyse behoort o.a. het CDD-beleid daarop te worden aangepast. De compliance officer heeft net zoals bij de risicoanalyse een initiërende, faciliterende, coördinerende, adviserende en monitorende rol. De business behoort in principe in de lead te zijn voor het beleid, maar vaak komt het bij middelgrote en kleine organisaties voor dat de compliance officer een grotere rol op zich neemt. Gezien de kleinere omvang van de organisatie is dat enigszins te begrijpen, maar het three lines of defense-model behoort het uitgangspunt te zijn. Wees je als compliance officer daarvan bewust. Het is ook hier gewenst om alle geledingen van de organisatie bij het nieuwe beleid te betrekken.
Dit door bijvoorbeeld gezamenlijke voorbereidingssessies, vergaderingen, multidisciplinaire projectgroepen e.d. te organiseren. In dit stadium is het ook gewenst dat

3 Bijvoorbeeld face-to-face-dienstverlening, digitaal of dienstverlening door middel van een intermediair.

4 M. Elmas (2018), CIRA: Cliëntintegriteitsrisicoanalyse, *Tijdschrift voor Compliance*, Uitgeverij: Den Hollander, februari 2018.

compliance de beleidsbepalers, het managementteam en de business bijstaat met advies en expertise, bezien vanuit de rol van sparringspartner. Dit met het oog op de strategische overwegingen en keuzes bij de creatie van het nieuwe CDD-beheersingsraamwerk.

In deze fase is het van belang om niet alleen aan de slag te gaan met het beleid, maar ook met procedures, processen, werkinstructies, formats, wijzigingen in CMS-systemen e.d. In de dagelijkse praktijk is het niet altijd uitnodigend voor de medewerkers om een beleidsstuk van grote omvang er direct bij te nemen en in detail te bestuderen. De hiervoor genoemde nadere initiatieven zullen bijdragen aan een duidelijker en beter begrip van hetgeen in de dagelijkse praktijk wordt verwacht.

UITLEGGEN BELEID

De uitlegfase is een zeer belangrijke fase in de compliance-cyclus. Medewerkers behoren bewust te worden gemaakt van de Wwft 2018 en het nieuwe beheersingsraamwerk van de instelling. De uitdaging in deze fase is om draagvlak te creëren binnen de organisatie. De praktijk leert dat de business niet direct enthousiast wordt van nieuwe regels. Het kan in geval van CDD ervaren worden als nog meer regelgeving die het complexer maakt om klantrelaties aan te gaan of in stand te houden. Het is cruciaal om over te brengen wat de gedachtegang is achter de CDD-regelgeving, de aanleiding voor de nieuwe regelgeving en wat er van de medewerkers wordt verwacht. Het accent behoort niet te liggen op de letter van de wet of het beleid, maar juist op de geest daarvan. In geval van CDD is dat niet het vangen van boeven, maar juist de bescherming van de financiële sector en de organisatie tegen misbruik van financiële producten en diensten, en daarmee de instandhouding van bovenal de integriteit en reputatie van de organisatie.

Aan de compliance officer de belangrijke taak om in samenwerking met de beleidsbepalers, het management-team en HR een awarenessprogramma te initiëren en op te zetten. Een awarenessprogramma waarin de centrale boodschap en de doelgroepen helder zijn geformuleerd, waar er qua leerdoelen en methodiek differentiatie is per doelgroep, waarin de planning en de tijdslijnen duidelijk zijn, waarvoor voldoende budget is, waar de awarenesstools divers zijn en waarbij bovenal betrokkenheid is vanuit het managementteam en de beleidsbepalers. Voor de beleidsbepalers schrijft de Wwft 2018 overigens ook expliciet een periodieke opleidingsplicht voor.

Beperk je als organisatie verder niet tot jaarlijkse e-learning-modules o.i.d. Denk in ruimere mogelijkheden zoals workshops, open opleidingen, incompanyopleidingen, dillemmatrainingen, aandacht voor CDD in werkoverleggen, beoordelings- en functioneringsgesprekken, op het intranet, in nieuwsbrieven, Q&A-formulieren et cetera.

MONITOREN BELEID

De monitoringsrol van de compliance officer moet in dit kader niet verward worden met transactiemonitoring- en transactiefiltering in het kader van de Wwft en de Sanctiewet 1977. Alhoewel compliance vaak ook bij die werkzaamheden betrokken is, wordt met monitoring een ruimer blikveld van de compliance officer bedoeld, gericht op de werking van het CDD-beheersingsraamwerk. Daartoe worden bijvoorbeeld steekproefsgewijs dossiers gelicht door de compliance officer, met meer focus op bepaalde risico-profielen en risico-indicatoren. Regelmatig wordt de vastlegging van de business door de compliance officers ervaren als een zoektocht waar je door de bomen (lees informatie, documentatie en overige vastgelegde data) het bos niet meer overziet (lees het klantdossier). Introduceer in samenwerking met de business en andere staffunctionarissen systemen, formats, templates, sjablonen e.d. voor de inrichting van de klantdossiers.

De vastlegging is voor veel instellingen een aandachtspunt. Dossiers zijn regelmatig onoverzichtelijk en niet compleet. Het streven moet zijn dat het gehele cliëntacceptatie- dan wel reviewproces voor een derde partij, bijvoorbeeld een compliance officer, auditor of externe toezichthouder, toegankelijk, inzichtelijk, duidelijk en reproduceerbaar is. Het uitgangspunt, 'if it's not documented, it's not done', gaat hier op. Het gaat om een eenduidige en consistente vastlegging in dossiers. Gebruik bij de beoordeling van dossiers als compliance officer ook een modellijst aan de hand waarvan je beoordeelt of bijvoorbeeld de regels uit de nieuwe Wwft adequaat worden toegepast. In de beginfase zal de nieuwe aanpak enigszins wennen zijn. Probeer de business juist ook mee te nemen in dit traject. Koppel bijvoorbeeld je bevindingen terug naar aanleiding van de dossierbeoordelingen en monitor de tijdige en adequate follow-up van je bevindingen door de business. Persoonlijke terugkoppelingsgesprekken met de accountmanagers en de managers van een afdeling zijn in dit kader ook behulpzaam.

HANDHAVEN BELEID

Blik eind 2018 of begin 2019 terug op het nieuwe CDD-beheersingsraamwerk en rapporteer als compliance officer over de ondernomen initiatieven, de belangrijkste onderdelen van het nieuwe CDD-beheersingsraamwerk, de uitkomsten van de risicoanalyse, voortgang van het awarenessprogramma, de monitoringsresultaten, het aantal gerapporteerde transacties aan de FIU-Nederland, de cijfermatige resultaten van de indeling van cliënten in risicocategorieën, het aantal verbroken relaties i.c.m. CDD, good and bad practices, adviezen voor oplossing van de tekortkomingen e.d. In de rapportage kunnen ook de bevindingen van andere stafafdelingen zoals interne controle of audit worden meegenomen.
Zorg er ook voor dat de rapportage niet in een bureaulade verdwijnt, maar daadwerkelijk met het management en de beleidsbepalers wordt besproken. Awareness is hier ook van belang. Vervolgens kan de cyclus opnieuw beginnen.

AFSLUITING

De compliancecyclus zal een belangrijke basis zijn voor de organisatie en de compliance officers om effectief gestalte te geven aan de Wwft 2018. De betrokkenheid van de compliance officers behoort in overeenstemming te zijn met de tweedelijnsfunctie, conform het three lines of defense-model. Een brede betrokkenheid en een groot draagvlak vanuit de organisatie zijn een must. Tot slot de klassieke afsluiter als slot op de deur: 'If you think that compliance is expensive, try non-compliance.' Handel proactief en loop alvast vooruit op de Wwft 2018.
Succes toegewenst daarmee!

Musa Elmas is als senior compliance officer, adviseur en trainer werkzaam bij het Nederlands Compliance Instituut. Hij is verantwoordelijk voor het Focusteam CDD.

DE PARADISE PAPERS: INCIDENT OF TREND?

JAN VAN KONINGSVELD

NA DE STORM RONDOM DE PANAMA PAPERS IN 2016 STAAN DE MEDIA NU BOL VAN DE PARADISE PAPERS. EEN OVEREENKOMST TUSSEN AL DEZE DATALEKKEN IS DAT ALLE BETROKKEN PARTIJEN ACTIEF ZIJN BIJ HET OPZETTEN EN BEHEREN VAN OFFSHORE-ENTITEITEN EN BANKACCOUNTS VOOR CLIËNTEN WERELDWIJD. DE VRAAG DRINGT ZICH DAN OOK OP: WAT BETEKENEN DEZE DATALEKKEN VOOR DE COMPLIANCE-MEDEWERKERS?

INLEIDING

Na de Lux Leaks, Swiss Leaks, Offshore Leaks en de Panama Papers werd er op zondag 5 november 2017 een nieuw datalek geopenbaard, de Paradise Papers: 13,4 miljoen gelekte documenten, e-mails en contracten. In wezen gaat het om drie aparte datalekken met de gezamenlijke naam: de Paradise Papers. Het eerste lek is bij advocatenkantoor Appleby en haar voormalige dochteronderneming Esteria. Bij het tweede lek gaat het om documenten afkomstig uit de administratie van Asiaciti Trust in Singapore. Het derde lek omvat overzichten en uittreksels van negentien verschillende bedrijfsregisters.[1] De gegevens zijn door een anonieme tipgever doorgespeeld aan de Duitse krant de Süddeutsche Zeitung, die ze vervolgens heeft gedeeld met het International Consortium of Investigative Journalists (ICIJ) en de hieraan verbonden groep van journalisten. Voor Nederland zijn dat het FD en Trouw.

Een compliancemedewerker maakt een op risico gebaseerde afweging van de dienstverlening van een bepaalde cliënt (risicoanalyse) en stelt op basis daarvan een risicoprofiel op. Het gebruik van entiteiten gevestigd in offshore-jurisdicties is daar een belangrijk onderdeel van. Zonder identificatie en mitigatie van risico's aangaande relevante offshore-participatie zal het risicoprofiel onvolkomen en incorrect zijn en daarmee voorbijschieten aan het doel ervan.

Een compliancemedewerker kan op verschillende manieren betrokken raken bij offshore-entiteiten en -jurisdicties: zo kan een dergelijke entiteit cliënt zijn van een financiële instelling, optreden als wederpartij van een transactie of deel uitmaken van een internationale bedrijfsstructuur. Ook kan ze optreden als bestuurder en/of aandeelhouder en tenslotte kan offshore ook een rol spelen bij het aanleggen van een lijst van offshore-jurisdicties die eventueel worden geïmplementeerd in de SIRA en/of het cliëntenacceptatie-dossier.

DATALEKKEN: INCIDENT OF TREND?

De gelekte documenten onderstrepen nogmaals het significante belang van goed cliëntenonderzoek door financiële instellingen. Dit om te voorkomen dat ze ongewild verwijtbaar betrokken raken bij onregelmatigheden van hun cliënten. Overigens waren de Paradise Papers niet het eerste lek dat plaatsvond. Hierna een overzicht van de belangrijkste datalekken vanaf 2007 tot en met 2017.

1 Betreft de volgende offshore jurisdicties: Antigua & Barbuda, Aruba, de Bahama's, Barbados, Bermuda, de Kaaimaneilanden, Cookeilanden, Dominica, Grenada, Labuan, Libanon, Malta, Marshalleilanden, Saint Kitts & Nevis, Saint Lucia, Saint Vincent, Samoa, Trinidad & Tobago en tenslotte Vanuatu.

JAAR	NAAM	TYPE INSTELLING
2007	UBS	Bank in Zwitserland
2007	Swiss Leaks	HSBC-bank in Zwitserland
2008	LGT	Bank in Liechtenstein
2013	Offshore Leaks	Twee trustkantoren: Portcullis trustNet in Singapore en Commonwealth Trust Limited in de BVI
2014	Lux Leaks	Belastingadviseur PWC Lux
2016	Panama Papers	Advocaten- en trustkantoor Mossack Fonseca in Panama
2016	Bahama Leaks	Handelsregister in de Bahama's
2016	Football Leaks	Onbekend
2017	Credit Suisse	Bank in Zwitserland
2017	Paradise Papers	Advocatenkantoor Appleby in Bermuda

Tabel 1: Overzicht van enige belangrijke datalekken

Er hebben dus in deze periode tenminste tien datalekken plaatsgevonden bij dienstverleners zoals banken, belastingadviseurs, trustkantoren en handelsregisters. Opvallend in deze tabel is dat de frequentie, de omvang en de verscheidenheid van instellingen de laatste twee jaar is toegenomen. Bij de Paradise Papers gaat het vooral om belastingontwijking door multinationale ondernemingen zoals Nike, Apple, Uber, Facebook en Glencore. Veelal gaat het om banken in Zwitserland waar de accounts worden aangehouden en om Caribische landen zoals Panama, de Britse Maagdeneilanden, de Bahama's en Bermuda waar de offshore-entiteiten zijn gevestigd.

De keuze voor een land als vestigingsplaats van een offshore-vennootschap zal vanuit misbruikperspectief gezien, vooral ingegeven worden door de aanwezigheid van anonimiteit bevorderende elementen, zoals belastingvrijdom (waardoor er geen aangiftebiljet moet worden ingevuld en ingeleverd en de lokale overheden over minder informatie beschikken en zodoende ook niet kunnen uitwisselen met andere landen); de mogelijkheid om van nominee-dienstverlening gebruik te maken; het niet hoeven opmaken van een jaarrekening; en een minimum aan deponeringsverplichtingen in openbare registers, waardoor er vrijwel geen informatie beschikbaar is over de eigenaren en bestuurders van deze bedrijven.

DE GEBRUIKTE OFFSHORE-STRUCTUREN EN TRANSACTIES

De Paradise Papers en eerdere datalekken geven een uniek inkijkje in de wereld die weinig transparant is voor de buitenwereld. Zij geven een beeld van structuren die zijn opgezet voor multinationale ondernemingen, politici en vermogende particulieren om belasting te ontwijken en/of corruptiebetalingen te verhullen. Een veel voorkomende constructie, vooral bij belastingfraude en corruptie, is de volgende: het oprichten van een offshore-vennootschap in een belastingparadijs met een nominee director, statutair gevestigd op het adres van een lokaal trust- of advocatenkantoor die een factuur stuurt met een niet-stoffelijke omschrijving zoals: 'consulting' of 'management fee'. Deze offshore-vennootschap is veelal louter opgericht om een factuurstroom te creëren, met als doel om betalingen in de administratie te rechtvaardigen en gelden aan de betalende onderneming te onttrekken. Een belangrijke indicatie hierbij is de datum van oprichting van de vennootschap in relatie tot de datum van de factuur c.q. contract.

Bij offshore-structuren gaat het om een hoog risico en zijn instellingen verplicht om een diepgaand onderzoek in te stellen naar de (economische) reden van de structuur.[2] Al kan het onderzoek 'beperkt' blijven tot de relevante delen van de structuur. De vraag is natuurlijk wat er wordt verstaan onder de relevante delen van de structuur. Gelukkig zijn er maar een beperkt aantal standaardstructuren, zoals de holdingstructuur, de rente- en royaltystructuur, de re-invoicing-structuur en de cv-bv-structuur. De compliancemedewerker moet deze gebruikelijke standaard structuren kennen en begrijpen om zodoende de ongebruikelijke structuren te herkennen en de risico's te mitigeren.

Hierbij dient opgemerkt te worden dat het, mits aan alle fiscale verplichtingen wordt voldaan, in principe gaat om legale commerciële activiteiten die – zolang er voldoende vraag is naar deze producten – zal blijven bestaan. De financiële instellingen in offshore-jurisdicties zullen in het algemeen voldoen aan de lokale wet- en regelgeving die het mogelijk maakt om een grote mate van anonimiteit

2 DNB, 17 juli 2017.

voor niet-inwonende cliënten te realiseren. Vragen die hierbij een rol spelen zijn: Wat is het doel van de structuur? Wat is het doel voor de inzet van een bepaalde jurisdictie? Gaat het om een fiscaal gedreven structuur en zo ja, waaruit blijkt dat? Is er een fiscale opinie van een erkende belastingadviseur aanwezig? Is de structuur fiscaal agressief te noemen?

HEEFT MIJN CLIËNT EEN RELATIE MET DE PARADISE PAPERS?

Een deel van de Paradise Papers is per 17 november 2017 aan de bestaande database van ICIJ toegevoegd en voor iedereen raadpleegbaar. Deze database laat een netwerk zien van offshore-entiteiten, hun adressen en de hierbij betrokken (rechts)personen. Persoonlijke gegevens, zoals paspoorten, bankrekeningnummers en e-mailadressen, zijn niet vrijgegeven.
De gegevens in de database zijn een momentopname: regelmatig wordt nieuwe data toegevoegd, zoals op 19 december 2017 van vier companiesregisters uit Barbados, de Bahama's, Aruba en Nevis. Eind 2017 is informatie van zeshonderdtachtig duizend offshore-entiteiten uit vijfenvijftig verschillende belastingparadijzen opgenomen in deze database. Het feit dat een (rechts)persoon voorkomt in de database wil nog niet zeggen dat er sprake is van fraude.

Toezichthouder DNB wil dat banken en trustkantoren hun klanten door de ICIJ-database halen en onderzoeken op betrokken relaties en waarom een relatie voorkomt in deze database. Bij een hit verwacht DNB nader onderzoek en een melding van deze bevindingen.[3] De vraag hierbij is hoe je als compliancemedewerker een database met meer dan vijfentwintig miljoen documenten doorzoekt? Handmatig zoeken lijkt geen oplossing. Als je per document een minuut nodig hebt, dan ben je meer dan vijfenveertig jaar bezig. Het moet dus anders en het liefst geautomatiseerd en snel. Een doelmatige en effectieve oplossing is om de database te downloaden en vervolgens te combineren met de (transactie)gegevens van uw eigen cliënten. Hierdoor is het makkelijker om verbanden te leggen en zal de functionaliteit van de database aanmerkelijk toenemen.

Daarnaast kan voor aanvullende informatie gebruikgemaakt worden van open bronnen. Zie bijvoorbeeld opencorporates.com voor informatie over bedrijven en de daarbij betrokken bestuurders.
Verder zijn Panama en Bermuda slechts twee landen van de ongeveer veertig offshore-landen in de wereld. Om het landenrisico van uw cliënten sneller, actueel en betrouwbaar in kaart te brengen, kunt u (binnenkort) gebruikmaken van de Offshore Risk Index (ORI)-database die door het Offshore Kenniscentrum is ontwikkeld. In de ORI-database kunt u zien welke (financiële) informatie offshore-vennoot-

3 Nieuwsbrief DNB, 29 november 2017.

schappen zelf moeten opmaken en welke informatie moet worden gedeponeerd bij een lokaal handelsregister en zodoende beschikbaar is.

WAT ZIJN DE GEVOLGEN EN LESSEN VAN DEZE DATALEKKEN?

Wat kunnen wij afleiden uit de gelekte data en andere in het publieke domein beschikbare data? Hieronder een niet-limitatieve opsomming van de verschillende perspectieven om dit te bekijken.

Ten eerste dat toezicht en handhaving, zowel onshore als offshore, tekortschieten.
Ten tweede dat er een veel beter zicht is ontstaan op de wijze waarop multinationals en vermogende particulieren hun heffingsgrondslag verminderen met behulp van offshore-entiteiten.
Ten derde heeft het niet of nauwelijks geleid tot structurele aandacht van deze dienstverleningssector. Wel hebben deze incidenten voor veel media en politieke aandacht gezorgd, maar die was veelal van korte duur en zit duidelijk niet in het collectieve geheugen van wetgevers en handhavers. Het heeft vooral geleid tot incidentele en adhoc-wet- en regelgeving, zoals het instellen van de Parlementaire ondervragingscommissie Fiscale constructies, de invoering van de Wtt 2018, het opstellen van een zwarte lijst van belastingparadijzen en het invoeren van een UBO-register.

Verder zullen de cliënten zich realiseren dat de vertrouwelijkheid en veiligheid van hun gegevens niet meer gegarandeerd is. Het risico bestaat dat cliënten daardoor niet meer alle relevante informatie verstrekken. Belangrijk is om goed uit te leggen aan de cliënt wat de (wettelijke) grond is van de vraag om informatie en welk belang daarbij voor de cliënt zelf speelt.
Daarnaast komt uit de gelekte informatie naar voren dat een CDD-onderzoek naar offshore-entiteiten vrijwel nooit alle feiten en omstandigheden zal blootleggen. Zo is het lastig voor een compliancemedewerker om in offshore-landen informatie bij het een handelsregister te krijgen. Ook is het lastig om de werkelijke UBO te identificeren en te verifiëren. In dossiers met offshore-entiteiten is het alleen (laten) invullen van een UBO-formulier vaak onvoldoende en zal men aanvullend onderzoek moeten doen. Bijvoorbeeld door een persoonlijke ontmoeting met de UBO en hem/haar dan de juiste vragen te stellen. Als je niets vraagt weet je ook niets.
Ook zal er meer aandacht moeten komen voor (IT-) beveiliging van uw data; stel u voor wat er zou gebeuren als uw data wordt gehackt. Honderd procent veiligheid is onmogelijk, maar bepaal uw kroonjuwelen en bescherm deze maximaal.

Tenslotte is de les dat compliance zich nog meer moet focussen op offshore-risico's en beperking van deze risico's: 'hoe zou een onafhankelijke derde hier tegenaan kijken?' is een belangrijk toetsingscriterium geworden.

TOT SLOT: ENKELE PRAKTISCHE TIPS

1. De eerste stap is om te beseffen dat offshore-structuren en -transacties een structurele en belangrijke rol spelen in het dagelijkse werk van de compliancemedewerker.
2. Stel een goede en actuele klantbeeldanalyse op van de offshore-structuren en van de risico's van de cliënten en hun cliënten. Denk hierbij ook aan de volgende offshore-risico's: landenrisico's; sectorale risico's; substance-eisen; gebruik van nominee-dienstverlening, betalingen aan offshore-entiteiten buiten de structuur en gebrek aan transparantie van de UBO en aan informatie. De combinatie van deze factoren helpt bij het kwalificeren van het risico.
3. Gebruik de aanwezige, beperkte compliancecapaciteit optimaal: besteed meer aandacht aan de meest risicovolle cliëntdossiers (80-20-regel).
4. The devil is in the detail: in de offshore-wereld worden de werkelijke feiten niet altijd gepresenteerd en de gepresenteerde feiten zijn niet altijd de werkelijke feiten. Een goede analyse van de offshore-structuren, de aanwezige red flags, het (her)beoordelen van de contracten en facturen en het stellen van de juiste vragen, blijft belangrijk werk voor de compliancemedewerker.
5. Naar mijn mening zal de compliancedienstverlening substantieel verbeteren als de rol van het gebruik van offshore-structuren explicieter wordt meegenomen in de beschrijving van fraudepatronen en typische kenmerken van misbruik van offshore-vennootschappen worden betrokken in de risicoanalyse.

Ik durf te stellen dat de Paradise Papers geen incident zijn, maar onderdeel zijn van een trend die zich zal voortzetten. De komende jaren zal er steeds meer informatie internationaal worden uitgewisseld, waardoor de kans op datalekken zal worden vergroot. Als ik in dit kader nog een wens mag doen voor 2018: de Delaware Papers.

Mr. dr. T.J. (Jan) van Koningsveld werkte 25 jaar bij de FIOD en is directeur van het Offshore Kenniscentrum in Almere. Op 7 oktober 2015 is hij gepromoveerd aan de Universiteit van Tilburg op het onderwerp misbruik van offshore-vennootschappen. Een handelseditie van zijn proefschrift is verkrijgbaar via zijn website: www.okcnl.nl.

Q&A CUSTOMER DUE DILIGENCE

MUSA ELMAS

Regelmatig ontvangen wij in onze adviespraktijk praktische vragen van onze relaties omtrent de toepassing van CDD in de dagelijkse praktijk. In deze bijdrage is een selectie van vragen uitgelicht en voorzien van een antwoord. Heeft u ook vragen over CDD? Benader gerust het CDD-Focusteam van het Nederlands Compliance Instituut.

1. BEHOORT EEN KLANT WAAROP AFGELEIDE IDENTIFICATIE IS TOEGEPAST, IN DE RISICO-CATEGORIE HOOG TE WORDEN INGEDEELD?

De methode van afgeleide identificatie (bijvoorbeeld door middel van de naam-nummercontrole) is, als onderdeel van de situatie dat een cliënt niet fysiek aanwezig is voor de verificatie van diens identiteit, benoemd in artikel 8 lid 2 van de Wwft (verscherpt cliëntenonderzoek). Met betrekking tot afgeleide identificatie staat een verscherpt cliëntenonderzoek niet per definitie gelijk aan de kwalificatie van een klant als hoog risico. Alhoewel de andere aangewezen gevallen in de Wwft voor een verscherpt cliëntenonderzoek, zoals hoogrisicolanden, PEP's en correspondentbankrelaties in de regel wel tot een dergelijke conclusie leiden (afhankelijk van het beleid van een instelling), gaat dat sec op basis van afgeleide identificatie niet op. Vooral bij direct writers zou een dergelijke interpretatie enorme impact hebben op m.n. de monitoring- en reviewactiviteiten. Het beschreven uitgangspunt zal de nodige inspanningen besparen en meer focus op hogere risico's mogelijk maken.

2. BEHOORT EEN CONTANTE GELDSTORTING VAN € 15.000 OP EEN BANKREKENING TE WORDEN GEMELD AAN DE FIU-NEDERLAND?

Vaak bestaat in de praktijk de aanname dat de beschreven situatie in de vraagstelling voldoet aan de objectieve indicator en dientengevolge dient te worden gemeld aan de FIU-Nederland. Dat is niet het geval. De bedoelde objectieve indicator luidt als volgt:

'Een transactie voor een bedrag van € 15.000 of meer, waarbij contante omwisseling in een andere valuta of van kleine naar grote coupures plaatsvindt.'[1]

Bij de toepasselijke objectieve indicator behoort zowel aan de ingaande als aan de uitgaande kant sprake te zijn van een contante geldstroom. In casu is daarvan geen sprake. Derhalve voldoet het niet aan de objectieve indicator, omdat het door middel van een contante storting op de bankrekening wordt omgezet in giraal geld.

Wellicht ontstaat deze verwarring ook, omdat in de Wwft (en de onderliggende regelgeving) meerdere keren het bedrag van € 15.000 wordt genoemd, echter in een andere context.[2]

3. IS KONINGIN MÁXIMA EEN PEP?

De PEP-status komt gedurende trainingen regelmatig aan de orde. Op dit moment is koningin Máxima, gebaseerd op artikel 8 lid 4 van de Wwft, formeel geen PEP. De PEP-definitie is op 1 januari 2013 in de Wwft aangepast als gevolg van de FATF-evaluatie van Nederland. De huidige PEP-definitie heeft betrekking op politiek prominente functionarissen die in het buitenland woonachtig zijn

1 Zie Bijlage Uitvoeringsbesluit Wwft.

2 Beroeps- of bedrijfsmatig handelende verkopers van goederen vallen onder de reikwijdte van de Wwft, voor zover betaling van deze goederen in contanten plaatsvindt voor een bedrag van € 15.000 of meer, ongeacht of de transactie plaatsvindt in een handeling of door middel van meer handelingen waartussen een verband bestaat (artikel 1 Wwft). De tweede verwijzing betreft de noodzaak voor een instelling om een cliëntenonderzoek uit te voeren indien zij in of vanuit Nederland een incidentele transactie verricht ten behoeve van de cliënt van ten minste € 15.000, of twee of meer transacties waartussen een verband bestaat met een gezamenlijke waarde van ten minste € 15.000.
In het Uitvoeringsbesluit Wwft (in de daarin opgenomen bijlage) zijn verder andere objectieve indicatoren aangewezen waarin het bedrag van € 15.000 wordt genoemd.

of die in Nederland woonachtig zijn, maar niet de Nederlandse nationaliteit hebben. Denk bijvoorbeeld aan ambassadeurs. Koningin Máxima heeft de Nederlandse nationaliteit en is woonachtig in Nederland. Derhalve gaat de PEP-definitie niet op. Een instelling mag in haar CDD-beleid overigens er wel voor kiezen om dit strenger toe te passen en een hogere risicocategorie toewijzen.

Deze vraag zal na de implementatie van de Vierde Anti-witwasrichtlijn in de Wwft overigens niet langer relevant zijn. Er zal dan namelijk geen onderscheid meer zijn tussen binnenlandse en buitenlandse politiek prominente functionarissen. De functie zal leidend zijn.

4. BESTAAN ER OPENBARE PEP-LIJSTEN?

Er bestaan geen openbare PEP-lijsten. De PEP-lijsten zijn beschikbaar via commerciële providers. Door een bundeling van data maken zij PEP's op grote schaal inzichtelijk.

Dergelijke lijsten worden gekoppeld aan het relatiebestand van de instelling en kunnen vervolgens worden gebruikt voor de screening van potentiële en bestaande relaties. Vanuit de overheid of een andere gouvernementele organisatie zal een dergelijke lijst er (vooralsnog) niet komen.

5. IS EEN PERIODIEKE CDD-REVIEW VERPLICHT BIJ KLANTEN MET DE RISICOCLASSIFICATIE 'LAAG'?

Bij laagrisicoklanten is een event-driven review in principe gangbaar en is een periodieke review niet verplicht, overigens naar gelang het risicoprofiel van een instelling. In de Wwft en de onderliggende regelgeving is er geen (specifieke) informatie te vinden over de periodiciteit van reviews, de methode e.d. In de leidraad Wwft en Sw van DNB, en in nieuwsitems van DNB, wordt deze optie wel genoemd en in principe geaccepteerd. Van belang is wel dat event-driven reviews worden omgeven met goede waarborgen (opzet, implementatie, testen, periodiek onderhoud, onafhankelijke periodieke controle van het systeem, et cetera).

Musa Elmas is als senior compliance officer, adviseur en trainer werkzaam bij het Nederlands Compliance Instituut. Hij is verantwoordelijk voor het Focusteam CDD.

ANNEMARIJE SCHOONBEEK:

“DENK VANUIT KANSEN, ZIE DE ANTI-WITWAS-RICHTLIJN ALS KANS.”

Annemarije Schoonbeek en Virgil Matroos: twee bevlogen mensen die zichtbare passie hebben voor hun vak. Met als rode draad in hun beide carrières: integriteit. Tijd voor een nadere kennismaking.

WAT IS PRECIES JULLIE ACHTERGROND? *Virgil*: "Ik ben jurist – heb gestudeerd in Rotterdam en ben afgestudeerd in zowel privaat- als bedrijfsrecht – en ben begonnen als rijkstrainee bij het ministerie van Justitie. Daarna ben ik gaan werken voor het ministerie van Financiën, het College financieel toezicht en vervolgens voor de AFM. Momenteel ben ik werkzaam voor de Nederlandse Orde van Advocaten (NOvA) waar ik lid ben van de unit Financieel Toezicht Advocatuur.
Sinds 1 januari 2015 is het toezicht op advocaten belegd bij de dekens. Nederland is verdeeld in elf arrondissementen en elk arrondissement heeft een deken en een lokaal bureau. De elf dekens houden toezicht op 17.350 advocaten, die verdeeld zijn over 5.000 kantoren. Onder het 'toezicht houden' valt het complete toezicht, inclusief financieel toezicht en toezicht op de naleving van de Wwft. De unit Financieel Toezicht Advocatuur ondersteunt de dekens bij hun toezichtstaken en fungeert als een soort expertisecentrum."

Annemarije: "Ik ben opgeleid als fiscalist en heb ook Nederlands recht gestudeerd. Ik ben begonnen als internationaal belastingadviseur bij de rechtsvoorganger van Loyens & Loeff, Loyens & Volkmaars. Uiteindelijk vond ik de rechtsbeschermende rol en het sanctierecht, de grens tussen bestuurs- en strafrecht meer interessant en ben ik advocaat geworden bij Loyens & Loeff. Hierdoor kreeg ik meer te maken met het fiscaal procesrecht, maar ook met het financieel economisch (bestuurs)strafrecht. En met daaraan gerelateerde compliancevraagstukken zoals over naleving van anti-witwasregels en het adviseren daarover. Als advocaat heb ik benadeelde partijen, verdachte partijen of partijen die in onderzoek werden genomen, zoals financiële instellingen, bijgestaan.
In 2011 ben ik overgestapt naar de AFM en projectleider geworden bij de afdeling Integriteitstoezicht, een operationele afdeling die integriteitsissues behandelt bij vergunninghouders zoals accountantsorganisaties en financiële ondernemingen. Daar richtte ik mij onder meer op projecten op het gebied van betrouwbaarheidsonderzoeken, integere bedrijfsvoering en corruptie en belangenverstrengeling. Daarbij werkte ik vaak samen met andere toezichthouders zoals DNB al dan niet in het kader van het Financieel Expertise Centrum (FEC).
Sinds anderhalf jaar ben ik weer terug in de advocatuur. Ik hou mij nog steeds bezig met integriteitstoezicht, maar dan meer vanuit de private invalshoek. Ik adviseer over het voldoen aan wet- en regelgeving op het gebied van het integriteitstoezicht. In mijn werkzaamheden richt ik mij ook op het bijstaan van vergunninghouders, accountantsorganisaties en financiële ondernemingen, als ze te maken krijgen of dreigen te maken te krijgen met toezichthouders. Naast mijn praktijk ga ik per 1 maart a.s. parttime werken als directeur van Orde van Advocaten Overijssel. Vanuit mijn achtergrond heb ik te maken met de verschillende beroepsbeoefenaren, waaronder accountants, belastingadviseurs, notarissen, advocaten. Tijdens het Nationaal Anti-witwascongres zullen Virgil en ik een presentatie geven over de uitdagingen voor beroepsbeoefenaren bij witwasbestrijding. Als je kijkt naar onze beide carrières, dan is integriteit daarin de rode draad."

Virgil: "En passie. Ook op het gebied van technologische ontwikkelingen. Neem bijvoorbeeld blockchain en de ontwikkelingen rondom cryptocurrency; tussen nu en vijf jaar zullen deze ontwikkelingen een nog grotere rol van betekenis gaan spelen. De uitdaging daarbij is om het toezicht daarop te laten aansluiten. Die ontwikkeling, dat is ontzettend boeiend."

IN HOEVERRE IS HET MOGELIJK ALS TOEZICHTHOUDER OM VOOR TE SORTEREN OP DE TECHNOLOGISCHE ONTWIKKELINGEN, ZOALS BLOCKCHAIN? *Annemarije*: ""Mijns inziens zouden de professionele dienstverleners, zoals banken die te maken hebben met blockchain, het voortouw moeten nemen; zij zouden een visie moeten ontwikkelen. Want hoe je het wendt of keert, er komt een moment waarop je te maken zult krijgen met blockchain. De klant kan bijvoorbeeld gaandeweg de relatie zelf besluiten om in blockchain te stappen. Als professionele dienstverlener zal je daarop voorbereid moeten zijn en een visie moeten ontwikkelen over hoe je ermee omgaat en wat je nodig hebt om de risico's die ermee samenhangen adequaat te beheersen. Eigenlijk is het een taak van de toezichthouder en van de marktpartijen samen."

WAT MAAKT HET VAK DAT JULLIE UITOEFENEN BETEKENISVOL? *Virgil*: "Wat ik leuk aan het werk vind, is hoe er wordt omgegaan met regulering en toezicht, en hoe het gedrag zich daarbij ontwikkelt. Bij de AFM en het College financieel toezicht ging het juist over gedrag. Je hebt een set regels die moeten worden nageleefd, maar hoe zorgen we er nu voor dat het ook daadwerkelijk nageleefd wordt? Hoe effectief zijn de regels eigenlijk en hoe maken we ze effectiever? Voor mij vormt dit een constante prikkel en maakt het betekenisvol. Werken aan een integere advocatuur, die de rechtszoekende zo goed mogelijk dient."

Annemarije: "Wat ik leuk en betekenisvol vind, is de verbinding maken tussen de toezichthouder en de onder toezicht gestelde. Uiteindelijk dienen zij beide een gezamenlijk doel. Al wordt het vaak gezien als tegengesteld. Ik denk juist dat we er allemaal bij gebaat zijn dat de markt integer is, en dat de uitdaging ligt in het leren spreken van elkaars taal. Als toezichthouder moet je je kunnen inleven in hoe de onder toezicht gestelde het toezicht beleeft. En moet je kunnen begrijpen wat de onder toezicht gestelde nodig heeft om de regels goed na te kunnen leven. De onder toezicht gestelde daarentegen zal zijn best moeten doen om het belang van een integere markt en niet puur het commerciële belang voorop te stellen. Ik ben ervan overtuigd dat als je zichtbaar bijdraagt aan integriteit binnen de markt, je dit ook commercieel gaat helpen. Als je bouwt aan een goede reputatie, o.a. door de integriteitsrisico's te beheersen, dan heeft dat een zelfversterkend effect op je eigen professionaliteit."

ZIEN JULLIE VOORUITGANG IN HET MAKEN VAN DE VERBINDING TUSSEN DE TWEE PARTIJEN? *Annemarije*: "Ik heb wel het idee dat er meer verbinding ontstaat, maar ik zie ook dat er nog wel wat stappen gezet kunnen worden. Heel veel partijen worstelen met de vraag: 'Wat verwacht de toezichthouder eigenlijk van ons?' Doordat ik bij de toezichthouder heb gewerkt, maar ook met mijn voeten in de klei heb gestaan, snap ik de vraag én kan ik uitleggen wat het vertrekpunt is van de toezichthouder. Zo kun je elkaar vinden. Één van de speerpunten in het financieel toezicht is transparantie, zorgen dat je helder communiceert over wat de verwachtingen zijn."

Virgil: "Je ziet een verplaatsing van 'lijstjes afvinken' naar proactief en preventief toezicht, waarbij inderdaad meer wordt gecommuniceerd door de toezichthouder. De kracht van de communicatie zit vooral in het duidelijk kunnen maken dat er geen tegenstellingen zijn, maar dat er sprake is van een gezamenlijk belang. Daarvan zijn de toezichthouders zich wel bewust, ook al zijn er nog stappen te zetten. Uiteindelijk zal je ook de professionele dienstverleners die te maken krijgen met het toezicht hierin mee krijgen.
Bij een kantooronderzoek heb ik meegemaakt dat de advocaat in kwestie aangaf het niet prettig te vinden dat er onderzoek werd uitgevoerd, maar dat het hem uiteindelijk wel alert had gemaakt. En dat hij zich realiseerde dat de rechtszoekende, de cliënt, uiteindelijk bij goed toezicht gebaat is. Dat die verbinding, tussen mij en de onder toezicht staande advocaat, doorwerkt in de relatie naar de cliënt. Dát is waar het om gaat. Perfect zal het niet worden, maar we doen wel ons best het zo perfect mogelijk te krijgen."

WELKE ONTWIKKELINGEN BINNEN WITWASBESTRIJDING JUICHEN JULLIE TOE EN WELKE ZIEN JULLIE LIEVER ANDERS? WAAROM? *Annemarije*: "Wat ik toejuich is dat binnen de Vierde Anti-witwasrichtlijn de instellingen zelf hun risico's in kaart moeten brengen, dat dit heel belangrijk wordt gevonden. Instellingen zullen goed moeten nadenken over de risico's die ze lopen. Eigenlijk zou zo'n verplichting niet nodig moeten zijn, maar ik zie zeker de meerwaarde ervan.
De financiële sector loopt hierin voorop. De systematische integriteitsrisicoanalyse (SIRA) is daarin al geruime tijd gemeengoed. Ik denk dat andere sectoren, waaronder de beroepsbeoefenaren, kunnen leren van hetgeen al voorhanden is en ik zou hen willen uitnodigingen daar naar te kijken. Kijk vooral naar de lessons learned in de financiële sector."

Virgil: "Wat ik jammer vind is dat er binnen de Vierde Anti-witwasrichtlijn te weinig rekening wordt gehouden met vernieuwingen en dat er te weinig vooruit wordt gekeken. In de richtlijn – en waarschijnlijk ook in de Vijfde Anti-witwasrichtlijn, daarvan is de tekst inmiddels ook vastgesteld – is onvoldoende ruimte/provisie ingebouwd over hoe om te gaan met bijvoorbeeld cryptocurrencies. Dat had ik liever breder gezien, want dan kun je er ook in nationale wetgeving en bij toezicht op inspelen en loop je minder achter de feiten aan."

IN HOEVERRE IS DE COMPLIANCEFUNCTIE INGERICHT BIJ BEROEPSBEOEFENAREN, ZOALS DE ADVOCATUUR? *Virgil*: "De advocatuur is heel divers; van heel grote organisaties, tot specifieke rechtsgebieden, tot eenmanskantoren. Wat je ziet is dat bij de grote kantoren de compliancefunctie beter is ingericht. Op zich is dat ook logisch, want zij hebben veel te maken met de financiële sector en het is in hun belang om het goed geregeld te hebben. Binnen die kantoren vind je compliance-afdelingen waar compliance officers werken. Wat je ziet is dat de aandacht voor de compliancefunctie anders ligt naarmate het kantoor kleiner wordt en verder verwijderd is van het rechtsgebied van de financiële sector. Binnen de Vierde Anti-witwasregeling is de compliance-functie duidelijk ingeregeld, ook voor beroepsbeoefenaren. De advocatuur, maar ook het notariaat, de accountants en belastingadviseurs, worstelen ermee hoe hieraan invulling te geven."

> PROBEER ZOVEEL MOGELIJK VOOR-UIT TE DENKEN EN JE FUNCTIE DUURZAAM EN TOEKOMST-BESTENDIG TE MAKEN.

Annemarije: "De crux van de hele risicobeheersing, inclusief compliance, zit in het feit dat het moet zijn toegespitst op de aard en omvang van de activiteiten. Er zit dus een bepaalde grenswaarde in waarbij het moet zijn ingericht. Ik vind dat elke organisatie, ook buiten de financiële sector, in beginsel een risicomanagementmodel zou moeten hebben waarin compliance is opgenomen.
De nieuwe Wwft kan hierbij een aanjager zijn, omdat deze organisaties verplicht tot het invoeren van een risicomanagementmodel en het uitgangspunt is dat je een compliancefunctie hebt ingericht. Tenzij de aard en omvang zodanig is dat het nergens op zou slaan, zoals bij een organisatie waar maar drie medewerkers werken."

IN HOEVERRE ZAL DE VIERDE ANTI-WITWAS-RICHTLIJN IMPACT HEBBEN OP DE BEROEPS-BEOEFENAREN? *Virgil*: "Het zal een flinke impact hebben op de beroepsbeoefenaren, maar zeker ook op het toezicht. Je zult aan meer open normen moeten voldoen, ook al zie je een zekere afbakening. Het betekent in ieder geval dat onder toezicht gestelden daarmee aan de slag moeten, net als de toezichthouder. Die laatste moet zorgen voor goede guidance."

Annemarije: "Mee eens. De beroepsbeoefenaren worden door de richtlijn nog eens extra gedwongen om goed naar zichzelf te kijken. Wat ook een impact zal hebben is het handhavingsregiem. Dat wordt echt anders, strenger. Door het specifieker zijn over de inrichting van het risicomanage-ment worden professionele dienstverleners uitgenodigd om het goed in te regelen. Zij zijn als eersten aan zet om te laten zien dat ze het goed op orde hebben. Dat biedt, als gezegd, ook kansen. En heeft ook een belang, omdat naast een strenger handhavingsregiem, ook de publicatie-mogelijkheden groter worden.
Het is een uitdaging voor de toezichthouder om de verbin-ding te blijven houden met de onder toezicht gestelden; dat zij aan die partijen vraagt naar wat haalbaar is en bijdraagt aan de integriteit van de markt."

ER IS VEEL TE DOEN (GEWEEST) OVER DE PARADISE PAPERS. WIE DAARIN VOORKOMT, HOEFT NOG NIET PER SE ILLEGAAL BEZIG TE ZIJN. TOCH LIGT DE MAATSCHAPPELIJKE PERCEPTIE VEELAL ANDERS. HOE KIJKEN JULLIE TEGEN DERGELIJKE DATALEKKEN AAN? WELK NUT ZIEN

JULLIE ERVAN IN? *Annemarije*: "Zoals ik er tegenaan kijk is dat de Paradise Papers aantonen dat bij reputatierisico's het niet langer alleen gaat om de vraag of je wel of niet de wet hebt overtreden, maar dat het daarbij ook draait om wat de perceptie is van het publiek over je gedrag. Wat je van de Paradise Papers kunt leren, is dat je als dienstverlener midden in de maatschappij moet staan om goed te kunnen weten wat er van jou wordt verwacht. Dat is niet makkelijk; het leven is nu eenmaal niet zwartwit, er zijn ook grijstinten. Het is belangrijk dat je binnen deze grijstinten probeert een bepaald kompas te volgen en dat je dit kunt uitleggen aan het publiek. Toen ik begon met werken, was een belangrijke vraag: 'Mag het van de wet?' Dat was best amoreel. Nu is belangrijk dat de risk appetite voldoende helder is; dat duidelijk zichtbaar is dat er op een integere manier wordt omgegaan met de maatschappelijke belangen. Ik vind het een goede ontwikkeling dat de Paradise Papers uitdagen daarover na te denken; dat het aanzet tot beheersing van de reputatierisico's en tot nadenken over welke rol je inneemt in de maatschappij.
Het is tevens een dynamisch speelveld; iets wat een jaar geleden misschien maatschappelijk geaccepteerd werd, kan vandaag de dag als onbetamelijk worden gezien. Onder toezicht gestelde partijen en toezichthouders moeten hier continue alert op zijn en moeten erop anticiperen. Zij zullen een professionele weg moeten vinden die goed uitlegbaar is. Je moet geen speelbal willen worden van de pers."

Virgil: Eens. De nadruk komt steeds meer te liggen op ethisch verantwoord handelen. Dat is een zichtbare ontwikkeling die je goed in de gaten moet houden."

IS ETHISCH VERANTWOORD HANDELEN TYPISCH IETS WAT HOORT BIJ DEZE TIJD? OF IS HET ER ALTIJD AL GEWEEST? *Virgil*: "Ik denk dat het meer past bij deze tijd. Voorheen was het meer van: 'dit is de wet- en regelgeving, dit zijn de kaders en zolang we binnen de kaders blijven doen we het goed'."

Annemarije: "Ik ben wat positiever. Ik denk dat er wel aandacht voor was, maar dat de groep mensen die er aandacht voor heeft gaandeweg is gegroeid. Ook vanuit het toezicht is er meer aandacht voor gekomen. Eerlijk gezegd is het voor een toezichthouder heel moeilijk om invulling te geven aan open normen, zoals 'maatschappelijk betamelijk'. Daarvan kun je niet zomaar zeggen 'het is fout', maar gaat het meer om de vraag of er op een zinvolle manier over iets is nagedacht."

WELKE TIPS ZOU JE AAN CO'S WILLEN GEVEN EN VOOR WELKE VALKUILEN ZOU JE ZE WILLEN WAARSCHUWEN IN HET KADER BESTRIJDING WITWASSEN EN CDD? *Annemarije*: "De tip die ik wil geven is: blijf professioneel kritisch.

Bij witwasbestrijding gaat het vaak om de kritische blik naar de cliënt. Dat levert een spanningsveld op, want zij zijn immers degenen waarmee je je brood verdient. Je moet in staat zijn je daarvan los te koppelen en professioneel kritisch te kijken naar wat er werkelijk gebeurt. Dat is soms gewoon boerenlogica met een gezonde dosis achterdocht. Veel mensen en dus ook dienstverleners redeneren vanuit vertrouwen. Dat kan, maar je moet altijd in staat zijn verder na te denken en ook verder durven te kijken."

REDENEREN VANUIT VERTROUWEN? IS ER NIET JUIST SPRAKE VAN HET TEGENOVERGESTELDE? *Virgil*: "Nee, dat denk ik niet. Er wordt met name vanuit vertrouwen gehandeld, maar professionals vergeten soms kritisch te kijken. Ik heb het gezien in de praktijk. Als ik aan de hand van een dossieronderzoek zie dat er geen slimme zet gezet is, dan had de professional, als hij een goede professioneel kritische bril op had gehad, dat ook moeten zien. De reden dat het dan toch niet gezien is, kan te wijten zijn aan professionele naïviteit. Wees je ervan bewust dat niet elke cliënt het goede met je voor heeft en je daarnaast als instrument wil gebruiken. Blijf dus zelf nadenken. Discussieer met vakgenoten of consulteer intern bij collega's, want dat kan tot bepaalde inzichten leiden en houd je scherp. Wij doen het zelf ook. Voordat er een rapportage de deur uitgaat, stellen we onszelf de vraag: 'Hebben we het goed gezien?' Of daaraan voorafgaand: 'Hoe kijken we er tegenaan, hoe denken we erover?' Blijf in ieder geval niet in je eigen cocon zitten."

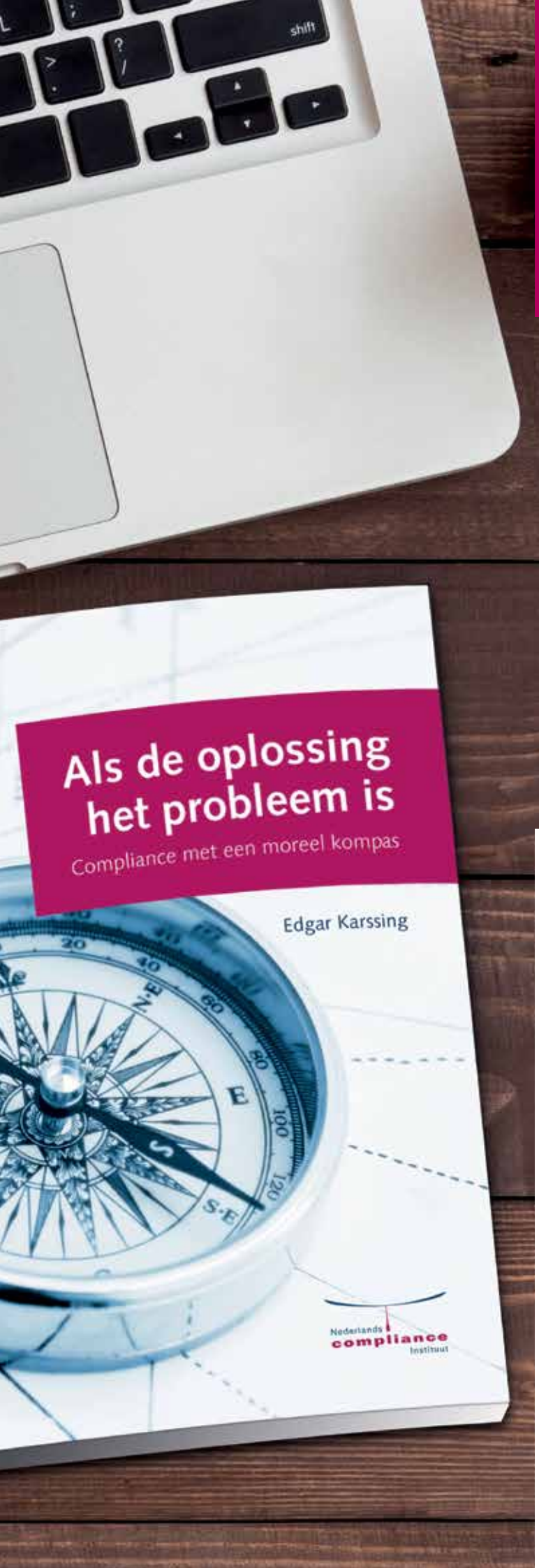
Annemarije: "Wat ook nog een tip is: probeer te leren van dingen die fout gaan. Een fout is een mooie kans om iets te leren."

WELKE AFSLUITENDE QUOTE WILLEN JULLIE MEEGEVEN AAN DE COMPLIANCE OFFICERS? *Annemarije*: "Denk vanuit kansen, zie de Anti-witwasrichtlijn als kans. Richt je functie zo in dat deze dynamisch blijft. Blijf nieuwsgierig en anticipeer."

Virgil: "En probeer zoveel mogelijk vooruit te denken en je functie duurzaam en toekomstbestendig te maken."

MUST-READ

Meer informatie, of een inkijkje in het boek? Kijk dan op: www.compliance-instituut.nl/product/als-de-oplossing-het-probleem-is-compliance-met-een-moreel-kompas



Veel bestuurders en compliance officers gaan gebukt onder 'controle-obesitas': problemen worden opgelost met meer regels. In zijn nieuwe boek 'Als de oplossing het probleem is - Compliance met een moreel kompas' draagt Edgar Karssing oplossingen aan om op deze vragen antwoord te kunnen geven.

Edgar Karssing maakt al meer dan 20 jaar inzichten uit de bedrijfsethiek concreet en hanteerbaar voor praktijkmensen. Het motto is steeds: de oplossing is het probleem niet! Karssing is teveel filosoof om meteen op zoek te gaan naar oplossingen. Wat is de vraag achter de vraag? Wat is het echte probleem?

Hoe geef je handen en voeten aan compliance met een moreel kompas? Hoe ziet dat eruit, wat kun je doen? Dat blijkt in de praktijk zo gemakkelijk nog niet. Daarom worden in dit boek praktische handvatten gegeven.

HET NATIONAAL ANTI-WITWAS-CONGRES

13 MAART 2018

Het nationaal Anti-witwascongres: dé gelegenheid om uw kennis over de ontwikkelingen op het gebied van de bestrijding van witwassen, terrorismefinanciering en andere vormen van (financieel-economische) criminaliteit snel op peil te brengen.

U bent van harte welkom om te komen kijken en luisteren naar toonaangevende sprekers die de laatste ontwikkelingen binnen deze thema's zullen belichten.

KIJK VOOR DE DETAILS, HET VOLLEDIGE PROGRAMMA EN OM IN TE KUNNEN SCHRIJVEN OP WWW.COMPLIANCE-INSTITUUT.NL/OPLEIDINGEN/AWWC