Leidraad Wwft en Sw

Versie december 2019

DeNederlandscheBank

EUROSYSTEEM

Inhoud

1 Inleiding 4

2 Inrichting bedrijfsvoering 6
2.1 Integere bedrijfsvoering 6
2.2 Opleiding, training en awareness 8
2.3 Integere bedrijfscultuur 9
2.4 Interne klokkenluidersregeling en meldpunt misstanden 9
2.5 Know your customer (KYC) / Customer due diligence (CDD) 10
2.6 Sanctieregelgeving 10
2.7 Buitenlandse bijkantoren en dochters van Nederlandse instellingen 11

3 Risicogebaseerd denken: de systematische integriteitrisicoanalyse 13
3.1 Inrichting integriteitbeleid 13
3.2 Opzet systematische integriteitrisicoanalyse (SIRA) 13
3.3 Risicofactoren 16
3.4 Indeling van cliënten in risicocategorieën 18
3.5 Cliënten en producten met verhoogd integriteitrisico 21
3.6 Onacceptabele risico's 22

4 Cliëntenonderzoek 24
4.1 Wettelijk kader 24
4.2 Identificatie en verificatie 25
4.3 Aangaan zakelijke relatie 30
4.4 Niet aangaan van- of beëindiging van de zakelijke relatie 33
4.5 Uiteindelijke belanghebbende (UBO) 35
4.6 Doel en aard zakelijke relatie 38
4.7 Bron van de middelen 38
4.8 Vereenvoudigd cliëntenonderzoek, laag-risico factoren en uitzonderingen op het cliëntenonderzoek 39
4.9 Verscherpt cliëntenonderzoek en hoog-risico factoren 42
4.10 Uitbesteding 51

5 Transactiemonitoring en melden ongebruikelijke transacties 52
5.1 Algemeen 52
5.2 Patronen en transacties herkennen 54
5.3 Aandacht voor hoog-risico jurisdicties 55
5.4 Beoordeling transacties, maatregelen en vastlegging 56

5.5 Meldplicht ongebruikelijke transacties 56
5.6 FIU meldprocedure 60
5.7 Vrijwaringen 60
5.8 Geheimhouding Wwft 61
5.9 Rechtsvorderingen en geheimhouding Wwft 61

6 De Verordening betreffende bij geldovermakingen te voegen informatie (Wire Transfer Regulation 2) 63
6.1 Algemeen 63
6.2 Achtergrond van de WTR2 63
6.3 Toepassingsbereik 63
6.4 Verplichtingen van (intermediaire) betalingsdienstaanbieders 63
6.5 Opsporen en beoordelen van onvolledige informatie 64
6.6 EBA Richtsnoeren 64
6.7 FIU meldingen 64
6.8 Integriteitstoezicht Wwft 65

7 Sanctieregelgeving 66
7.1 Algemeen 66
7.2 Administratieve organisatie en interne controle (AO/IC) 67
7.3 Het 'relatie'-begrip 68
7.4 De controle van transacties 69
7.5 Melden aan DNB 70
7.6 'Hit'-meldingen, FIU-meldingen en termijnen 71

8 Vastlegging, bewaarplicht en de Algemene verordening gegevensbescherming (AVG) 73

1 Inleiding

Integriteit is – naast soliditeit – een voorwaarde voor een gezond financieel stelsel. De Nederlandsche Bank (DNB) houdt integriteittoezicht op een breed scala aan (financiële) instellingen. Dit specifieke toezicht is gebaseerd op de Wet op het financieel toezicht (Wft), de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft), de Pensioenwet (Pw), de Wet toezicht trustkantoren 2018 (Wtt) en de Sanctiewet 1977 (Sw). De Wwft is de implementatie van de Europese richtlijnen ter voorkoming van witwassen en terrorismefinanciering.[1] Deze Europese richtlijn is gebaseerd op de aanbevelingen van de Financial Action Task Force (FATF).

Het doel van het integriteittoezicht is onder andere het voorkomen van het gebruik van het financiële stelsel voor witwassen en financieren van terrorisme. Het toezicht op de naleving van de Wwft is toebedeeld aan DNB voor wat betreft de volgende soorten instellingen: banken, bijkantoren, levensverzekeraars, betaaldienstverleners en -agenten, elektronisch geldinstellingen, wisselinstellingen, trustkantoren en instellingen genoemd in artikel 1a derde lid onder a van de Wwft.[2] Daarnaast moeten deze instellingen ook voldoen aan de Sw. Een ieder in Nederland heeft zich te houden aan de Sw. Bepaalde instellingen vallen onder het toezicht van DNB waaronder pensioenfondsen en verzekeraars.[3]

DNB is belast met de uitvoering en handhaving van de Wwft. Handhaving vindt plaats conform het Handhavingsbeleid van de AFM en DNB aan de hand van de normen die zijn neergelegd in wet- en regelgeving.[4]

In 2011 is op aanbeveling van de FATF een eerste leidraad opgesteld door DNB. Hiermee gaf DNB de onder DNB toezicht staande instellingen handvatten voor het adequaat uitvoeren van de wettelijke verplichtingen die voortvloeien uit de integriteitsregelgeving. In deze vierde versie van de leidraad zijn aanpassingen verwerkt naar aanleiding van de relevante wijzigingen in de Wwft, die per 25 juli 2018 herzien is (Staatsblad nr. 239, 2018) en het Uitvoeringsbesluit Wwft 2018 (Staatsblad nr. 241, 2018). Het wetsvoorstel Wijziging vierde anti-witwasrichtlijn is in deze versie van de Leidraad nog niet meegenomen.

Naast het verwerken van relevante wetswijzigingen zijn bij sommige onderdelen nieuwe *Good practices* toegevoegd, die in de afgelopen jaren uit de toezichtonderzoeken van DNB naar voren zijn gekomen.

1 Richtlijn 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering.
2 De Wwft verwijst naar degenen die, geen bank zijnde, in hoofdzaak hun bedrijf maken van het verrichten van een of meer van de werkzaamheden opgenomen onder de punten 2, 3, 5, 6, 9, 10, 12 en 14 van bijlage I bij de richtlijn kapitaalvereisten.
3 Artikel 1 Aanwijzing rechtspersonen Sanctiewet 1977 verwijst naar artikel 10, tweede lid, onder a, c en e tot en met j, van de Sanctiewet 1977.
4 Zie ook: https://www.toezicht.dnb.nl/5/15/50-204888.jsp.

Deze Leidraad is geen juridisch bindend document of beleidsregel van DNB als bedoeld in artikel 1:3 vierde lid van de Algemene wet bestuursrecht en heeft of beoogt geen rechtsgevolg. Deze Leidraad komt niet in de plaats van wet- en regelgeving en beleidsregels of toezichthouderregelingen op dit gebied. De voorbeelden in deze Leidraad zijn niet uitputtend en zullen niet altijd als voldoende zijn aan te merken voor de naleving van de wettelijke vereisten. Met de Leidraad beoogt DNB een handreiking te doen voor de uitleg en toepassing van de wettelijke verplichtingen.

Deze Leidraad geldt voor de onder toezicht van DNB staande instellingen en is een aanvulling op de "Algemene Leidraad Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) en Sanctiewet (Sw)" van het ministerie van Financiën.[5] Beide leidraden verduidelijken de verschillende verplichtingen uit de Wwft en Sw en bieden handvatten voor de implementatie van deze verplichtingen. De algemene leidraad en Leidraad van DNB dienen in samenhang gelezen te worden. Naast de algemene leidraad bieden de andere Wwft-toezichthouders[6] leidraden voor de onder hun toezicht staande instellingen.

In deze Leidraad wordt verwezen naar internationale (niet bindende) guidance documenten van de FATF, European Banking Authority (EBA), Basel Committee on Banking Supervision (BCBS) en International Association of Insurance Supervisors (IAIS) Hoewel de guidance van deze organisaties veelal op bepaalde sectoren is gericht, is veel van de informatie in deze guidance documenten ook nuttig voor andere sectoren. Daarnaast kunnen voor sommige instellingen de documenten van de Wolfsberg Group bruikbaar zijn.[7]

Relevante wet- en regelgeving

Dit document is een leidraad voor de volgende wet- en regelgeving:

- Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)[8]
- Sanctiewet 1977 en Regeling toezicht Sanctiewet 1977 (Sw)
- (EU) Verordening 2015/847 betreffende bij geldovermakingen te voegen informatie (WTR2)

5 Te raadplegen op: https://www.rijksoverheid.nl/documenten/richtlijnen/2011/02/21/algemene-leidraad-wet-ter-voorkoming-van-witwassen-en-financieren-van-terrorisme-wwft-en-sanctiewet-sw;
6 Wwft-toezichthouders: DNB, AFM, Belastingdienst/Bureau Toezicht Wwft, Bureau Financieel Toezicht, Kansspelautoriteiten en de dekens van de Nederlandse Orde van Advocaten.
7 De Wolfsberg Group is een groep van elf internationale banken, die standaarden ontwikkelt voor de financiële sector op het gebied van 'Ken uw Cliënt/ KYC' en de bestrijding van witwassen en terrorismefinanciering (https://www.wolfsberg-principles.com/).
8 Wettekst van augustus 2019. De wijzigingen tot aan die maand zijn betrokken in deze Leidraad.

2 Inrichting bedrijfsvoering

2.1 Integere bedrijfsvoering

De integriteit van financiële instellingen is één van de pijlers van vertrouwen en een randvoorwaarde voor het goed functioneren van instellingen. Integriteit is ook als expliciete norm opgenomen in de financiële toezichtsregelgeving, de artikelen 3:10 en 3:17 Wft, 143 Pw en art. 14 Wtt bevatten wettelijke vereisten voor het bewaken van een integere bedrijfsvoering. Het gaat er hierbij om dat instellingen voorkomen dat zij betrokken raken bij handelingen die tegen de wet ingaan en/of handelingen die, kort gezegd, maatschappelijk onbetamelijk zijn en dat zij een integere uitoefening van het bedrijf waarborgen. In de uitwerking van deze norm staat de beheersing van integriteitrisico's centraal. De regelgeving (Wft, Bpr, Pw, Wtt, Wwft en Sw) schrijft in essentie een beheersingskader voor, gericht op het beheersen van integriteitrisico's. Deze Leidraad richt zich op de beheersing van de integriteitrisico's: witwassen, terrorismefinanciering en schendingen van sanctieregelgeving. Ook andere onderwerpen vallen onder het begrip integriteitrisico's zoals corruptie, belangenverstrengeling, fraude, en niet-integer fiscaal handelen. Deze integriteitsrisico's worden in deze Leidraad betrokken voor zover er een relatie is met witwassen en/of terrorismefinanciering en de naleving van Wwft verplichtingen.

Verschillende Wwft-plichtige instellingen hebben ook op grond van andere (toezicht)wetten verplichtingen in het kader van de integere bedrijfsvoering in gevolge de Wft, Bpr, Pw en Wtt. Dit is bepalend voor de reikwijdte van de beheersmaatregelen die instellingen treffen om hun integriteitsrisico's te beheersen. De maatregelen die een instelling neemt om betrokkenheid bij witwassen en terrorismefinanciering te voorkomen vormen daar een onderdeel van.

Integriteit bestuurders en werknemers

Aandacht voor de integriteit van bestuurders en werknemers is minstens zo belangrijk als het inrichten van adequate processen, procedures en maatregelen om de integriteitrisico's van een instelling te mitigeren. Dagelijks beleidsbepalers van instellingen dienen, conform de Beleidsregel Geschiktheid 2012, onder andere geschikt te zijn met betrekking tot de integere bedrijfsvoering, en dagelijks beleidsbepalers moet onder meer kunnen waarborgen dat de instelling integriteitrisico's beheerst. De dagelijks beleidsbepalers zijn daarmee eerstverantwoordelijk binnen de instelling voor het toezien op het bestaan, de opzet en adequate werking van het integriteitbeleid. Dit kan bijvoorbeeld door middel van 'mission statements', 'business principles' of strategische beschouwingen. Daarnaast zien de dagelijks beleidsbepalers erop toe dat de instelling geen cliënten accepteert of producten en diensten verleent ten aanzien waarvan de instelling geen kennis of ervaring heeft, verder zien zij bij de ontwikkeling en vóór de introductie van nieuwe producten en diensten erop toe dat voldoende rekening wordt gehouden met de integriteitrisico's. Ten slotte geven de dagelijks beleidsbepalers goedkeuring aan gedragslijnen, procedures en maatregselen die de risico's op witwassen, financieren van terrorisme en schendingen van sanctieregelgeving, en andere relevante integriteitsrisico's, beperken en effectief beheersen.

Het beheersingskader voor integriteitrisico's bestaat in ieder geval uit

- Een systematische analyse van integriteitrisico's (SIRA) waaronder de risico's op witwassen en financieren van terrorisme;[9] (Zie ook: artikel 2b Wwft);
- Het vaststellen van de risicobereidheid (*'risk appetite'*) op basis van de analyse van integriteitrisico's waaronder de risico's op witwassen en financieren van terrorisme;
- Het vaststellen van een adequaat (groeps)beleid gericht op risicobeheersing en integer handelen;
- Het uitwerken en implementeren van de beleidsuitgangspunten in gedragslijnen, procedures en maatregelen (zie ook: artikel 2c Wwft);
- Een systematische toetsing en beoordeling van de toereikendheid van de beheersomgeving, gevolgd door eventueel aanpassing van die beheersomgeving:
- Het inrichten van een compliancefunctie voor zover passend bij de aard en de omvang van de instelling. (zie ook: Artikel 2d Wwft);
- Het zorg dragen voor de uitoefening van een onafhankelijke auditfunctie ten aanzien van haar werkzaamheden voor zover passend bij de bij de aard en de omvang van de instelling. (Zie ook: Artikel 2d Wwft);

Verantwoordelijke Wwft-beleidsbepaler

Op basis van artikel 2d, eerste lid, Wwft wijst een instelling, indien een instelling beschikt over twee of meer beleidsbepalers, één dagelijks beleidsbepaler aan binnen het bestuur die verantwoordelijk is voor de naleving van de Wwft. De aangewezen beleidsbepaler is feitelijk de 'portefeuillehouder Wwft'. Gelet op deze verantwoordelijkheid is een Wwft-beleidsbepaler altijd in voldoende mate op de hoogte van het integriteitbeleid en bijbehorende procedures van de instelling. Daarbij stuurt de Wwft-beleidsbepaler actief op de naleving van betrokken regelgeving en draagt de verantwoordelijkheid voor de uitvoering van het eigen beleid. Tot slot volgt de Wwft-beleidsbepaler (aantoonbaar) relevante opleidingen.

9 Instellingen die alleen onder de Wwft vallen maken een systematische analyse van de risico's op witwassen en financieren van terrorisme op grond van artikel 2b Wwft. De SIRA systematiek zoals omschreven in hoofdstuk 3 wordt hierbij gehanteerd.

DNB Visie op toezicht 2018 – 2022: Streng op financieel-economische criminaliteit

Financieel-economische criminaliteit kent vele verschijningsvormen zoals bijvoorbeeld witwassen, corruptie, financiering van terrorisme, handel met voorwetenschap en het niet naleven van sancties. De bestrijding hiervan heeft hoge prioriteit omdat financieel-economische criminaliteit het vertrouwen in het financiële stelsel kan aantasten. Financiële instellingen hebben een sleutelrol in deze bestrijding door te signaleren en te weren dat criminele geldstromen door het financiële stelsel lopen; de zogenoemde "poortwachtersfunctie".

Bij instellingen die passende maatregelen nemen om financieel-economische criminaliteit te voorkomen, zien we – niet toevallig – veelal eigenaarschap van de poortwachtersrol. Deze onder toezicht staande instellingen zien hun eigen risico's onder ogen, identificeren, analyseren en mitigeren deze risico's, met inzet van de 'three lines of defence'. DNB stuurt er daarom op dat instellingen en bestuurders zelf de verantwoordelijkheid nemen om te voorkomen dat ze betrokken raken bij financieel-economische criminaliteit. De toezichtpraktijk toont aan dat eigenaarschap te vaak beperkt blijft tot de compliance- en in mindere mate de auditfuncties. Robuuste verdedigingslinies met een duidelijke eindverantwoordelijkheid bij het bestuur zijn noodzakelijk.

Meer informatie over de Visie op toezicht

2.2 Opleiding, training en awareness

Bij instellingen hangt de werking van de Wwft en Sw processen en procedures voornamelijk af van de mate van awareness, ervaring en kennis van dagelijks beleidsbepalers en van medewerkers. Toereikende awareness, ervaring en kennis van het personeel van instellingen met betrekking tot de beheersing van de risico's van witwassen en terrorismefinanciering zijn belangrijke voorwaarden voor een effectief beheersingskader. Het opleiden van het personeel is een belangrijke manier om kennis van de Wwft en de Sw, de integriteitbeleidsuitgangspunten en procedures binnen de instelling te communiceren en te borgen.

DNB toetst in haar toezicht in hoeverre instellingen op structurele wijze invulling geven aan hetgeen in artikel 35 Wwft bepaald is.

Instellingen bieden opleidingen aan waardoor het personeel bekend raakt met de bepalingen van de Wwft en de Sw, en die het personeel in staat stellen het cliëntenonderzoek goed en volledig uit te voeren, ongebruikelijke transacties te herkennen en zorgen voor een effectieve naleving van sanctieregelgeving. Deze opleidingen behandelen bijvoorbeeld witwas- en terrorismefinancieringstechnieken, methodes en trends, de internationale context en standaarden, en nieuwe ontwikkelingen op dat gebied.

Omdat de integriteitrisico's dynamisch zijn en de beheersing van instellingen daaraan wordt aangepast is het noodzakelijk dat instellingen de inhoud van hun opleidingen met voldoende regelmaat evalueren en herzien. Om op de hoogte te blijven van de nieuwe ontwikkelingen en de bewustwording blijvend te bevorderen, is een opleiding in de regel niet eenmalig, maar wordt deze regelmatig aangeboden. De frequentie van het aanbod is afhankelijk van het doel, de doelgroep en de inhoud. De opleidingsvormen die instellingen aanbieden sluit hier dan ook bij aan. Instellingen kunnen onder andere denken aan, gecertificeerde opleidingen, (in-house) trainingen, e-learning modules en awareness-sessies.

Om opleidingen zo effectief mogelijk in te richten is het van belang om het aanbod toe te spitsen op de verschillende functies binnen de instelling. Zo zal de inhoud, diepgang en frequentie afhankelijk zijn van de functie die de medewerker bekleedt. Het ligt in de rede dat de compliancefunctie aanvullende opleidingen volgt om op de hoogte te blijven van ontwikkelingen inzake de internationale wet- en regelgeving en witwas- en terrorisme-financieringsrisico's. De dagelijks beleidsbepalers – die belast zijn met de verantwoordelijkheid voor de naleving van de Wwft en Sw – krijgen voldoende opleidingen om hun (eind)verantwoordelijkheid te kunnen dragen.

Een adequate vastlegging van het aanbod, de gevolgde trainingen, de frequentie en van wie opleidingen volgen stelt instellingen in staat om het kennisniveau binnen de organisatie doorlopend vast te stellen, te monitoren en daarop in te spelen.

2.3 Integere bedrijfscultuur

Een integere bedrijfscultuur en integer gedrag zijn essentieel voor de effectiviteit van de integriteitbeheersmaatregelen. Integer gedrag is een professionele, individuele verantwoordelijkheid waarbij iemand zich bewust is van en zorgvuldig rekening houdt met rechten, belangen en wensen van andere belanghebbenden, een open en transparante houding heeft, en bereid is om verantwoordelijkheid te nemen en verantwoording af te leggen over genomen beslissingen en acties. Een integere cultuur doelt vervolgens op een sfeer en klimaat waarin een onderneming zich ook in ruimere zin gedraagt of handelt op een manier die uitlegbaar en te verantwoorden is: niet slechts naar de letter, maar ook naar de geest van de wet handelen.

2.4 Interne klokkenluidersregeling en meldpunt misstanden

Op grond van artikel 20a Wwft beschikken instellingen over procedures, die passend zijn bij de aard en omvang van de instellingen, die werknemers in staat stellen om de door de instelling begane Wwft overtredingen intern te melden. In de memorie van toelichting staat dat de melder van de Wwft overtredingen dit op onafhankelijke en geanonimiseerde wijze moet kunnen melden. Artikel 20a Wwft sluit aan bij de bepalingen in de Wet Huis voor klokkenluiders op basis waarvan werkgevers werknemers in staat stellen een interne klokkenluidersmelding te doen.

Los hiervan kunnen personen misstanden melden bij het Meldpunt Misstanden DNB. Professionals in de financiële sector kunnen in aanraking komen met fraude, corruptie en andere vormen van (ernstige) overtredingen van wet- en regelgeving bij een financiële instelling. DNB verwacht dat een misstand eerst (intern) bij de instelling wordt gemeld. Bijvoorbeeld door gebruik te maken van een interne klokkenluidersregeling (zoals een regeling die gebaseerd is op artikel 20a Wwft). Het DNB Meldpunt Misstanden staat echter open voor wie het rechtstreeks melden bij de betreffende instelling niet goed mogelijk is. Dit kan bijvoorbeeld als er gegronde vrees bestaat voor zware persoonlijke gevolgen. Daarbij is het mogelijk dat er al een interne melding bij de instelling is gedaan maar dat deze melding niet of onvoldoende is opgepakt.

Meer informatie over de interne klokkenluidersregeling.
Meer informatie over het DNB meldpunt misstanden.

2.5 Know your customer (KYC) / Customer due diligence (CDD)

Een onderdeel van een integere bedrijfsvoering is het cliëntenonderzoek. Voor het waarborgen van een integere bedrijfsvoering is het essentieel dat instellingen weten met wie zij een zakelijke relatie aangaan of voor wie zij een incidentele transactie verrichten. De Wft, Wwft verplichten instellingen om hun cliënten te kennen én geen zakelijke relaties aan te gaan met personen die het vertrouwen in de instelling kunnen schaden, met behulp van adequate CDD. De CDD-normen zijn niet alleen relevant voor de integere bedrijfsvoering van instellingen als geheel, maar ook voor het beheersen van de specifieke integriteitrisico's waarop de Wwft betrekking heeft. Aangezien zowel de Wft (integere bedrijfsvoering) als de Wwft de beheersing van integriteitrisico's voor ogen hebben kunnen de maatregelen die door instellingen worden genomen op grond van deze wetten worden geïntegreerd en kan op eenzelfde wijze invulling worden gegeven aan de vereisten van de Wwft en de Wft.[10] Het hoofddoel is dat de instelling weet met wie zij zaken doet, waarvoor de zakelijke relatie gebruikt wordt, en dat de instelling dit doorlopend op risicogebaseerde wijze controleert. Zie voor een nadere uitwerking navolgend hoofdstuk 4 'cliëntenonderzoek' en hoofdstuk 5 'transactiemonitoring en melden ongebruikelijke transacties'.

2.6 Sanctieregelgeving

Met de Sw en de regelingen op grond van die wet wordt nationaal uitvoering gegeven aan internationale sanctieregimes, die van de Verenigde Naties en de Europese Unie. Via de Sw worden bepalingen in deze internationale sanctieregimes nationaal geldende normen. Het overtreden van voorschriften die gesteld worden bij of krachtens de Sw, waartoe internationale sanctieregimes

10 Zie brief van de minister van Financiën aan de Tweede Kamer van 15 oktober 2008 (Kamerstuk 31237, nr. 9).

kunnen horen, is strafbaar gesteld in de Wet op de economische delicten. Het accent ligt hierbij op het strafbaar stellen van de overtreding van bepalingen die in Europese verordeningen zijn neergelegd.

De Regeling toezicht Sanctiewet 1977 (Rtsw) van AFM en DNB biedt financiële instellingen een kader om maatregelen te treffen. Er zijn twee soorten financiële sancties te onderscheiden: een gebod tot het bevriezen van tegoeden en een verbod of restricties op het verlenen van financiële diensten. Deze sancties zien op voorkomen van ongewenste handel (embargo's) en het voorkomen en bestrijden van terrorisme. Met hun maatregelen waarborgen instellingen dat zij in staat zijn relaties te identificeren die overeenkomen met (rechts)personen en entiteiten als bedoeld in de sanctieregelgeving. Vervolgens voorkomen instellingen dat zij financiële middelen of diensten ter beschikking stellen aan die relatie, en dat zij de financiële middelen van die relatie kunnen bevriezen. In hoofdstuk 7 wordt verder ingegaan op de sanctieregelgeving.

2.7 Buitenlandse bijkantoren en dochters van Nederlandse instellingen

Op basis van artikel 2 Wwft zorgt een instelling met een bijkantoor of een meerderheids-dochteronderneming (dochterondernemingen) buiten de Europese Unie of de Europese Economische Ruimte (een staat waar de wettelijke voorschriften ter voorkoming van witwassen en financieren van terrorisme minder verstrekkend zijn dan die van de Wwft) ervoor dat haar bijkantoor of dochteronderneming de Wwft naleeft. Internationaal opererende instellingen met een zetel in Nederland definiëren groepsbeleid en procedures voor de naleving van de Wwft die gelden voor de gehele groep. Daarnaast zorgen deze instellingen ervoor dat het groepsbeleid en de procedures effectief worden toegepast. Dit betekent dat de integriteitbeheersmaatregelen in ieder geval worden toegepast ten aanzien van de gehele bedrijfsvoering, alle functionele activiteiten, cliënten en producten wereldwijd. Het kan voorkomen dat een instelling opereert in jurisdicties (niet EU-lidstaten) waar de lokale wet- en regelgeving minder verstrekkende voorschriften stellen dan het vastgestelde groepsbeleid. Instellingen passen in die gevallen de meer verstrekkende eisen van de groep binnen die bijkantoren en dochterondernemingen toe. Indien de lokale wet- en regelgeving meer verstrekkende eisen stelt aan integriteitbeheersmaatregelen dan het groepsbeleid, houdt de instelling zich aan de nationale wetgeving en past daarmee het groepsbeleid lokaal aan. Tot slot kan het voorkomen dat lokale wetgeving in een niet EU-lidstaat de naleving van de Wwft belemmert. Indien instellingen dit constateren melden instellingen dit aan DNB en nemen zij maatregelen om de potentiele risico's doeltreffend te beheersen.

Technische reguleringsnormen: belemmeringen in derde landen.

Vanaf 3 september 2019 gelden de 'Regulatory Technical Standards' (RTS) inzake 'de minimumactie en de soort bijkomende maatregelen waartoe krediet- en financiële instellingen verplicht zijn met het oog op het beperken van het witwasrisico en het risico van terrorismefinanciering in bepaalde derde landen'.

In deze RTS staan situaties omschreven van mogelijke wettelijke belemmeringen waar instellingen in niet EU-lidstaten tegenaan kunnen lopen, hoe instellingen dienen om te gaan met deze belemmeringen en op welke wijze belemmering gemeld dienen te worden. Dergelijke wettelijke belemmeringen meldt een instelling bij DNB.

3 Risicogebaseerd denken: de systematische integriteitrisicoanalyse

3.1 Inrichting integriteitbeleid

Het regelgevend kader voor een adequaat integriteitbeleid en meer specifiek, het beheersen van het risico op witwassen en terrorismefinanciering, is risicogebaseerd. Dit betekent dat instellingen de maatregelen toepassen die de wet voorschrijft, terwijl de intensiteit waarmee zij dat doen is afgestemd op de risico's die bepaalde cliënten (waaronder de uiteindelijk belanghebbende (UBO) van de cliënt), producten, transacties, diensten, leveringskanalen (de wijze waarop doorgaans het contact met de cliënt plaatsvindt) en land- of geografie met zich meebrengen. Ten aanzien van deze risico's zijn er factoren die duiden op een hoger witwas- of terrorismefinancieringsrisico, dit worden de risicofactoren genoemd (hoofdstuk 3.3 gaat hier verder op in).

Het raamwerk van de Wft (dat een integere bedrijfsvoering vereist) en de Wwft gaat er van uit dat instellingen op basis van het onderscheid in aard en omvang van het risico cliënten indelen in risicocategorieën. Dit stelt de eigen verantwoordelijkheid van instellingen voorop: zij maken zelf een inschatting van de relevante risico's en stellen daar vervolgens voldoende mitigerende maatregelen tegenover. De risicocategorieën variëren van laag- tot hoog-risico, en de indeling geschiedt op basis van objectieve en kenbare factoren. Hoe hoger de risico's, des te meer inspanningen de instelling verricht om die risico's te mitigeren (zie 3.4 'Indeling van cliënten in risicocategorieën').

Van belang is dat de instelling haar afwegingen op systematische en consequente wijze maakt en vastlegt, zodanig dat deze voor een toezichthouder of andere derde[11] te volgen en te beoordelen zijn. Dit geldt zowel voor het formuleren van beleid als voor het besluiten tot het maken van uitzonderingen op dat beleid. In de uitvoering van haar toezichthoudende taak toetst DNB de risicogebaseerde aanpak van instellingen.

3.2 Opzet systematische integriteitrisicoanalyse (SIRA)

Het voorkomen van betrokkenheid bij integriteitsschendingen waaronder witwassen en terrorismefinanciering begint voor instellingen bij het identificeren van de inherente integriteitrisico's die zij lopen door, onder meer, hun dienstverlening aan klanten. Met inherente risico's worden de kwetsbaarheden bedoeld van instellingen om gebruikt te worden voor bijvoorbeeld witwassen en financieren van terrorisme door de dienstverlening die zij bieden. Om hun kwetsbaarheden te kunnen onderkennen, te accepteren (binnen de 'risk appetite') of juist te vermijden[12] dienen instellingen een systematische analyse van de integriteitrisico's (SIRA) op te stellen en deze periodiek te herzien. Het opstellen van een SIRA is een verplichting die al eerdere voortvloeide uit de Wft maar nu ook als verplichting is opgenomen in de Wwft. De risicoanalyse uit de Wwft richt zich op witwassen en terrorismefinanciering, de risicoanalyse uit de Wft

11 Denk hierbij bijvoorbeeld aan partijen met een controlerende taak zoals de auditfunctie.
12 Zie ook de Good Practice 'Integrity Risk Appetite'. Te raadplegen op: http://www.toezicht.dnb.nl/binaries/50-236706.pdf.

kent een bredere reikwijdte.[13] Instellingen houden bij het opstellen van de SIRA rekening met de voor hun relevante risicofactoren. De SIRA houdt in ieder geval in dat de instelling deze periodiek uitvoert volgens een vooraf vastgestelde methodiek. Hierna legt de instelling de uitkomsten daarvan schriftelijk vast.

De inhoud van de SIRA is afhankelijk van de organisatie en de activiteiten van de betreffende instelling. Een instelling van een grotere omvang met een complexe dienstverlening op internationale markten zal met meer risico's rekening dienen te houden dan een instelling van een kleinere omvang met eenvoudige dienstverlening en simpele producten. Ook hier is het kernbegrip: risicogebaseerd. Meer informatie over hoe een SIRA wordt opgesteld is te vinden in de *Good Practices* van DNB getiteld "De Integriteitrisicoanalyse – meer waar dat moet, minder waar dat kan".

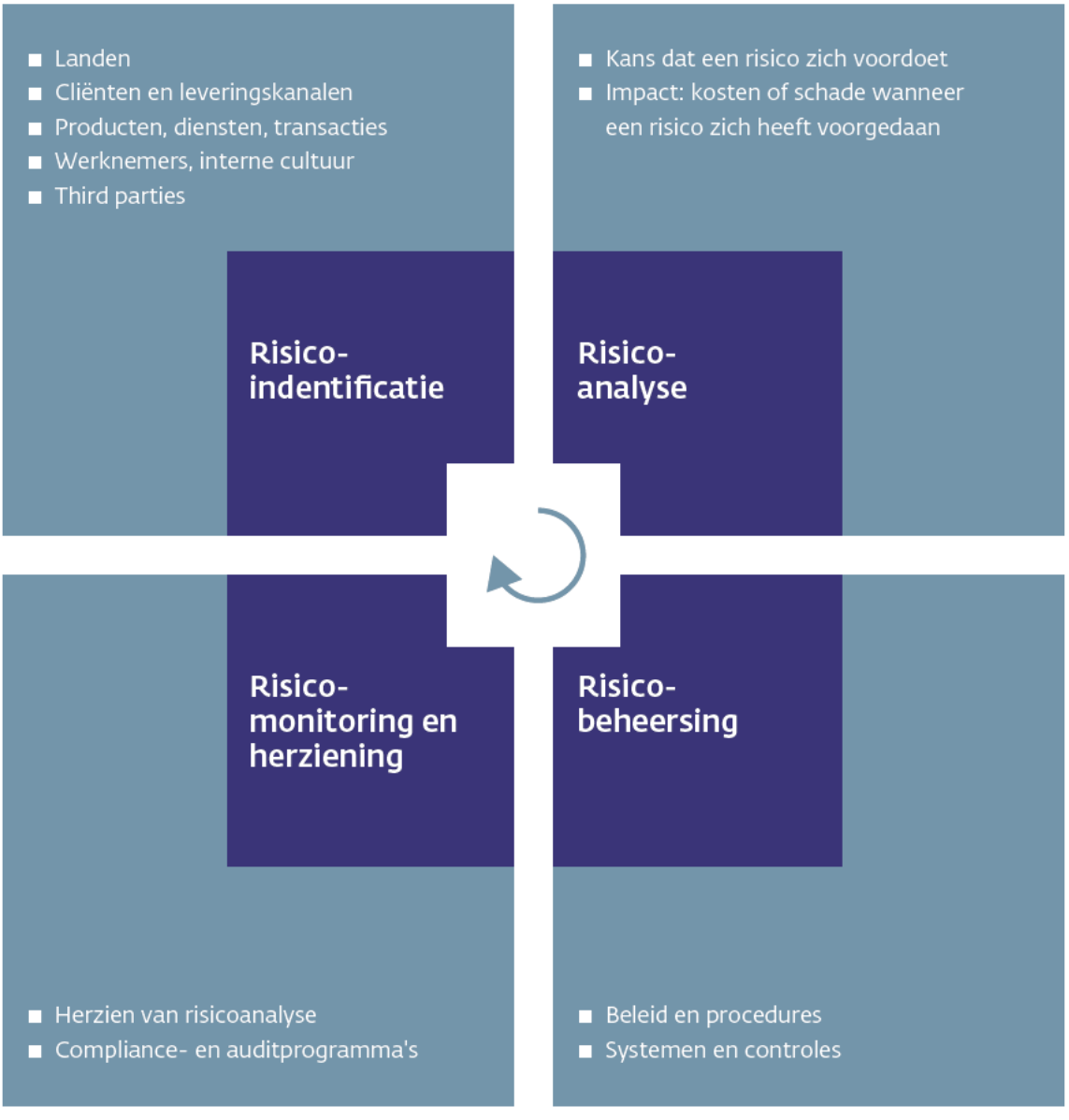
Het analyseren van de integriteitrisico's kent vier stappen:

1. **Risico-identificatie**: het identificeren van die gebieden van de dienstverlening die kwetsbaar zijn voor integriteitrisico's, zoals witwassen en terrorismefinanciering
2. **Risicoanalyse**: het uitvoeren van een risicoanalyse om de kans en impact van integriteitrisico's, zoals witwassen en terrorismefinanciering, te beoordelen
3. **Risicobeheersing**: het opstellen en vormgeven van de risicobeheersing; en
4. **Risicomonitoring en herziening**: het monitoren van de risico's en herzien van de risicoanalyse.

Good practices – De integriteitrisicoanalyse (SIRA)
In de Good practices 'De integriteitrisicoanalyse, meer waar dat moet, minder waar het kan' biedt DNB praktische handvatten voor het opstellen en uitvoeren van de SIRA.

Good practices – Integrity Risk Appetite (SIRA)
In deze Good practices staan de belangrijkste aandachtspunten voor een financiële instelling die de integriteitrisico's voor zichzelf in kaart wil brengen en wil analyseren in welke mate zij deze wenst te accepteren of vermijden.

13 Ingevolge artikel 2b Wwft stellen financiële instellingen een systematische risicoanalyse op. Deze verplichting geldt voor alle in de Wwft genoemde instellingen. Daarnaast volgt de systematische integriteitrisicoanalyse verplichting voor bepaalde financiële instellingen uit artikel 3:10, 3:17 Wft, artikel 10 Bpr, artikel 19 Besluit financieel toetsingskader pensioenfondsen en artikel 14 Besluit uitvoering Pensioenwet. De SIRA heeft voor de laatstgenoemde instellingen een bredere reikwijdte met als overkoepelend begrip integriteitrisico's. Zie ook de omschrijving in hoofdstuk 2.1.


Landen
Cliënten en leveringskanalen
Producten, diensten, transacties
Werknemers, interne cultuur
Third parties
Risico-indentificatie
Kans dat een risico zich voordoet
Impact: kosten of schade wanneer een risico zich heeft voorgedaan
Risico-analyse
Risico-monitoring en herziening
Herzien van risicoanalyse
Compliance- en auditprogramma's
Risico-beheersing
Beleid en procedures
Systemen en controles

3.3 Risicofactoren

De factoren die een integriteitrisico met zich meebrengen hebben betrekking op: cliënten, diensten, producten, transacties, leveringskanalen en land- of geografie en zijn het uitgangspunt voor de identificatie en beoordeling van integriteitrisico's. Bij het opstellen van een integriteitrisicoanalyse kijkt de instelling in de eerste plaats naar de kenmerken van cliënten. Gedacht kan worden aan branches of beroepen[14], ingezetenschap, vermogen, inkomstenbron, en fiscale integriteitrisico's.[15] Hierbij is ook relevant hoe doorgaans het contact met cliënten tot stand komt en de wijze waarop diensten worden aangeboden (de zogenaamde leveringskanalen, bijvoorbeeld wel of niet in persoon, via tussenpersonen, telefonisch of online). Tot slot speelt land- of geografie een rol, dit zijn de landen en regio's waar de instelling zelf actief is, en de landen waar de cliënten gevestigd zijn of activiteiten ondernemen.

Het toepassen van de risicofactoren stelt de instelling ook in staat om haar cliënten in te delen in risicocategorieën. Hierbij kijkt de instelling niet alleen naar risicofactoren die betrekking hebben op de cliënt maar naar een combinatie van factoren die bijvoorbeeld raken aan product, dienst, transactie, leveringskanaal, land- of geografie (zie hoofdstuk 3.4).

Bij het identificeren van de risico's passen instellingen de voor hen relevante risicofactoren toe. Vervolgens schatten zij de hoogte van hun risico's in. De instelling beoordeelt hierna de kans dat een bepaald risico van witwassen of terrorismefinanciering zich voordoet, en, zo ja, wat de impact is. Het gewicht dat een instelling aan elke risicofactor toekent om het overall risico op witwassen en terrorismefinanciering te bepalen kan per instelling verschillen. Belangrijk is dat instellingen met inachtneming van wet- en regelgeving zelfstandig de risicofactoren afwegen. De Wwft beschouwt immers bepaalde typen cliënten (zoals PEP's) of bepaalde soorten dienstverlening (zoals dienstverlening aan correspondentrelaties) per definitie als hoog-risico.

De geïdentificeerde integriteitrisico's zijn uiteraard niet statisch, maar dynamisch. Zo kunnen bijvoorbeeld (risicovolle) activiteiten van de instelling wijzigen. Verder kunnen zich bepaalde trends voordoen binnen het financieel–economische verkeer, ook wet- en regelgeving kan wijzigen. De SIRA is daarom ook een levend document, dat regelmatig wordt aangepast aan de nieuwste in- en externe ontwikkelingen en de risk appetite van de instelling.

14 Sommige branches of beroepen brengen specifieke risico's met zich mee. Zie bijvoorbeeld de Factsheet 'Integriteitrisico's rond de voetbalsport'. Te raadplegen op: https://www.toezicht.dnb.nl/binaries/50-237528.pdf.

15 Met fiscale integriteitrisico's wordt het risico bedoeld op het faciliteren van belastingontduiking en het daarmee samenhangende witwasrisico. Lees meer over fiscale integriteitrisico's in de DNB Good practices fiscale integriteitrisico's banken en de Good practices fiscale integriteitrisico's trustkantoren. Te raadplegen op: https://www.toezicht.dnb.nl/5/50-237753.jsp en https://www.toezicht.dnb.nl/7/50-237536.jsp.

Hieronder is een overzicht van voorbeelden van risicofactoren opgenomen. Dit overzicht van risicofactoren is niet-limitatief en generiek van aard. Dit betekent enerzijds dat instellingen zelf alert moeten zijn op andere factoren die een indicatie zijn van het risiconiveau. Anderzijds betekent dit dat het kan zijn dat de instelling tot de conclusie komt dat bepaalde factoren voor hun situatie niet van toepassing zijn of reeds in voldoende mate gemitigeerd worden. Voor meer voorbeelden wijst DNB instellingen op de 'Risk Factors Guidelines' van de gezamenlijke Europese toezichthouders op de financiële markten (European Banking Authority, European Securities and Markets Authority en European Insurance and Occupational Pensions Authority). Deze guidelines bevatten een nadere uitwerking van relevante risicofactoren gerelateerd aan witwassen en terrorisme financiering per financiële sector.

Op basis van artikel 2c moeten instellingen in hun gedragslijnen, procedures en maatregelen in ieder geval rekening houden met de risico's genoemd in

Mogelijke risicofactoren met betrekking tot cliënten, diensten, producten, transacties en leveringskanalen en land- of geografie.

Zie voor uitgewerkte risicofactoren die relevant zijn voor verschillende sectoren de 'Risks Factors Guidelines' van de European Supervisory Authorities (EBA, ESMA en EIOPA).

In bijlage II en III van de vierde anti-witwasrichtlijn staan factoren van een potentieel lager en potentieel hoger risico opgenomen.

De Financial Action Task Force geeft in haar 'interpretive note' bij Recommendation 10 (Customer Due Diligence) voorbeelden van risicofactoren. Zie de website van de FATF voor haar Recommendations.

De Financial Action Task Force wijst landen aan waar tekortkomingen zijn geconstateerd in de bestrijding van witwassen en financieren van terrorisme. De zogenaamde 'High-risk and other monitored jurisdictions'. Raadpleeg de FATF website voor de actuele landenlijst.

De Europese Commissie wijst landen aan waar tekortkomingen zijn geconstateerd in de bestrijding van witwassen en financieren van terrorisme. Raadpleeg de website 'EU Policy on High-Risk Third Countries' voor de actuele landenlijst.

Tot slot houdt de Europese Commissie een lijst bij van 'niet-coöperatieve rechtsgebieden voor belastingdoeleinden'. Landen die tekort schieten bij het tegengaan van belastingfraude, belastingontduiking en belastingontwijking.

de Supranationale risicobeoordeling en de nationale risicobeoordeling. De Europese Commissie brengt tweejaarlijks de 'Supranational Risk Assessment' (SNRA) uit waarin de grootste witwas- en terrorismefinancieringsrisico's omschreven staan voor de Europese Unie. Het Ministerie van Financiën en het Ministerie van Justitie en Veiligheid brengen verder periodiek twee 'National Risk Assessments (NRAs)' uit waarin de grootste witwas- respectievelijk terrorismefinancieringsrisico's omschreven worden voor Nederland.[16] Daarnaast wordt voor de Caribische eilanden Bonaire Sint Eustatius en Saba een aparte NRA uitgebracht.

(Supra)national Risk Assessment

Zie voor Europese en nationale witwas- en terrorismerisico's de 'Supra-National Risk Assessment' op de website van de Europese Commissie en de 'National Risk Assessments' op de website van het Wetenschappelijk Onderzoek- en Documentatiecentrum.

3.4 Indeling van cliënten in risicocategorieën

Op basis van de risicoanalyse bepaalt de instelling haar integriteitbeleid en bijbehorende procedures. Onderdeel van het beleid is de wijze waarop de instelling het gehele cliëntenbestand indeelt in risicocategorieën. De instelling houdt hierbij rekening met alle factoren (zie 3.3 risicofactoren) die mogelijk van invloed kunnen zijn op het integriteitrisico dat de zakelijke relatie met een cliënt meebrengt.

De instelling documenteert de systematiek voor de indeling schriftelijk in bijvoorbeeld het cliëntacceptatiebeleid. Zij bepaalt zelf hoeveel risicocategorieën worden gehanteerd en waarborgt daarbij dat het beleid aansluit bij de aard, omvang en complexiteit van de risicofactoren van de instelling. Dit kan betekenen dat een instelling die meerdere verschillende diensten aanbiedt aan verscheidene cliëntgroepen meer risiconiveaus hanteert in haar indeling. In samenhang met de risicocategorieën die de instelling hanteert wordt bepaald met welke frequentie cliëntendossiers herzien worden. Indien er aanleiding voor is, bijvoorbeeld vanwege wijzigingen aan de zijde van de cliënt, kan ook een 'event-driven' herziening plaatsvinden van het cliëntendossier. Een instelling bedenkt zelf onder welke omstandigheden een 'event-driven' herziening plaatsvindt. Het is aan de instelling om haar cliëntendossiers actueel te houden.[17] Indien een instelling enkel de 'event-driven' herziening van cliëntendossiers hanteert is het vanzelfsprekend dat de scenario's die een 'event-driven' herziening op gang brengen aantoonbaar voldoende effectief zijn.

Naast het indelen van cliënten in risicocategorieën stellen instellingen een risicoprofiel op van een individuele cliënt én monitoren aan de hand daarvan

16 Voor de meest recente versie van de National Risk Assessments, zie de website van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) op https://www.wodc.nl/.
17 Artikel 3, elfde lid, van de Wwft. Daarnaast wordt ook in het kader van het vereenvoudigd cliëntenonderzoek en verscherpt cliëntenonderzoek van instellingen verlangd dat zij gegevens actueel houden op grond van artikel 6, derde lid en artikel 8, elfde lid, van de Wwft.

onder meer de relatie. Bij het opstellen van een risicoprofiel van de cliënt worden de relevante risicofactoren in aanmerking genomen. Uiteindelijk heeft een instelling inzicht in de rationaliteit en passendheid van de transacties en producten voor die cliënt zodat signalen van witwassen en terrorisme financiering daarbij opvallen. Voor meer informatie zie hoofdstuk 5.

Diensten en producten die een instelling levert, kunnen ook ingedeeld worden naar risico. Sommige producten vertegenwoordigen naar hun aard een hoger integriteitrisico. In algemene zin hebben eenvoudige producten en producten met een lange termijn waarop voordelen kunnen worden gerealiseerd een inherent lager integriteitrisico dan complexe producten en producten met een korte looptijd. Toch zijn dit slechts vuistregels, het integriteitrisico wordt per product ingeschat waarbij ook andere risicofactoren, zoals bijvoorbeeld land en leveringskanaal, worden meegewogen. Naast de hier genoemde risico-categorieën houdt de instelling ook met andere, nieuwe, risico's rekening: bijvoorbeeld risico's die kunnen ontstaan door het gebruik van nieuwe technologieën.

In de zakelijke relatie met een cliënt kunnen onder meer de volgende risico-indicatoren zich voordoen:

- het doel van de te openen rekening of de relatie die wordt aangegaan,
- de hoeveelheid te deponeren tegoeden door een cliënt, of de omvang of bestemming van de uit te voeren transacties,
- de mate en wijze waarop een cliënt onder toezicht staat (zoals een financiële instelling),
- de intensiteit en duur van de cliëntrelatie,
- achtergronden van de cliënt, zoals inwoners van geografische gebieden met een lager of hoger witwas- en/of terrorismefinancieringsrisico,
- het gebruik van 'corporate vehicles' of andere structuren die geen aanwijsbaar (commercieel) doel hebben en complexiteit of intransparantie met zich meebrengen.
- fiscale risico-indicatoren. Zie hiervoor de DNB Good practices fiscale integriteitrisico's banken[18] en trustkantoren.

In de vierde anti-witwasrichtlijn staan niet-limitatieve lijsten opgenomen van potentieel lager- en hoger risicofactoren.

18 De Good practices fiscale integriteitsrisico's bij cliënten van banken is te raadplegen op: https://www.toezicht.dnb.nl/5/50-237753.jsp.

Voorbeeld risicocategorisering

Risicocategorie	Voorbeelden	Frequentie review
Laag risico	■ standaarddiensten voor particulieren (spaarrekeningen, salarisrekening, creditcard betalingen voor lage bedragen, etc.) ■ standaarddiensten voor commerciële relaties van kleine omvang (rekening courant faciliteiten etc.) ■ levensverzekeringen met een laag bedrag aan jaarlijkse premie of een lage eenmalig premie ■ pensioenproducten	Bijvoorbeeld elke 3 tot 5 jaar
Normaal risico	■ rekeningen en routinematige internationale (documentaire) betalingen voor middelgrote en grote ondernemingen ■ routinematige en standaard producten en diensten met betrekking tot private banking ■ correspondentbankrekeningen voor banken onderhevig aan gelijkwaardige wetgeving als de Wwft	Bijvoorbeeld 2 tot 3 jaar
Hoog risico	■ complex gestructureerde financieringstransacties of zekerhedenconstructies aan particulieren ■ PEP's of cliënten die transacties verrichten waar PEP's bij betrokken zijn ■ bankproducten en dienstverlening die naar zijn aard vatbaar is voor onoorbaar gebruik (bijvoorbeeld back-to-back leningen, grote contante stortingen, zakelijke vastgoedactiviteiten) ■ cliënten met transacties van/naar gesanctioneerde landen (waaronder handelssancties), free trade zones, offshore centra, tax havens en landen waarvoor de FATF in het kader van het zogenoemde ICRG-proces waarschuwt ■ cliënten met frequente, niet routinematige, complexe treasury en private banking producten en diensten ■ niet-routinematig, grensoverschrijdend betalingsverkeer door niet-cliënten ■ correspondentbankrekeningen met banken uit jurisdicties met zwakke wetgeving op het gebied van bestrijden van witwassen en terrorismefinanciering	Bijvoorbeeld jaarlijks

3.5 Cliënten en producten met verhoogd integriteitrisico

Bepaalde typen cliënten of producten kunnen een inherent verhoogd integriteitrisico met zich meebrengen. Deze typen kunnen naar voren komen uit de eigen risicoanalyse van een instelling. Denk bijvoorbeeld aan bedrijven met een hoge mate van inkomend cash geld, waarvan de herkomst minder makkelijk te bepalen is, zorgt ervoor dat de instelling bij dit type cliënten extra maatregelen moet treffen om het integriteitrisico te mitigeren. Niet alleen bij cash geld is de herkomst minder makkelijk te bepalen. Ook bij nieuwe betaalmethoden zoals crypto's is de herkomst van het vermogen lastig vast te stellen.

Een ander voorbeeld van een mogelijk verhoogd (fiscaal) risico is het samenspel van grensoverschrijdende transacties en cliënten met een complexe internationale bedrijfsstructuur. De verhoogde inherente risico's die bepaalde cliënten en producten met zich meebrengen kunnen door het nemen van maatregelen worden gemitigeerd. Maatregelen om het verhoogde integriteitrisico te mitigeren zijn bijvoorbeeld het stellen van een limiet aan de transacties, het verlangen van meer transparantie door de cliënt en het verlangen van girale betalingen door de cliënt. Een verhoogd risico betekent dus niet dat dit type cliënten categoraal geweigerd moet worden.[19]

De Europese Commissie heeft in bijlage III van de vierde anti-witwasrichtlijn bepaalde factoren geïdentificeerd die wijzen op een inherent verhoogd risico. Artikel 8, tweede lid, van de Wwft bepaalt dat instellingen tenminste rekening te houden met deze risicofactoren. Naast de in bijlage III genoemde risicofactoren kan DNB met een beleidsuiting ook aangeven bij welke activiteiten zij een verhoogd risico ziet. Zakelijke vastgoedactiviteiten zijn hiervan een goed voorbeeld, omdat zij naar hun aard een hoger risico op fraude en witwassen met zich meebrengen vanwege de relatief hoge waarde van vastgoedobjecten, de vaak ondoorzichtige prijsvorming en de complexiteit van transacties. DNB heeft in 2011 de beleidsregel 'Integriteitbeleid ten aanzien van zakelijke vastgoedactiviteiten' gepubliceerd. De beleidsregel geeft aan dat instellingen dit verhoogde witwasrisico met adequaat integriteitbeleid moeten afdekken.

Internationale Guidance en aanvullende informatie: vastgoed en professionele witwastechnieken

FATF, 'Money Laundering and Terrorist Financing through the real estate sector', 2007,
Financieel Expertise Centrum, 'Rapportage project vastgoed', 2008,
Financieel Expertise Centrum, 'Red flags Misbruik Vastgoed-actualisering 2010', juni 2010,

FATF, 'Professional Money Laundering', 2018

19 Zie ook de brief van de minister van Financiën van 18 januari 2010 aan de Tweede Kamer die weergeeft welke afspraken er met de Nederlandse Vereniging van Banken zijn gemaakt ten aanzien van betaalfaciliteiten voor integriteitgevoelige sectoren https://zoek.officielebekendmakingen.nl/kst-27863-35.html.

3.6 Onacceptabele risico's

Een instelling kan op basis van het cliëntenonderzoek en het vastgestelde risicoprofiel concluderen dat een bestaande of voorgenomen relatie met een cliënt te grote integriteitrisico's met zich brengt. Daarnaast kan het voorkomen dat het cliëntenonderzoek mislukt, bijvoorbeeld door het ontbreken van noodzakelijke informatie, waardoor de instelling niet kan vaststellen wie haar cliënt precies is en/of welk doel de voorgenomen zakelijke relatie heeft, en of de beoogde dienstverlening passend is. Dit kan gebeuren bij de aanvang van de relatie, maar ook gedurende de relatie, wanneer de eisen aan het cliëntacceptatieproces worden aangescherpt naar aanleiding van interne en/of externe ontwikkelingen.

In de bovengenoemde gevallen gaat de instelling geen zakelijke relatie aan met de cliënt of verbreekt zij de zakelijke relatie bij de eerstvolgende mogelijkheid. Deze verplichting vloeit voort uit artikel 5, derde lid, van de Wwft. Indien er indicaties zijn dat de cliënt betrokken is bij witwassen of het financieren van terrorisme, is zij op grond van artikel 16, vierde lid, van de Wwft daarbij verplicht een melding te doen bij de Financiële Inlichtingen Eenheid (FIU-NL), zie hoofdstuk 5.6 voor meer informatie. Om te waarborgen dat aan al deze verplichtingen wordt voldaan en op een adequate manier afscheid kan worden genomen van bestaande cliënten, stelt de instelling een cliëntexitbeleid op. Hierin geeft zij aan onder welke omstandigheden en volgens welke procedure en termijn de relatie met de cliënt wordt beëindigd.

Voorbeelden van onacceptabele risico's:

- Problemen bij het verifiëren van de identiteit van de cliënt of de UBO;
- Cliënten die anoniem wensen te blijven dan wel fictieve identiteitsgegevens verstrekken;
- Shellbanks (banken die geen fysieke aanwezigheid hebben in het land waar ze gevestigd zijn en een vergunning hebben);
- De cliënt staat op een sanctielijst;
- Cliënten waarvan blijkt dat, op basis van nadere informatie uit bijvoorbeeld EVA, VIS of anderszins, de combinatie van cliënt met de producten die deze wil afnemen onacceptabele risico's met zich meebrengt;
- Cliënten die geen of onvoldoende informatie willen verstrekken over (dan wel ontoereikende documentatie ter verificatie daarvan kunnen overleggen) de aard en achtergrond van de cliënt, het doel van de zakelijke relatie, en in het bijzonder de bron van de middelen van de cliënt;
- Organisatiestructuur van de cliënt of het doel van de structuur waar de doelvennootschap toe behoort blijkt na onderzoek complex of niet transparant, gelet op de activiteiten van de cliënt, zonder dat hier een logische, bedrijfseconomische verklaring aan ten grondslag ligt;
- Professionele tegenpartijen die niet over de vereiste vergunningen beschikken, zogenaamde illegale financiële ondernemingen. NB: Zowel DNB als de AFM beschikken over openbare registers waarin de toegelaten financiële instellingen zijn opgenomen. Hierin kan worden nagegaan of een instelling over een vergunning of registratie beschikt.
- (Beoogd) cliënt geeft de instelling onvoldoende inzicht met betrekking tot structuren, geldstromen en/of zijn fiscale motieven.

4 Cliëntenonderzoek

4.1 Wettelijk kader

De Wwft verplicht instellingen om cliëntenonderzoek te verrichten. Voor een groot gedeelte mag een instelling de mate van het cliëntenonderzoek op een op risico gebaseerde wijze vorm te geven.[20] Dit betekent dat de instelling in elk geval cliëntenonderzoek doet, maar dat de intensiteit van het onderzoek (mede) wordt bepaald door de risico's die bepaalde typen cliënten, producten, diensten, leveringskanelen, transacties en landen- of gebieden met zich meebrengen. Instellingen treffen daarbij extra mitigerende maatregelen in gevallen waar een hoger risico bestaat op witwassen en/of financiering van terrorisme. Dit alles stelt de eigen verantwoordelijkheid van de instelling voorop: de instelling spant zich in om op de hoogte te zijn van technieken en methodologieën van witwassen en financieren van terrorisme, actuele ontwikkelingen, relevante risico-indicatoren en verwerkt dit in beleid, procedures en maatregelen.

Het cliëntenonderzoek stelt de instelling in staat om:

- de cliënt te identificeren, en zijn of haar identiteit te verifiëren;
- de uiteindelijk belanghebbende (UBO's) van een cliënt te identificeren en redelijke maatregelen te nemen om zijn identiteit te verifiëren
- indien de cliënt een rechtspersoon is: redelijke maatregelen te nemen om inzicht te verwerven in de eigendoms- en zeggenschapsstructuur van de groep waartoe een cliënt behoort;
- het doel en de beoogde aard van de zakelijke relatie vast te stellen.
- een voortdurende controle op de zakelijke relatie en de tijdens de duur van deze relatie verrichte transacties uit te oefenen om zich ervan te verzekeren dat deze overeenkomen met de kennis die de instelling heeft van de cliënt en diens risicoprofiel, met zo nodig een onderzoek naar de bron van de middelen die bij de zakelijke relatie of de transactie gebruikt worden (zie hoofdstuk 5)
- vast te stellen of de natuurlijke persoon die de cliënt vertegenwoordigt daartoe bevoegd is en wanneer er inderdaad sprake is van vertegenwoordiging de natuurlijke persoon te identificeren en diens identiteit te verifiëren;
- redelijke maatregelen te nemen om te verifiëren of de cliënt ten behoeve van zichzelf optreedt dan wel ten behoeve van een derde.

20 Het cliëntenonderzoek wordt beslagen door artikelen 3 tot en met 11 Wwft.

De instelling beschikt op het moment van het aangaan van de relatie dan ook over voldoende documenten en gegevens om de cliënt te kunnen accepteren en bovengenoemde resultaten te realiseren. Het gaat dan tenminste om de informatie en gegevens opgesomd in artikel 33, tweede lid.[21]

Succesvol cliëntenonderzoek heeft als resultaat dat instellingen weten met wie zij zaken doen en dat alle relevante risico's in beeld zijn. Instellingen die niet met zekerheid de identiteit van hun cliënten vaststellen, lopen daardoor een onacceptabel hoog risico om gebruikt te worden voor witwassen of het financieren van terrorisme.

4.2 Identificatie en verificatie

4.2.1 Algemeen

Het begrip 'cliënt' is ruim gedefinieerd in de Wwft. Het betreft de "natuurlijke persoon of rechtspersoon met wie een zakelijke relatie wordt aangegaan of die een transactie laat uitvoeren". Een cliënt is een ieder met wie een zakelijke, professionele, of commerciële relatie wordt aangegaan die verband houdt met de professionele activiteiten van de instelling. Tot de professionele activiteiten behoren de hoofdactiviteiten van een instelling die bijvoorbeeld onder de vergunning vallen. Echter, als een instelling andere activiteiten verricht die een financiële component hebben waarbij er een risico op witwassen of terrorismefinanciering is, dan dient de instelling ook voor deze activiteiten de Wwft toe te passen.

Deze ruime definitie betekent dat ook relaties met professionele tegenpartijen in het kader van de kernactiviteiten van de instelling onder de Wwft vallen, zoals relaties tussen financiële instellingen (zoals correspondentrelaties) en dienstverleners.

Bij het identificeren verstrekt de cliënt gegevens over zijn identiteit. Dit is vormvrij, dit kan bijvoorbeeld door het invullen van een (web) formulier. Bij het verifiëren van de identiteit gaat het om het vaststellen dat de opgegeven identiteit overeenkomt met de werkelijke identiteit. Aan de hand van documenten, gegevens of inlichtingen uit betrouwbare en onafhankelijke bron controleert de instelling de juistheid van de door de cliënt opgegeven identiteit. In artikel 4 van de Uitvoeringsregeling Wwft wordt een aantal documenten genoemd die hiervoor gebruikt kunnen worden. Bij rechtspersonen dienen, naast

21 a. van natuurlijke personen, niet zijnde uiteindelijk belanghebbenden als bedoeld in artikel 1, eerste lid: 1°. de geslachtsnaam, de voornamen, de geboortedatum, het adres en de woonplaats, dan wel de plaats van vestiging van de cliënt alsmede van degene die namens die natuurlijke persoon optreedt, of een afschrift van het document dat een persoonidentificerend nummer bevat en aan de hand waarvan de verificatie van de identiteit heeft plaatsgevonden; 2°. de aard, het nummer en de datum en plaats van uitgifte van het document met behulp waarvan de identiteit is geverifieerd;
b. van natuurlijke personen, zijnde uiteindelijk belanghebbenden als bedoeld in artikel 1, eerste lid:1°. de identiteit, waaronder ten minste de geslachtsnaam en voornamen van de uiteindelijk belanghebbende; en 2°. de gegevens en documenten die zijn vergaard op basis van de redelijke maatregelen die zijn genomen om de identiteit van de uiteindelijk belanghebbende te verifiëren;
c. van vennootschappen of andere juridische entiteiten: 1°. de rechtsvorm, de statutaire naam, de handelsnaam, het adres met huisnummer, de postcode, de plaats van vestiging en het land van statutaire zetel; 2°. indien de vennootschap of andere juridische entiteit bij de Kamer van Koophandel is geregistreerd, het registratienummer bij de Kamer van Koophandel en de wijze waarop de identiteit is geverifieerd; 3°. van degenen die voor de vennootschap of juridische entiteit bij de instelling optreden:
de geslachtsnaam, de voornamen en de geboortedatum.
d. van trusts of andere juridische constructies: 1°. het doel en de aard van de trust of andere juridische constructie; 2°. het recht waardoor de trust of andere juridische constructie wordt beheerst.

de cliënt zelf, ook de vertegenwoordigers te worden geïdentificeerd. Hierover meer onder 4.2.3.

Er kunnen ook andere documenten, inlichtingen of gegevens dan genoemd in artikel 4 van de Uitvoeringsregeling Wwft worden geaccepteerd ten behoeve van de verificatie van de identiteit van een natuurlijk persoon, mits deze afkomstig zijn uit een betrouwbare en onafhankelijke bron. Dit laatste wordt overgelaten aan de risicobeoordeling van de instelling die de betreffende persoon als cliënt wil accepteren, waarbij verwacht mag worden dat de instelling heeft vastgelegd welke documenten, inlichtingen of gegevens acceptabel zijn voor de instelling, en waarom. In de risicobeoordeling door instellingen wordt rekening gehouden met de hoog-risico landenlijst van de Europese Commissie. Raadpleeg de website 'EU Policy on High-Risk Third Countries' voor de actuele landenlijst.

Voor buitenlandse rechtspersonen, die niet gevestigd zijn in Nederland, geschiedt de verificatie ook aan de hand van documenten of gegevens of inlichtingen uit betrouwbare en onafhankelijke bron, die in het internationale verkeer gebruikelijk zijn. Hiertoe kunnen vergelijkbare documenten worden opgevraagd als voor de verificatie van Nederlandse rechtspersonen zoals beschreven in artikel 4, tweede lid van de Uitvoeringsregeling Wwft, waarbij het van belang is dat de bron voldoende betrouwbaar en onafhankelijk is. Dit impliceert dat de instelling begrijpt en boordeelt welke bronnen betrouwbaar en onafhankelijk zijn waarbij het feit dat deze bij wet erkend zijn als identificatiemiddel in de staat van herkomst van de cliënt, wordt meegenomen als een relevante overweging bij het vaststellen van de betrouwbaarheid en onafhankelijkheid. Ook bij de acceptatie van rechtspersonen wordt rekening gehouden met de hoog-risico landenlijst van de Europese Commissie.

Bij documenten die niet afkomstig zijn van overheidsinstanties of rechterlijke instanties, moet de instelling zich afvragen of de documenten voldoende betrouwbaar zijn. Dergelijke documenten zijn op zichzelf onvoldoende om de identiteit op een adequate wijze te verifiëren. Documenten waarvan niet vaststaat dat daaraan adequate identificatie en verificatie vooraf is gegaan, zoals studentenpassen, werknemerspassen en afschriften van bijvoorbeeld nuts- of telecombedrijven, volstaan over het algemeen niet om de identiteit te verifiëren. Ook bij de zogenoemde 1-cent betaling die door sommige instellingen wordt gebruikt ter verificatie van de identiteit staat niet vast dat daaraan een adequate identificatie en verificatie door een andere instelling vooraf is gegaan. Deze kan daarom niet zonder meer dienen als verificatie van de identiteit van een cliënt. Dit houdt in dat er naast deze bron nog gebruik gemaakt wordt van (een) andere onafhankelijke en betrouwbare bron(nen).

Voor alle documentatie geldt in het geval een instelling twijfelt aan de echtheid daarvan dat zij de echtheid controleert en indien nodig aanvullende documentatie opvraagt.

4.2.2 Stromannen en vertegenwoordiging

Tijdens het cliëntenonderzoek kijkt de instelling ook of een cliënt voor zichzelf optreedt of voor een ander. De bedoeling is om te beoordelen of iemand als stroman handelt ten behoeve van

(criminele) derden. Als het duidelijk is dat een cliënt ten behoeve van een andere persoon handelt, dan kwalificeert deze andere persoon als cliënt (de "natuurlijke of rechtspersoon [...] die een transactie laat uitvoeren") en gelden de verplichtingen ten aanzien van het cliëntenonderzoek uit de Wwft ook ten aanzien van deze persoon. In andere gevallen kan een risico gebaseerde benadering worden gekozen: de instelling treft redelijke maatregelen waarmee kan worden vastgesteld of iemand voor zichzelf optreedt of voor een ander (zie artikel 3, tweede lid, onderdeel f, Wwft). Een instelling kan hiertoe bijvoorbeeld indicatoren opstellen die worden toegepast in het cliëntenonderzoek. Te denken valt aan gevallen dat de persoon bepaalde vragen niet kan beantwoorden zoals over de herkomst van het geld of wanneer er onduidelijke, vage redenen voor de transactie worden gegeven. Indien de instelling vermoedt dat de cliënt een stroman is, is dit vanzelfsprekend een verhoogd of onacceptabel risico.

Wanneer een natuurlijke persoon beweert als vertegenwoordiger van een cliënt op te treden, stellen instellingen ook vast of deze persoon vertegenwoordigingsbevoegd is. Bij een rechtspersoon zijn de vertegenwoordigers vaak de bestuurders. Wanneer een natuurlijke persoon stelt dat hij indirect een rechtspersoon vertegenwoordigt (waarbij geldt dat de rechtspersoon de cliënt is), wordt ook de keten van vertegenwoordigingsbevoegdheid vastgesteld. Dit kan bijvoorbeeld door uittreksels uit het handelsregister. Als deze bevoegdheid is vastgesteld, dan is de cliënt het onderwerp van het cliëntenonderzoek zoals voorgeschreven in artikel 3 Wwft. De natuurlijke persoon die optreedt als vertegenwoordiger dient ook te worden geïdentificeerd en zijn identiteit geverifieerd (zie artikel 3, tweede lid, aanhef en onder e, Wwft).

4.2.3 Personenvennootschap

Voor personenvennootschappen wordt een met de rechtspersonen vergelijkbaar cliëntenonderzoek verricht. De personenvennootschap is te omschrijven als een gemeenschap van personen die door een overeenkomst tot stand is gebracht. Een personenvennootschap bezit geen rechtspersoonlijkheid en is daarom niet degene met wie een zakelijke relatie wordt aangegaan of die een transactie laat uitvoeren. Het gaat hier bijvoorbeeld om een maatschap, een vennootschap onder firma, een commanditaire vennootschap, of soortgelijke gemeenschappen van personen zonder rechtspersoonlijkheid en vergelijkbare entiteiten naar buitenlands recht. Bijvoorbeeld bij de vennootschap onder firma zijn de natuurlijke personen of rechtspersonen die samen de vennootschap vormen aan te merken als cliënten.

De instelling identificeert de vennoten en neemt op risico gebaseerde en adequate maatregelen om, voor zover toepasselijk, hun hoedanigheid van vennoot te verifiëren. Een instelling stelt daarbij vast welke natuurlijke personen in belangrijke mate invloed kunnen uitoefenen of belangen hebben, dan wel een grote mate van invloed op meer ingrijpende besluiten van de personenvennootschap hebben en het beleid van de personenvennootschap wezenlijk naar hun hand kunnen zetten. Bij het vaststellen van de zeggenschapsstructuur vallen personen die bevoegd zijn inzake beheer eveneens onder

het cliëntenonderzoek: de instelling identificeert hen. Voor de verificatie van deze personen neemt de instelling op risico gebaseerde en adequate maatregelen om hun hoedanigheid van vennoot te verifiëren. De risico gebaseerde verificatie van de identiteit vindt wel plaats bij de natuurlijke personen die kwalificeren als equivalent van UBO's. Verificatie van de identiteit van alle vennoten zou in sommige gevallen praktisch onmogelijk zijn, bijvoorbeeld bij een zogenoemde open commanditaire vennootschap.

4.2.4 Trust

Een trust is een buitenlandse rechtsvorm die niet naar Nederlands recht kan worden opgericht, maar wel in Nederland wordt erkend. Ook wel bekend onder de noemer 'Angelsaksische Trust'. Vergelijkbare juridische constructies zijn de Franse fiducie en Duitse Treuhand. Een trust (of andere juridische constructie) bezit geen rechtspersoonlijkheid en is om die reden niet degene met wie een zakelijke relatie wordt aangegaan of die een transactie laat uitvoeren. Zodoende kwalificeert de trust niet als cliënt; de trustee wordt gezien als de cliënt. De verplichtingen van de Wwft zien dan ook op dienstverlening ten behoeve van een trust. In voorkomend geval moeten de gebruikelijke stappen van het cliëntenonderzoek worden doorlopen, maar moeten ook de personen zoals genoemd in artikel 3, eerste lid, onder e bekend zijn bij de instelling omdat zij worden gezien als de UBO's van de trust. De cliënt moet opgave doen van hun identiteit en de instelling moet deze opgegeven identiteit verifiëren.

4.2.5 Wanneer identificatie en verificatie

De gevallen waarin cliëntenonderzoek dient plaats te vinden staan vermeld in artikel 3 Wwft. Dit betreft in de eerste plaats de gevallen waarin een instelling een zakelijke relatie aangaat dan wel een transactie of samenstel van transacties verricht boven een bepaald grensbedrag.

Artikel 3, vijfde lid, onderdeel b, Wwft schrijft voor dat een instelling bij twee of meer transacties waartussen een verband bestaat met een gezamenlijke waarde van ten minste 15.000 euro een cliëntenonderzoek verricht. De instelling beoordeelt dit aan de hand van het soort transactie en de bedragen waar het om gaat. Vooropgesteld staat dat het gaat om incidentele transacties, hetgeen betekent dat er geen zakelijke relatie aanwezig hoeft te zijn. Verondersteld wordt dat het gaat om gelijksoortige transacties. Te denken valt aan een persoon die in meerdere transacties in een tijdsbestek van enkele weken of maanden contante gelden stort op een rekening waarvan hij of zij niet de rekeninghouder is (en ook niet handelt voor de rekeninghouder) waarbij die bedragen in totaal uitkomen boven 15.000 euro. Deze bepaling is daarentegen bijvoorbeeld niet van toepassing op een bedrijf dat elke dag de contante opbrengsten afkomstig uit de reguliere bedrijfsvoering afstort op eigen rekening, omdat deze stortingen binnen de zakelijke relatie vallen.

Uit de wetsgeschiedenis kan worden opgemaakt dat bij elke individuele money transfer transactie[22] een zakelijke relatie mag worden verondersteld.

22 Een geldtransfer in de zin van richtlijn (EU) 2015/2366.

Voorts volgt uit het hoge risico bij money transfers op witwassen en terrorismefinanciering, dat instellingen die money transfers verrichten, bij money transfers altijd cliëntenonderzoek verrichten.

Bij alle cliënten, ook bij bestaande cliënten, vindt cliëntenonderzoek plaats indien:

- er indicaties zijn dat de cliënt betrokken is bij witwassen of financieren van terrorisme; dergelijke indicaties kunnen bijvoorbeeld worden verkregen uit openbare bronnen ('bad press') of uit de monitoring van de transacties door de cliënt
- de instelling twijfelt aan de juistheid of volledigheid van eerder verkregen gegevens van de cliënt;
- het risico van betrokkenheid van een bestaande cliënt bij witwassen of financieren van terrorisme daartoe aanleiding geeft;
- er een hoger risico bestaat op witwassen of terrorismefinanciering vanwege het land waar de cliënt woont;
- er sprake is van een incidentele elektronische geldovermaking[23] van ten minste € 1.000.

Identificatie en verificatie zijn afgerond voordat de zakelijke relatie ontstaat en de dienstverlening aanvangt. In afwijking hiervan is het mogelijk om de identiteit van de cliënt en, indien van toepassing, de identiteit van de UBO te verifiëren tijdens het aangaan van de zakelijke relatie, indien dit noodzakelijk is om de dienstverlening niet te verstoren.[24] Bij deze uitzondering wordt wel het doel van de wet in de gaten gehouden, namelijk het voorkomen dat de dienstverlening wordt gebruikt voor witwassen of terrorismefinanciering. Voorwaarden zijn dat er een laag witwas- of terrorismefinancieringsrisico is en dat de verificatie van de identiteit zo spoedig mogelijk plaatsvindt na het eerste contact met de cliënt. Hierbij kan worden gedacht aan situaties waarbij vanwege het soort instelling of dienstverlening er technische of organisatorische redenen zijn dat een beperkte aanvang wordt gemaakt met de dienstverlening. De voorwaarde daarbij is dat deze initiële dienstverlening alleen plaatsvindt in situaties met een laag risico. Dit betekent dus dat een instelling een eerste risico-inschatting moet maken om te bekijken of er inderdaad sprake is een laag witwas- of terrorismefinancieringsrisico.

Tevens geldt dat een rekening geopend kan worden maar dat de verificatie later kan plaatsvinden, zolang de instelling er in die tussentijd voor zorgt dat de rekening niet gebruikt kan worden.[25] Dit geldt ook voor creditcards die door banken en daartoe gerechtigde instellingen uitgegeven worden. Zolang de creditcard geblokkeerd is (te vergelijken met een rekening die nog niet gebruikt kan worden) kan de instelling nog de verificatie uitvoeren, maar als de creditcard gedeblokkeerd is en de kaart gebruikt

23 Als bedoeld in artikel 3, negende lid, van verordening (EU) 2015/847 van het Europees Parlement en de Raad van 20 mei 2015 betreffende bij geldovermakingen te voegen informatie over de betaler en tot intrekking van Verordening (EG) nr. 1781/2006 (PbEU 2015, L 141).
24 Artikel 4, lid 2, Wwft.
25 Artikel 4, lid 3, Wwft.

kan worden (ongeacht of hij daadwerkelijk gebruikt wordt) moet de identificatie en de verificatie afgerond zijn.

In aanvulling op bovengenoemde cliëntenonderzoeksmaatregelen dient een financiële onderneming in het geval van een levensverzekering na het aanwijzen van de begunstigde te voldoen aan de in artikel 3a Wwft opgenomen verplichtingen. Verificatie van de identiteit van de begunstigde vindt uiterlijk plaats op het tijdstip van de uitkering.

Ten aanzien van cliënten die reeds op grond van de Wwft van vóór de wetswijziging van 25 juli 2018 zijn geaccepteerd, geldt op grond van artikel 38 Wwft dat een revisie van, delen van, het cliëntenonderzoek dient plaats te vinden bij eerste gelegenheid na datum van inwerkingtreding van de wetswijziging. In veel gevallen is het moment dat er sprake is van klantcontact die eerste gelegenheid. De eerste gelegenheid is echter ook het moment waarop de instelling op grond van de risicogevoeligheid van de klant aanleiding heeft om cliëntenonderzoek te doen. Dit is bijvoorbeeld bij cliënten die een hoger risico met zich meebrengen. In die gevallen zal het cliëntendossier op initiatief van de instelling moeten worden gereviseerd. De revisie van bestaande cliëntendossiers wordt op een risico-gebaseerde manier ingevuld en valt samen met de herzieningstermijnen die een instelling hanteert voor haar cliëntendossiers (zie hoofdstuk 3 onderdeel 4).[26]

4.3 Aangaan zakelijke relatie

In beginsel mag een instelling de zakelijke relatie pas aangaan wanneer zij het volledige cliëntenonderzoek heeft uitgevoerd, het onderzoek heeft geleid tot het beoogde resultaat en de instelling ook over alle identificatie- en verificatiegegevens en overige gegevens beschikt. Een instelling hoeft niet zelf het cliëntenonderzoek te verrichten, maar kan dat ook door een andere (Wwft-plichtige)instelling laten doen (de introducerende partij).[27] Een instelling maakt in dat geval gebruik van introducerend cliëntenonderzoek zoals beschreven in artikel 5 Wwft.

Indien een instelling een derde partij inschakelt, dit kan een niet Wwft-plichtige partij zijn, om het cliëntenonderzoek te verrichten (of onderdelen daarvan) is er sprake van uitbesteding zoals beschreven in artikel 10 Wwft.[28]

4.3.1 Introducerend cliëntenonderzoek

De verantwoordelijkheid voor het cliëntenonderzoek en naleving van de Wwft verplichtingen ligt te allen tijde bij de accepterende instelling en niet bij de introducerende partij. De eigen verantwoordelijkheid geldt niet alleen ten aanzien van de verplichtingen aangaande het cliëntenonderzoek maar ook ten aanzien van de naleving van de bepalingen met betrekking tot de vastlegging van dit onderzoek. Opgemerkt wordt dat een accepterende instelling direct bij

26 Dit betekent dat cliëntendossiers met een hoog risico op het moment van publicatie van de Leidraad grotendeels gereviseerd zullen zijn.
27 Artikel 5, lid 1, onder a, geeft aan welke instellingen cliënten kunnen introduceren.
28 Hierbij wordt aangetekend dat het cliëntenonderzoek in het kader van de voortdurende controle op de zakelijke relatie en de tijdens de duur van deze relatie verrichte transacties niet kan worden uitbesteed.

introductie moet beschikken over de gegevens die zijn gebruikt bij het cliëntenonderzoek door de introducerende instelling.[29] Daarnaast moet de instelling kunnen beschikken over de onderliggende documentatie die heeft geleid tot de acceptatie van de cliënt. De accepterende instelling is bovendien zelf verantwoordelijk voor het opstellen van het risicoprofiel en heeft daarvoor dan ook de juiste gegevens nodig. Indien de introducerende instelling de gegevens niet kan verstrekken, verricht de accepterende instelling alsnog het cliëntenonderzoek dat op grond van de Wwft of de interne regels noodzakelijk is.

Als door de introducerende instelling op een cliënt het vereenvoudigde cliëntenonderzoek is toegepast omdat deze cliënt een laagrisico product afnam, kan de accepterende instelling de introducerende instelling vragen om nadere identificatie- en verificatiegegevens overeenkomstig met het risico dat de cliënt op dat moment met zich meebrengt. Een instelling mag op grond van de interne procedures altijd meer doen dan de Wwft vereist en kan dus ook besluiten zelf alsnog een cliëntenonderzoek te verrichten. Ten overvloede: het vereenvoudigd cliëntenonderzoek is niet mogelijk in geval van vermoeden van witwassen en terrorismefinanciering. Als de instelling waar een cliënt geïntroduceerd wordt een dergelijk vermoeden heeft, dan heeft de instelling een extra reden de gegevens op te vragen.

Een instelling die zich baseert op de identificatie en verificatie van de identiteit door een andere instelling of partij die onder de Wwft valt, gaat hier zorgvuldig mee om. Aangezien de verantwoordelijkheid voor een correct cliëntendossier bij de accepterende instelling zelf ligt, is het belangrijk dat deze instelling zich er van vergewist dat de betreffende elementen van het cliëntenonderzoek hebben plaatsgevonden conform de Wwft (of vergelijkbare wetgeving in internationale situaties) en dat de andere instelling adequate procedures en maatregelen met betrekking tot de Wwft heeft. Dat houdt in dat de procedures van de introducerende partij in opzet en werking adequaat zijn. Een accepterende instelling kan een adequate werking van deze procedures en maatregelen niet veronderstellen. Als een instelling cliënten accepteert van dezelfde andere instelling, ligt het voor de hand dat zij, op risico gebaseerde wijze, de Wwft-procedures van deze instelling opvraagt en beoordeelt. Bij samenwerkingsverbanden worden altijd de Wwft procedures opgevraagd ter beoordeling.

Dit laatste is met name relevant voor levensverzekeraars die vertrouwen op het cliëntenonderzoek door financiële dienstverleners die bemiddelen in levensverzekeringen. De verzekeraar is verantwoordelijk voor een adequate uitvoering van de Wwft en het Wwft beleid. Concreet betekent dit dat een verzekeraar ten aanzien van identificatie en verificatie van cliënten beleid formuleert. Hierin legt zij vast op welke manier wordt omgegaan met het vertrouwen op de

29 Artikel 33, lid 1, Wwft

door de relevante financiële dienstverleners uitgevoerde identificatie en verificatie van de identiteit van de cliënt. Daarnaast wordt beleid geformuleerd op grond waarvan de betreffende financiële dienstverleners de gegevens omtrent de identificatie van cliënten desgevraagd onmiddellijk beschikbaar stelt. Financiële dienstverleners die bemiddelen in levensverzekeringen hebben een zelfstandige verplichting met betrekking tot de Wwft. In het geval waarin deze financiële dienstverlener de identiteit van de cliënt heeft vastgesteld en geverifieerd, behoudt de verzekeraar ter zake zijn eigen verantwoordelijkheid. Deze mag de verzekeringsovereenkomst bijvoorbeeld pas sluiten nadat hij zich ervan heeft vergewist dat de tussenpersoon de identiteit van de cliënt heeft vastgesteld en deze identiteit heeft geverifieerd. Verzekeraars zullen periodiek, op risico gebaseerde wijze, nagaan of de betreffende financiële dienstverleners maatregelen hebben om op een adequate uitvoering te geven aan het cliëntenonderzoek. Hier kan op verschillende manieren uitvoering aan gegeven worden. Zo kan de instelling bijvoorbeeld jaarlijks van een aantal financiële dienstverleners die bemiddelen in levensverzekeringen de Wwft procedures opvragen ter beoordeling. Andere mogelijkheden zijn het opvragen van een accountantsverklaring (voor met name grote financiële dienstverleners) of het steekproefsgewijs opvragen van een aantal cliëntendossiers.

4.3.2 Periodieke actualisatie en review

De instelling stelt aan de hand van het cliënten-onderzoek een risicoprofiel op van de cliënt dat past in één van de door de instellingen ingestelde risicocategorieën (zie onderdeel 3.4). Dit risicoprofiel is dynamisch, dat wil zeggen dat het in de loop der tijd kan wijzigen. Daarom verricht een instelling een review van het cliëntenonderzoek om vast te stellen of de cliënt nog steeds aan het vastgestelde risicoprofiel voldoet. De cliëntgegevens worden daartoe periodiek door de instelling geactualiseerd, inclusief het risicoprofiel van de cliënt, contact-informatie en (de) UBO('s). Uitgangspunt is dat de frequentie en diepgang van de review afhankelijk is van het risico dat de cliënt met zich meebrengt. Zie hiervoor ook onderdeel 3.3 en 3.4.

Instellingen besteden in het beleid en de procedures aandacht aan de frequentie en de wijze waarop cliëntgegevens periodiek worden geactualiseerd. Daarbij zijn van invloed het risicoprofiel en de daarmee samenhangende risicocategorisatie van de cliënt. In het licht van de voortgaande automatisering van CDD gerelateerde processen wordt de kwaliteit en kwantiteit van de data(velden) een steeds belangrijker factor. Instellingen houden hier in het formuleren van hun beleid nadrukkelijk rekening mee. Het gaat dan niet alleen om nieuwe klanten maar juist ook om de bestaande klantportefeuille.

Wanneer vindt een review van het cliëntenonderzoek plaats?

Bij **laagrisico cliënten** kan, naast het moment van de eerder vastgestelde reviewtermijn (zoals beschreven in 3.4), een review plaatsvinden op het moment dat:

- de cliënt een nieuwe dienst of product vraagt, of bij klantcontact waarbij de gelegenheid bestaat het cliëntenonderzoek uit te voeren;
- de cliëntkenmerken wijzigen (bijvoorbeeld verhuizing naar een hoog-risico jurisdictie),
- op basis van signalen van incidenten of transacties.

Bij **hoog-risico cliënten** zal in de praktijk regelmatiger (een keer tot enkele malen per jaar) een review worden uitgevoerd en bijvoorbeeld bij:

- eventuele signalen die duiden op een hoger risico, bijvoorbeeld vanwege het rekeninggebruik of specifieke transacties, een en ander bezien vanuit de geconsolideerde positie van de betreffende cliënt.

In alle gevallen zijn de betrokken medewerkers op de hoogte van mogelijke risico's rondom dit soort hoog-risico cliënten.

4.4 Niet aangaan van- of beëindiging van de zakelijke relatie

Het zal voorkomen dat een instelling op basis van het cliëntenonderzoek concludeert dat een bestaande of voorgenomen cliënt een te hoog risico op betrokkenheid bij witwassen of terrorismefinanciering met zich brengt. Daarnaast kan het voorkomen dat het cliëntenonderzoek niet volledig uitgevoerd kan worden, bijvoorbeeld door het ontbreken van noodzakelijke cliëntinformatie, en de instelling dus niet kan vaststellen wie haar cliënt precies is en/of welk doel de voorgenomen zakelijke relatie heeft.

In beide gevallen gaat de instelling geen zakelijke relatie aan met de cliënt[30], verbreekt zij de zakelijke relatie en voert zij geen transacties uit.[31]

Op grond van artikel 5 Wwft is het verboden een zakelijke relatie aan te gaan of een transactie uit te voeren indien er geen cliëntenonderzoek is verricht of indien het cliëntenonderzoek, inclusief het onderzoek naar de UBO, niet heeft geleid tot het vereiste resultaat. Er is voorts een wettelijke verplichting om de zakelijke relatie te beëindigen wanneer niet voldaan kan worden aan de eisen met betrekking tot het cliëntenonderzoek.

30 Artikel 4, lid 1, Wwft en artikel 5, lid 1, aanhef en onderdeel b, Wwft
31 Art 5, lid 3, Wwft

Indien de instelling bovendien aanwijzingen heeft dat de cliënt betrokken is bij witwassen of het financieren van terrorisme dan, is zij op grond van artikel 16, vierde lid, Wwft verplicht daarvan melding te doen bij de Financiële Inlichtingen Eenheid (FIU-NL).

Om te waarborgen dat aan al deze verplichtingen wordt voldaan en op een adequate manier afscheid kan worden genomen van bestaande cliënten, stelt de instelling een cliënt-exitbeleid op. Hierin geeft zij aan onder welke omstandigheden en volgens welke procedure de relatie met de cliënt wordt beëindigd.

Indien de instelling de zakelijke relatie niet (onmiddellijk) kan beëindigen, neemt de instelling (verdere) adequate maatregelen om alsnog het cliëntenonderzoek te verrichten en stelt een plan op waarbij de relatie zo spoedig mogelijk wordt beëindigd. Instellingen kunnen denken aan het 'ring-fencen' van de dienstverlening en het toepassen van verscherpte monitoring totdat beëindiging wel mogelijk is. Voorop staat dat de instelling zich maximaal inspant om de relatie te beëindigen en deze inspanning zorgvuldig vastlegt.

4.4.1 Verbod aangaan zakelijke relatie in specifieke gevallen

Het is niet toegestaan om correspondentrelaties aan te gaan of voort te zetten met een shellbank of met een bank of andere financiële instelling waarvan bekend is dat deze een shellbank toestaat van haar rekeningen gebruik te maken. [32] Shellbanken brengen vanwege de aard van hun organisatie risico's met zich mee: zij bieden dienstverlening aan in een land zonder dat zij daar over een fysieke vestiging beschikken, dat wil zeggen er is geen bestuur en management in dat land aanwezig. Gedragingen van dergelijke instellingen zijn voor toezichthouders moeilijk te controleren.

Bij levensverzekeringen, waar het veelal juridisch niet mogelijk is om een bestaande relatie te beëindigen, worden de tegoeden bevroren totdat het cliëntenonderzoek wel heeft geleid tot het bedoelde resultaat.

4.4.2 Afgeschermde rekeningen

De internationale standaarden op het gebied van CDD en de bestrijding van witwassen en terrorismefinanciering stellen dat instellingen geen relaties mogen onderhouden met personen die anoniem blijven of personen die een fictieve naam opgeven. Omdat het in een aantal beperkte gevallen – het beschermen van de privacy en veiligheid van betrokken cliënten en het voorkomen van vormen van gebruik van voorwetenschap – nuttig kan zijn de identiteit van een cliënt intern af te schermen, voorziet de Regeling afgeschermde rekeningen Wft[33] in een procedure volgens welke de identiteit van de cliënt bij transactieverwerkingen niet zichtbaar of anderszins afgeschermd is. De cliënt is dan wel bekend bij de instelling, alleen is het niet voor alle medewerkers duidelijk om wie het gaat. Daarnaast staat de Regeling toe dat aan personen als bedoeld in artikel 44, eerste lid, van de Politiewet en artikel 15,

32 Artikel 5, lid 5, Wwft. 'Shellbank' is gedefinieerd in artikel 1a lid 1 Wwft.
33 Zie ook: https://wetten.overheid.nl/BWBR0020672/2018-10-13

tweede lid van de Wet op de Inlichtingen- en Veiligheidsdiensten bancaire diensten worden verleend.

De Regeling staat een bank of een bijkantoor van een bank toe restrictief gebruik te maken van afgeschermde rekeningen. In deze regeling is beschreven op welke wijze banken en bijkantoren van banken een centraal register bijhouden waarbij de gegevens omtrent de identiteit van een cliënt bij transactieverwerkingen niet zichtbaar of anderszins afgeschermd zijn, terwijl deze wel elders bij de instelling bekend zijn. In het centrale register worden de gegevens opgenomen die op grond van artikel 33 Wwft worden vastgelegd. Het centrale register is zodanig ingericht dat op naam en nummer- of codesleutel kan worden geraadpleegd. Daarnaast wordt een beheerder van het centrale register aangewezen en heeft de compliance functie toegang tot het register.

De Regeling ziet dus alleen op het afschermen van de identiteit bij de transactieverwerking. De eisen van de Wwft omtrent het cliëntenonderzoek zijn onverminderd van toepassing, alsmede de Verordening van het Europees Parlement en de Raad van 20 mei 2015 betreffende bij geldovermakingen te voegen informatie.[34]

In dit kader is het ook relevant te verwijzen naar rekeningen met een andere tenaamstelling dan de naam van de cliënt of rekeninghouder, zoals bijvoorbeeld zogenaamde 'inzake-rekeningen'. Hoewel hier in sommige gevallen een legitieme verklaring voor kan zijn, zoals bij verzekeraars met verschillende labels of merken, zou een instelling hier extra alert op moeten zijn wanneer een cliënt een 'inzake-rekening' vraagt voor een tenaamstelling die niet verklaarbaar is. Bij de periodieke review kan het dan voorkomen dat een dergelijke rekening vanwege de andere tenaamstelling niet opvalt. Ook voor andere instellingen kan een dergelijke andere tenaamstelling misleidend zijn bij bijvoorbeeld de naam-nummer controle of bij het beoordelen van alerts uit de transactiemonitoring.

4.5 Uiteindelijke belanghebbende (UBO)

Het cliëntenonderzoek omvat onder meer dat de instelling de identiteit van de Uiteindelijke belanghebbende (UBO) vast stelt (identificeren en verifiëren). De instelling identificeert daartoe bij elke cliënt de UBO. De UBO is altijd een natuurlijke persoon. Deze norm is niet alleen relevant wanneer de cliënt een juridische entiteit is, zoals een rechtspersoon of stichting, of een juridische constructie zoals een trust maar is ook relevant als de cliënt een natuurlijke persoon is over wie een andere natuurlijke persoon feitelijke zeggenschap heeft of voor wiens rekening een transactie of activiteit wordt verricht.[35] Het cliëntenonderzoek naar de UBO is een wettelijke eis.[36] De achtergrond

34 Zie hoofdstuk 6 van de Leidraad over een toelichting op deze verordening.
35 Zie de definitie van uiteindelijk belanghebbende in artikel 1, lid 1 Wwft. Voorts is van belang het bepaalde in artikel 3 van het Uitvoeringsbesluit Wwft 2018, waaruit blijkt welke categorieën van natuurlijke personen in elk geval moeten worden aangemerkt als uiteindelijk belanghebbenden.
36 Artikel 3, lid 2, onderdeel b, Wwft.

hiervan is dat criminelen gebruik kunnen maken van constructies waarin (buitenlandse) rechtspersonen een rol spelen als een middel om de criminele herkomst van gelden te verbergen.

Aan de plicht tot het identificeren van de UBO's kan meestal voldaan worden door de cliënt opgave te laten doen van wie de UBO is. Vervolgens neemt de instelling "redelijke maatregelen" om de opgegeven identiteit te verifiëren, immers is met de door de cliënt verstrekte gegevens niet geverifieerd of deze informatie klopt. De verificatie geschiedt op risicogebaseerde wijze op basis van onafhankelijke en betrouwbare bronnen, bijvoorbeeld openbare bronnen, een uittreksel uit het handelsregister of een bevestiging van de eigen verklaring door een onafhankelijke derde. Een instelling dient altijd de identiteit van de UBO te verifiëren, onafhankelijk van het risico. De identiteit wordt dus altijd geverifieerd, maar de wijze en mate van diepgang waarop dat gebeurt is risicogebaseerd: dat betekent dat bij hoog-risico cliënten verdergaande maatregelen worden getroffen dan bij laag-risico cliënten. De verificatiemaatregelen stellen de instelling in staat om voldoende informatie te verkrijgen om overtuigd te zijn van wie de UBO is. Daarnaast controleert de instelling ook altijd of de UBO een PEP (politiek prominente persoon of politically-exposed person) is.

In specifieke gevallen kan vereenvoudigd cliënten-onderzoek worden toegepast bij het onderzoek naar de UBO('s). In bijlage II van de vierde anti-witwasrichtlijn wordt een niet-limitatieve lijst van cliëntgebonden risicofactoren die potentieel een lager risico met zich meebrengen genoemd. Deze factoren zijn van belang voor het gehele cliëntenonderzoek (zie hieronder par. 4.8). Vereenvoudigd cliëntenonderzoek betekent niet dat er geen onderzoek wordt verricht.

De instelling neemt ook op risicogebaseerde en adequate maatregelen om in het geval van rechtspersonen, stichtingen of trusts en andere juridische constructies inzicht te verkrijgen in de eigendoms- en zeggenschapsstructuur van de cliënt. Daaronder zijn ook maatregelen om de juridische status van cliënten anders dan natuurlijke personen te verifiëren, waar mogelijk middels het verkrijgen van bewijs van rechtspersoonlijkheid.[37] Uitgangspunt is dat de instelling deze structuur kent en ook begrijpt. Dit betekent dat bij ingewikkelde structuren van ondernemingen meer inspanningen worden verricht om de (internationale) aandelen- en beheersstructuur van de onderneming te begrijpen dan voor een Nederlandse BV met een directeur-grootaandeelhouder. De instelling onderzoekt hierbij ook waarom de cliënt gebruik maakt van complexe structuren. Dat kan door er naar te vragen bij de klant, maar bijvoorbeeld ook door het opvragen van een juridische of fiscale opinie of advies. Inzicht verkrijgen in de fiscale motieven in het kader van het cliëntenonderzoek stelt de instelling in staat om vast te stellen of er sprake is van fiscale integriteitrisico's. Hierbij hangt het onderzoek naar de eigendoms- en

37 Deze verificatie kan plaatsvinden zoals beschreven in Annex 4 van de Guidelines – Sound Management of Risk Related to Money Laundering and Financing of Terrorism, Basel Committee on Banking Supervision. Te raadplegen op: https://www.bis.org/bcbs/publ/d353.htm.

zeggenschapsstructuur nauw samen met het onderzoek naar het doel en de aard van de relatie.[38]

In artikel 3 van het Uitvoeringsbesluit Wwft 2018 staan voor een aantal rechtsvormen de natuurlijke personen die in elk geval moeten worden aangemerkt als UBO. Dit betreft een niet-limitatieve opsomming.

Uit Artikel 3, eerste lid, onder a sub 2, Uitvoeringsbesluit Wwft 2018 volgt dat instellingen kunnen volstaan met het aanmerken van het hoger leidinggevend personeel, bijvoorbeeld de statutair bestuurder(s), als UBO van de cliënt.[40] Deze terugvaloptie, ook bekend als de 'pseudo-UBO', kan enkel worden ingezet indien (a) alle mogelijke

Uitwerking UBO definitie in Uitvoeringsbesluit Wwft 2018

- Bij B.V.'s en N.V.'s (uitgezonderd 'beursvennootschappen') is een UBO de natuurlijke persoon die, direct of indirect, voor meer dan 25% economisch gerechtigd is tot de vennootschap, dan wel degene die de zeggenschap uitoefent.
- Bij personenvennootschappen zijn de UBO's de natuurlijke persoon die direct of indirect een eigendomsbelang heeft van meer dan 25%, dan wel meer dan 25% van de stemmen kan uitoefenen ingeval van beheersdaden en/of wijziging van de samenwerkingsovereenkomst.
- Bij stichtingen en verenigingen zijn de UBO's de natuurlijke persoon die direct of indirect een eigendomsbelang heeft van meer dan 25%, dan wel meer dan 25% van de stemmen kan uitoefenen ingeval van een statutenwijziging, dan wel de feitelijke zeggenschap heeft over de rechtspersoon.

De Memorie van Toelichting bij de implementatiewet van de AMLD4 geeft aan dat 25% regel indicatief is bedoeld.[39] Ook personen met een lager percentage kunnen als UBO worden aangemerkt, indien deze personen op andere wijze de uiteindelijke zeggenschap hebben. Hierbij wordt als voorbeeld een contractuele betrekking gegeven waaruit blijkt dat deze personen de uiteindelijke zeggenschap hebben.

- Bij een trust worden meerdere personen als UBO's aangemerkt waaronder; de oprichter(s), de trustee(s), de protector(s), de begunstigde(n), de groep personen in wier belang de trust hoofdzakelijk is opgericht.
- Bij kerkgenootschappen zijn de UBO's de natuurlijke personen die bij ontbinding van het kerkgenootschap als rechtsopvolger in het statuut van het kerkgenootschap zijn benoemd.

Zie voor een totaaloverzicht artikel 3 van het Uitvoeringsbesluit Wwft 2018

38 Voor meer informatie zie de DNB Good practices fiscale integriteitrisico's bij cliënten van banken.

39 Zie ook de mvt (Kamerstukken II 2017/18, 34808, nr. 3, p. 4): '(a) geen persoon of personen achterhaald kunnen worden die (direct of indirect) via aandelen, stemrecht of eigendom kwalificeren als UBO en ook geen persoon of personen zijn achterhaald die zeggenschap met andere middelen hebben, of (b) om de gevallen waarin twijfel bestaat of de achterhaalde personen daadwerkelijk UBO zijn. Het moet dan wel duidelijk zijn dat alle mogelijke middelen zijn aangewend om de UBO(s) te achterhalen en er mogen geen gronden zijn voor verdenking van witwassen of financieren van terrorisme.'

40

maatregelen van instelling zijn uitgeput, (b) er geen gronden voor verdenking bestaan en (c) het onderzoek niet geresulteerd heeft in het vaststellen van de daadwerkelijke UBO('s) of een instelling eraan twijfelt of de aangemerkte natuurlijke persoon een daadwerkelijke UBO is. Dit is een uiterste terugvaloptie die alleen in deze gevallen kan worden toegepast.[41]. Artikel 3, zesde lid, van het Uitvoeringsbesluit Wwft 2018 geeft aan wat in dit kader verstaan wordt onder hoger leidinggevend personeel.

Een essentieel onderdeel van het cliëntenonderzoek naar de UBO is de vastlegging hiervan. Het spreekt voor zich dat een instelling vastlegt welke maatregelen getroffen zijn om te achterhalen welke natuurlijk persoon de UBO is en, indien van toepassing, wat de ratio is voor het aanmerken van het hoger leidinggevend personeel als UBO. Bij dat laatste (pseudo-UBO) zal een instelling dus in het betreffende cliëntdossier goed moeten documenteren hoe zij aan de twee voorwaarden (a en b, hiervoor) heeft voldaan. Indien een instelling afwijkt van de door haar opgestelde procedures is het van belang dat onderbouwd en vastgelegd wordt waarom zij in bijzondere gevallen daarvan afwijkt.

4.6 Doel en aard zakelijke relatie

Het inwinnen van informatie over het doel en de beoogde aard van de zakelijke relatie stelt een instelling in staat om eventuele risico's die de dienstverlening aan de cliënt oplevert, in te schatten. Een deel van de benodigde informatie zal doorgaans reeds naar voren komen tijdens het contact voorafgaand aan de zakelijke relatie. De afgenomen diensten of producten kunnen een indicatie zijn van wat het doel van de relatie is. Aanvullende vragen van de instelling kunnen zich richten op het verkrijgen van helderheid over de gebruiker van het product of de afnemer van de dienst. Zo zal een instelling bij een cliënt die niet in Nederland woonachtig of gevestigd is, duidelijk moeten hebben waarom deze in Nederland diensten of producten afneemt bij de instelling. Als dat voor fiscale redenen is, beoordeelt de instelling de aanvaardbaarheid daarvan om te voorkomen dat belastingontduiking gefaciliteerd wordt dan wel dat fiscale structuren worden gefaciliteerd die buiten de risk appetite vallen van een instelling (agressieve belastingplanning). In een dergelijk geval zal een instelling op basis van haar risicoanalyse deze inschatting kunnen maken.[42] Bij doel en aard van de relatie brengt de instelling in hoger risico situaties ook in kaart wat voor soort transacties (zoals hoeveelheid, frequentie en grootte) de cliënt zal verrichten.

4.7 Bron van de middelen

Bij cliëntenonderzoek is het uitgangspunt dat de instelling zo nodig onderzoek verricht naar de bron van de middelen die bij de zakelijke relatie of de transactie gebruikt worden. De instelling

41 Artikel 3, lid 1, onder a sub 2, Uitvoeringsbesluit Wwft 2018.
42 Voor meer informatie zie de DNB Good practices fiscale integriteitrisico's bij banken en trustkantoren.

legt verklaringen en objectieve en onafhankelijke documenten over de bron van de middelen als bewijsstukken in het cliëntendossier vast. De instelling stelt waar nodig nadere vragen. Dat gelden afkomstig zijn van een gereguleerde instelling betekent niet dat de instelling geen zelfstandig onderzoek hoeft uit te voeren. De instelling identificeert indicatoren op basis waarvan de diepgang van het onderzoek wordt bepaald om de plausibiliteit van de legale bron van de middelen vast te stellen. Enkele combinaties van indicatoren zijn het betreffende bedrag, de opgegeven reden van de herkomst van de middelen, leeftijd en beroep of bedrijfsactiviteiten van de klant, land van herkomst of bestemming van de middelen en geleverde product of dienst. Bij levensverzekeringen gaat het dan bijvoorbeeld om de hoogte van de eerste inleg of eventuele bijstortingen. Zeker bij hoog-risico ligt het in de rede door middel van onafhankelijke, betrouwbare bronnen de plausibiliteit van de bron van de middelen vast te stellen en vast te leggen in het cliëntendossier. Dit geldt ook voor *private banking* klanten.

Om de bron van de middelen die bij de zakelijke relatie gebruikt wordt te kennen, kan het met name bij hoogrisico cliënten ook nodig zijn om inzicht te hebben in de vermogenspositie van de cliënt. Bij cliënten die hun vermogen spreiden, is het voor de instelling ook nodig om kennis te hebben van het verdere vermogen teneinde een correct risicoprofiel te kunnen opstellen. De instelling draagt zorg voor vastlegging van het uitgevoerde onderzoek naar de bron van de middelen.

4.8 Vereenvoudigd cliëntenonderzoek, laag-risico factoren en uitzonderingen op het cliëntenonderzoek

Voor bepaalde cliënten en transacties kan op basis van artikel 6 Wwft worden volstaan met een vereenvoudigd cliëntenonderzoek. De conclusie dat vereenvoudigd cliëntenonderzoek gepast is zal altijd op basis van een risicobeoordeling zijn. Er vindt in alle gevallen een risicobeoordeling plaats, vervolgens wordt de intensiteit van het cliëntenonderzoek afgestemd op het ingeschatte risico. De instelling kan op voorhand een inschatting maken in welke gevallen vereenvoudigd cliëntenonderzoek wordt toegepast. Dit wordt gedaan middels een vooraf uitgevoerde risicoanalyse, met inachtneming van de risicofactoren, op basis waarvan de laagrisico cliënten worden geïdentificeerd.
De instelling neemt in de risicobeoordeling in ieder geval de niet-limitatieve lijst van risicofactoren mee die genoemd is in bijlage II van de vierde anti-witwasrichtlijn. Deze factoren geven een indicatie wanner er sprake is van een 'potentieel lager risico'. Beursgenoteerde vennootschappen en overheidsinstellingen zijn als laagrisico voorbeelden genoemd. Dit geldt evenzeer voor beursgenoteerde vennootschappen en overheidsinstellingen uit andere EU-lidstaten en derde landen die doeltreffende wetgeving en toezicht hebben op de bestrijding van witwassen en terrorisme financiering.

Naast cliëntgebonden risicofactoren zijn er risicofactoren die een indicatie geven van een potentieel lager risico bij producten, diensten, transacties en leveringskanalen. Ook hier biedt bijlage II van de vierde anti-witwasrichtlijn een

aanknopingspunt. Bijvoorbeeld producten waarbij de voordelen niet ten behoeve van derden en alleen op lange termijn kunnen worden gerealiseerd, of producten waarbij het risico op witwassen en terrorismefinanciering laag is vanwege bestedingslimieten of transparantie van eigendom. De in bijlage II genoemde lijst is niet-limitatief, dit betekent dat er nog andere risicofactoren kunnen zijn die een indicatie geven van een potentieel lager risico. Nadere risicofactoren staan genoemd in de 'Richtsnoeren betreffende risicofactoren' van de gezamenlijke Europese toezichthouders op de financiële markten (EBA, ESMA en EIOPA). Zie ook hoofdstuk 3.3 waarin meer verwijzingen naar risicofactoren staan opgenomen. De 'Richtsnoeren betreffende risicofactoren' bieden voorbeelden van maatregelen die genomen kunnen worden bij het vereenvoudigd cliëntenonderzoek.[43]

Lijst van factoren van potentieel lager risico uit bijlage II van de vierde anti-witwasrichtlijn.

Cliëntgebonden risicofactoren

- beursgenoteerde vennootschappen die onderworpen zijn aan informatievereisten (op grond van het beursreglement of krachtens wettelijke of afdwingbare middelen) welke voorschriften omvatten om toereikende transparantie betreffende de uiteindelijk begunstigden te garanderen;*
- overheden of overheidsbedrijven;
- cliënten die inwoner zijn van geografische gebieden met een lager risico (zie punt 3 in bijlage II).

* zie voor meer informatie over beursgenoteerde vennootschappen en laag-risico onderdeel 4.5, vierde alinea.[44]

Product-, dienst-, transactie- of leveringskanaalgebonden risicofactoren:

- levensverzekeringspolissen met een lage premie;
- pensioenverzekeringsovereenkomsten die geen afkoopclausule bevatten en niet als zekerheidstelling kunnen dienen;
- een pensioenstelsel, een pensioenfonds of een soortgelijk stelsel dat pensioenen uitkeert aan werknemers, waarbij de bijdragen worden ingehouden op het loon en de regels van het stelsel de deelnemers niet toestaan hun rechten uit hoofde van het stelsel over te dragen;

43 Zie de Richtsnoeren betreffende risicofactoren onder punt 44 e.v.

44 Eén van de cliëntgebonden risicofactoren die genoemd zijn, ziet op beursgenoteerde vennootschappen die onderworpen zijn aan informatievereisten (openbaarmakingsvereisten). Het is van belang dat instellingen er niet zondermeer van uitgaan dat een beursgenoteerde cliënt altijd een lager risico met zich meebrengt. Zo is relevant aan welke beurs de onderneming genoteerd is en is van belang wat het percentage is van het aandelenkapitaal dat genoteerd is; ook onder de houders van beursgenoteerde aandelen kunnen zich UBO's bevinden. Voorts is het enkele feit dat een onderneming een notering heeft aan een "recognized stock exchange" niet voldoende om te besluiten tot vereenvoudigd cliëntenonderzoek. Er zal dus een risicoanalyse gemaakt worden om in te schatten met welke mate van diepgang het cliëntenonderzoek kan worden uitgevoerd.

- financiële producten of diensten die op passende wijze bepaalde en beperkte diensten voor bepaalde soorten cliënten omvatten, om voor financiële inclusiedoeleinden de toegang te vergroten;
- producten waarbij het witwasrisico en het risico van terrorismefinanciering wordt beheerd door andere factoren zoals bestedingslimieten of transparantie van eigendom (bv. bepaalde soorten elektronisch geld).

Geografische risicofactoren:

- lidstaten;
- derde landen met doeltreffende AML/CFT-systemen ter bestrijding van witwassen en terrorismefinanciering;
- derde landen die volgens geloofwaardige bronnen een laag niveau van corruptie of andere criminele activiteit hebben;
- derde landen die volgens geloofwaardige bronnen zoals wederzijdse beoordelingen, gedetailleerde evaluatierapporten, of gepubliceerde follow-uprapporten, voorschriften inzake de bestrijding van witwassen en terrorismefinanciering hebben die beantwoorden aan de herziene FATF-aanbevelingen en die voorschriften effectief ten uitvoer leggen.

Eén van de cliëntgebonden risicofactoren die genoemd zijn, ziet op beursgenoteerde vennootschappen die onderworpen zijn aan informatievereisten (openbaarmakingsvereisten). Het enkele feit dat een onderneming een notering heeft aan een "recognized stock exchange" is niet voldoende om te besluiten tot het toepassen van vereenvoudigd cliëntenonderzoek. Instellingen kunnen er niet zonder meer van uitgaan dat een beursgenoteerde cliënt altijd een lager risico met zich meebrengt. Er kunnen immers ook niet-cliëntgebonden risicofactoren spelen, verband houdend met bijvoorbeeld het type product, dienst of transactie en geografische risicofactoren. Zo is relevant aan welke beurs de onderneming genoteerd is en is van belang wat het percentage is van het aandelenkapitaal dat vrij verhandelbaar is. Het niet vrij verhandelbare deel van het aandelenkapitaal is niet uitgesloten van het UBO onderzoek (zie onderdeel 4.5). Er zal dus vooraf een risicoanalyse gemaakt worden om in te schatten met welke mate van diepgang het cliëntenonderzoek kan worden uitgevoerd bij dit type cliënt.

Tot 25 juli 2018 werden in artikel 6 Wwft gevallen genoemd waarin het cliëntenonderzoek geheel achterwege gelaten kon worden. Deze bepaling is komen te vervallen met de wetswijziging van 25 juli 2018. Instellingen identificeren per geval aan de hand van hun risicobeoordeling of er sprake is van laagrisico. Bij hun risicobeoordeling houden instellingen in ieder geval rekening met de risicofactoren genoemd in bijlage II van de vierde anti-witwasrichtlijn.

Instellingen verzamelen voldoende gegevens om te beoordelen of bij de cliënt kan volstaan met een vereenvoudigd cliëntenonderzoek. Hiertoe kan de instelling vragen naar een uittreksel van de Kamer van Koophandel, inschrijvingen in openbare registers, of andere openbare noteringen. De instelling houdt de informatie actueel die de basis vormt van het verrichte vereenvoudigd cliëntenonderzoek, op grond van artikel 6, derde lid, Wwft. Het actueel houden van de gegevens houdt ook in dat regelmatig moet worden bezien of inderdaad nog sprake is van het eerder vastgestelde lage risico. Een instelling zal in het geval van cliënten waarbij vereenvoudigd cliëntenonderzoek is toegepast over voldoende gegevens beschikken zodat zij in staat is om aan haar artikel 16 Wwft meldverplichting te voldoen.

Ook beoordeelt de instelling of een rekening wel voor eigen gebruik wordt aangehouden en gebruikt. Banken houden bijvoorbeeld soms een rekening op eigen naam aan bij een andere instelling, maar de gelden op die rekening zijn van een cliënt(en) van de bank en de transacties vinden voor rekening en risico van die cliënt(en) plaats. In dit soort gevallen overweegt de instelling of nog wel aan artikel 6 Wwft (vereenvoudigd cliëntenonderzoek vanwege een laag risico) wordt voldaan of dat de instelling toch conform artikel 3 Wwft dient te handelen met betrekking tot de cliënt(en) voor wiens rekening en risico wordt gehandeld of dat de relatie met de andere bank als hoger risico (conform artikel 8 Wwft) moet worden behandeld.

Het toepassen van artikel 6 laat onverlet dat instellingen genoeg informatie verzamelen om hun sanctiewetcontroles uit te voeren. Zie meer over sanctieregelgeving in hoofdstuk 7.

Artikel 7 Wwft bevat een specifieke uitzondering op bepaalde onderdelen van de CDD-verplichtingen omschreven in artikelen 3 en 4 Wwft, waar het gaat om zakelijke relaties en transacties waarbij elektronisch geld een rol speelt. Opgemerkt wordt dat de uitzondering beperkt is en met veel voorwaarden omgeven. Deze uitzondering laat bovendien onverlet dat de verplichtingen in artikel 3 tweede lid onder d Wwft van toepassing is. Dit betekent dat de verplichting tot een voortdurende controle op de zakelijke relatie (het doen van transactiemonitoring) onverkort geldt.

4.9 Verscherpt cliëntenonderzoek en hoog-risico factoren

Artikel 8, eerste lid, onderdeel a, Wwft schrijft voor dat bij een hoger witwas- en terrorisme-financieringsrisico verscherpt cliëntenonderzoek dient plaats te vinden. Verscherpt cliënten-onderzoek wordt in ieder geval toegepast in de volgende gevallen: (i) indien de zakelijke relatie of transactie naar haar aard een hoger risico op witwassen of financieren van terrorisme met zich brengt of, (ii) indien de cliënt woonachtig is, gevestigd is of zijn zetel heeft in een door de Europese Commissie op grond van artikel 9 van de vierde anti-witwasrichtlijn aangewezen staat met een hoger risico op witwassen of financieren van

terrorisme.[45] In de overige leden van artikel 8 staan nog andere gevallen waarin in ieder geval verscherpt cliëntenonderzoek plaatsvindt zoals bij de Politiek Prominente Persoon.

Of er sprake is van een hoog-risico situatie (waarbij verscherpt cliëntenonderzoek wordt toegepast) bepaalt een instelling zelf aan de hand van een risicobeoordeling. Instellingen houden in hun risicobeoordeling rekening met de lijst (niet-limitatieve) risicofactoren zoals genoemd in bijlage III van de vierde anti-witwasrichtlijn. Deze factoren zijn handvatten voor instellingen om in te kunnen schatten of er sprake is van een hoog-risico situatie. De genoemde voorbeelden zijn echter niet uitputtend, er kunnen ook andere factoren zijn die een indicatie zijn van hoog-risico. Instellingen stellen beleid en procedures op aan de hand van hun risicobeoordeling en identificeren in welke gevallen er sprake is van hoog-risico met in achtneming van bijlage III van de richtlijn. Een voorbeeld hiervan is een zakelijke relatie of transacties op afstand; het niet fysiek aanwezig zijn van de cliënt bij de acceptatie. In 4.9.1 wordt hier nader op ingegaan.

In gevallen waarin volgens de instelling een hoger risico bestaat op witwassen of financieren van terrorisme, neemt de instelling aanvullende beheersmaatregelen (Bovenop de maatregelen die op grond van artikel 3 Wwft genomen zijn). Deze maatregelen verschillen per risico. De aanvullende maatregelen die de instelling treft zijn afhankelijk van de risicobeoordeling van de instelling ten aanzien van de betreffende cliënt, transactie, product en het betrokken land of gebied.

Daarnaast bepaalt de Wwft dat een instelling redelijke maatregelen neemt om alle complexe en ongebruikelijk grote transacties, en alle ongebruikelijke transactiepatronen die geen duidelijk economisch of rechtmatig doel hebben, te onderzoeken. Daarbij dient de gehele zakelijke relatie met de cliënt aan een verscherpte controle te worden onderworpen.[46]

Hoog-risico cliënt, product, transactie en land

Wanneer jurisdicties door de Europese Commissie en/of de FATF zijn geïdentificeerd als jurisdicties die in onvoldoende mate een systeem ter voorkoming van witwassen en terrorismefinanciering hebben opgezet, moet dit worden gezien als een van de factoren die het risico op witwassen en terrorismefinanciering van een zakelijke relatie of transactie vergroot.[47] Instellingen dienen in dat geval aanvullende maatregelen te treffen om het verhoogde risico te mitigeren. Wanneer de cliënt geen natuurlijke persoon is, dan beoordeelt de instelling welke maatregelen zij treft om de juridische status van de cliënt vast te stellen. De te treffen maatregelen zijn afhankelijk van het risico van de desbetreffende jurisdictie. Indien sprake is van een cliënt die een Nederlandse rechtspersoon is, maar met een UBO woonachtig in een dergelijke

45 Naast de Europese Commissie houdt de Financial Action Task Force een landenlijst bij met 'High-risk and other monitored jurisdictions' te raadplegen op http://www.fatf-gafi.org/countries/.
46 Artikel 8, lid 3, Wwft.
47 Zie de DNB Q&A over FATF waarschuwingslijsten, te raadplegen op: http://www.toezicht.dnb.nl/3/50-223306.jsp.

Lijst van factoren van potentieel hoger risico uit bijlage III van de vierde anti-witwasrichtlijn.

Cliëntgebonden risicofactoren:

- de zakelijke relatie vindt in ongebruikelijke omstandigheden plaats;
- cliënten die inwoner zijn van geografische gebieden met een hoger risico als vermeld in punt 3);
- rechtspersonen of juridische constructies die vehikels zijn voor het aanhouden van persoonlijke activa;
- vennootschappen met gevolmachtigde aandeelhouders of met aandelen aan toonder;
- bedrijven waar veel geldverkeer in contanten plaatsvindt;
- de eigendomsstructuur van de vennootschap lijkt ongebruikelijk of buitensporig complex gezien de aard van de vennootschapsactiviteit;
- de cliënt is een onderdaan van een derde land die in de lidstaat verblijfsrechten of het staatsburgerschap aanvraagt in ruil voor kapitaaloverdrachten, de aankoop van onroerend goed of overheidsobligaties of investeringen in vennootschappen in die lidstaat.

Product-, dienst-, transactie- of leveringskanaalgebonden risicofactoren:

- private banking;
- producten of transacties die anonimiteit bevorderen;
- zakelijke relaties op afstand of transacties op afstand, zonder bepaalde garanties, zoals elektronische identificatiemiddelen of relevante vertrouwensdiensten zoals gedefinieerd in Verordening (EU) nr. 910/2014 of ieder andere identificatieproces dat veilig is, op afstand of langs elektronische weg plaatsvindt en door de relevante nationale autoriteiten is gereglementeerd, erkend, goedgekeurd of aanvaard;
- betalingen die worden ontvangen van onbekende of niet-verbonden derden;
- nieuwe producten en nieuwe zakelijke praktijken, daaronder begrepen nieuwe leveringsmechanismen, en het gebruik van nieuwe of in ontwikkeling zijnde technologieën voor zowel nieuwe als reeds bestaande producten;
- transacties in verband met aardolie, wapens, edele metalen, tabaksproducten, culturele kunstvoorwerpen en andere artikelen van archeologisch, historisch, cultureel en religieus belang of met grote wetenschappelijke waarde, alsook ivoor en beschermde soorten.

Geografische risicofactoren:
- onverminderd artikel 9, landen die op basis van geloofwaardige bronnen zoals wederzijdse beoordelingen, gedetailleerde evaluatierapporten, of gepubliceerde follow-uprapporten, worden aangemerkt als een land zonder effectieve AML/CFT-systemen;
- landen die volgens geloofwaardige bronnen significante niveaus van corruptie of andere criminele activiteit hebben;
- landen waarvoor sancties, embargo's of soortgelijke maatregelen gelden die bijvoorbeeld door de Unie of de Verenigde Naties zijn uitgevaardigd;
- landen die financiering of ondersteuning verschaffen voor terroristische activiteiten, of op het grondgebied waarvan als terroristisch aangemerkte organisaties actief zijn.

staat, betekent dit dat de instelling deze UBO ook als hoog risicofactor zou moeten meenemen.

Ook voor transacties en zakelijke relaties die verband houden met deze staten worden bijzondere maatregelen getroffen die kunnen variëren van extra controles op zakelijke relaties en correspondentrelaties, en het beperken of het niet uitvoeren van transacties.

Bij de acceptatie van cliënten die een product met een verhoogd risico afnemen, bijvoorbeeld producten of combinaties daarvan die afwijken van standaardproducten, kan niet worden volstaan met alleen standaardprocedures. De instelling doet dus meer dan alleen controleren of de cliënt of andere betrokkenen voorkomen op de sanctielijsten, of men kredietwaardig is (Bureau Krediet Registratie), of identiteitsdocumenten echt zijn (VIS) en of de cliënt voorkomt in interne of externe waarschuwingssystemen van instellingen. Aanvullende informatie kan betrekking hebben op de reputatie van de klant, van de UBO, maar ook van personen waarmee deze geassocieerd worden. Het verkrijgen en beoordelen van informatie over de zakelijke activiteiten en (negatieve) achtergrondinformatie over de klant hoort hier ook bij. Ook doet de instelling in het kader van het verscherpte cliëntenonderzoek diepgaander onderzoek naar de bron van de middelen.

Artikel 9, tweede lid, Wwft expliciteert welke bijzondere maatregelen kunnen worden vastgelegd in een ministeriële regeling, waar het gaat om cliënten en hun UBO's die wonen of gevestigd zijn in derde hoog-risico landen (landen die door de Europese Commissie als zodanig worden aangewezen). Maatregelen die genoemd worden zijn aanvullende informatie verzamelen over het doel en de aard van de zakelijke relatie, de herkomst van de fondsen die bij de zakelijke relatie of de transactie gebruikt worden en de bron van het vermogen van die cliënten en van die UBO's. Daarnaast wordt genoemd dat gegevens van deze cliënten zeer regelmatig geactualiseerd worden en dat de zakelijke relatie en de bijbehorende transacties extra gecontroleerd worden. Hierbij worden ook aanvullende informatie over de

achtergrond van en beweegredenen voor de transacties wordt verzameld. Artikel 9, derde lid, kent een vergelijkbare opsomming waar het gaat om transacties, zakelijke relaties en correspondentbankrelaties gerelateerd aan derde hoog-risico landen. Een ministeriële regeling op grond van artikel 9 Wwft is op het moment van publiceren van deze Leidraad nog niet vastgesteld.

4.9.1 Niet fysieke aanwezigheid cliënt

Tot 25 juli 2018 werd in artikel 8 Wwft verscherpt cliëntenonderzoek vereist in het geval van niet fysieke aanwezigheid van de cliënt bij de identificatie en verificatie van diens identiteit. Het risico van niet fysieke aanwezigheid is nu opgenomen in bijlage III bij de richtlijn als een van de hoog-risicofactoren. Artikel 8 Wwft verwijst naar deze bijlage. Het resultaat van deze wijziging is dat instellingen op basis van een risicogebaseerde benadering bepalen welke maatregelen worden genomen die het hogere risico van niet fysieke aanwezigheid compenseren. Hierbij staat voorop dat instellingen géén zakelijke relatie aangaan of transacties uitvoeren indien het cliëntenonderzoek niet is afgerond ingevolge artikel 3, 5 en 8 Wwft. Benadrukt wordt dat de maatregelen die worden genomen indien de cliënt niet fysiek aanwezig is op grond van artikel 8 komen bovenop de maatregelen die op grond van artikel 3 worden genomen. Niet fysieke-aanwezigheid van de cliënt en het toepassen van innovatieve technieken worden in bijlage III als hoog-risicofactoren genoemd. Dat cliënten op afstand geaccepteerd zijn door het toepassen innovatieve technieken betekent niet dat deze cliënten per definitie een hoge risicoclassificatie meekrijgen na de acceptatie (zie onderdeel 3.4).

Een instelling moet vaststellen of de opgegeven identiteit daadwerkelijk overeenkomt met de identiteit van de persoon die zich heeft aangediend. Instellingen zullen dus moeten kunnen vaststellen dat het identiteitsdocument hoort bij de persoon die zich niet fysiek heeft aangediend. Immers, instellingen moeten weten met wie zij zaken doen. Het zal daarom ook niet voldoende zijn te beschikken over twee identiteitsbewijzen waarvan niet vaststaan dat deze daadwerkelijk horen bij de potentiële cliënt. Er zullen meerdere onafhankelijke en betrouwbare bronnen dienen te worden geraadpleegd. Een instelling zal een inschatting maken welke bronnen daadwerkelijk onafhankelijk en betrouwbaar zijn. De wijze van totstandkoming van de bronnen is daarbij belangrijk. Ook is belangrijk in hoeverre de gegevens van de betreffende bron geverifieerd zijn. Tot slot beoordeelt de instelling de overgelegde documenten en andere bronnen op echtheid en houdt rekening met het risico op vervalsingen en pogingen tot misleiding.

Een instelling kan ook innovatieve technologieën toepassen om het (verscherpte) cliëntenonderzoek in te richten, zolang het hogere risico van de niet fysieke aanwezigheid van de cliënt gemitigeerd wordt. De instelling kan hiertoe nieuwe processen bedenken voor het inrichten van de identificatie en verificatie van de cliënt. Denk hier bijvoorbeeld aan (een combinatie van) video-identificatie en verificatie, het uitlezen van de chip op het identiteitsdocument, het toepassen van een liveness-check en het gebruik van een eID-middel met een adequaat betrouwbaarheidsniveau. Hoe dit proces er precies uitziet, bepaalt de instelling zelf op een risico gebaseerde wijze met in achtneming van de

verplichtingen opgenomen in artikel 3, 5 en 8 Wwft – de vastlegging en regelmatige herziening is hierbij van belang. Hierbij wordt opgemerkt dat het toepassen van nieuwe technologieën wordt genoemd als hoog-risicofactor in bijlage III van de vierde anti-witwasrichtlijn. Op 23 januari 2018 heeft de European Banking Authority in samenwerking met de andere European Supervisory Authorities (ESMA, EIOPA) een opinie over het toepassen van innovatie t.a.v. het cliëntenonderzoek gegeven.[48] Deze opinie biedt kaders voor het toepassen van innovatie in het 'Customer Due Diligence proces' door instellingen.

Bij het toepassen van innovatieve technologieën houden instellingen in ieder geval rekening met de volgende aspecten:

- whether or not firms have appropriate technical skills to oversee the development and proper implementation of innovative solutions, particularly where these solution are developed or used by a third party (where reliance is placed on such third party in line with Article 25 of Directive (EU) 2015/849) or an external provider;
- whether or not the senior management and the compliance officer have appropriate understanding of the innovative solution; and
- whether or not firms have proper contingency plans in place.[49]

4.9.2 Politiek prominente personen (PEP's)

Artikel 8, vijfde lid, Wwft verplicht instellingen tot het toepassen van verscherpt cliëntenonderzoek ten aanzien van een politiek prominente persoon. Het begrip politiek prominente persoon, beter bekend als de PEP (politically-exposed person), is een persoon die een "prominente publieke functie"[50] bekleedt of heeft bekleed. De relevante prominente publieke functies zijn omschreven in artikel 2 van het Uitvoeringsbesluit Wwft 2018. De regels met betrekking tot PEP's zijn van overeenkomstige toepassing op directe familieleden en naaste geassocieerden van een PEP. In het Uitvoeringsbesluit staan de functietitels omschreven van de personen die als zodanig worden aangeduid. De omschrijving van deze functies is niet limitatief. Een persoon wordt door de instelling beschouwd als PEP zo lang als nodig is. Indien een PEP niet meer als zodanig kwalificeert moet het verscherpt cliëntenonderzoek nog ten minste 12 maanden worden toegepast. Deze periode wordt verlengd zo lang als nodig totdat deze persoon niet langer een hoger risico vertegenwoordigt.

Met de implementatie van de vierde anti-witwas-richtlijn is de behandeling PEP's strenger geworden. Ook de binnenlandse PEP's worden nu aangemerkt als hoog risico. De vierde anti-witwasrichtlijn overweegt dat publieke functies die op lager dan nationaal niveau worden uitgeoefend gewoonlijk niet als prominent behoeven te worden aangemerkt.[51]

48 Zie de 'Opinion on the use of innovative solutions in the customer due diligence process' gepubliceerd op 23 januari 2018, te raadplegen op: https://www.eba.europa.eu/-/esas-publish-opinion-on-the-use-of-innovative-solutions-in-the-customer-due-diligence-process
49 Ibid.
50 Zie de definitie van politiek prominente persoon in artikel 1 Wwft.
51 Artikel 3, lid 9, van de vierde anti-witwasrichtlijn bevat 'Middelbare of lagere ambtenaren vallen niet onder de in de punten a) tot en met h) bedoelde publieke functies'.

Wanneer de politieke invloed ervan echter vergelijkbaar is met die van soortgelijke posities op nationaal niveau, wordt van instellingen verwacht dat zij overwegen om ook deze personen als hoog risico aan te merken.

PEP's in Nederland

De Rijksoverheid heeft op 18 september 2019 een concretisering van de functies die in Nederland als politiek prominent worden gekwalificeerd gepubliceerd. Instellingen moeten naar personen die een dergelijke functie vervullen, verscherpt cliëntenonderzoek verrichten.

De concretisering is hier te raadplegen.

Zakelijke relaties met dienstverlening aan PEP's vereisen aanvullende maatregelen omdat deze hogere integriteitrisico's en een grotere kans op reputatieschade met zich meebrengen. Daarnaast vergt dienstverlening aan PEP's bijzondere aandacht in het kader van het internationale beleid inzake de bestrijding van corruptie. Volgens overweging 32 van de vierde anti-witwasrichtlijn kunnen zakelijke relaties met PEP's, vooral wanneer zij afkomstig zijn uit landen waar corruptie veelvuldig voorkomt, een groot reputatierisico en/of juridisch risico met zich meebrengen voor de financiële sector. Hierbij kan gedacht worden aan passieve omkoping (het ontvangen van steekpenningen) of de verduistering van overheidsgelden. Een instelling stelt daarom risico-gebaseerde procedures en maatregelen in om PEP's te kunnen herkennen, en op basis van artikel 8, vijfde lid, nemen instellingen passende maatregelen om de bron van het vermogen en van de middelen die bij de zakelijke relatie of de transactie gebruikt worden vast te stellen. Verder bepaalt het vijfde lid dat de zakelijke relatie doorlopend aan verscherpte controle wordt onderworpen.

Instellingen beoordelen bij cliëntacceptatie en periodiek of haar cliënt én de UBO kwalificeert als PEP. Dit geldt dus ook voor de natuurlijke personen die in belangrijke mate invloed kunnen uitoefenen of belangen hebben, dan wel een grote mate van invloed op meer ingrijpende besluiten van een personenvennootschap hebben of het beleid van een personenvennootschap wezenlijk naar hun hand kunnen zetten. De Wwft vereist dat instellingen hiertoe over op risico gebaseerde procedures en maatregelen beschikken: de diepgang van dat onderzoek varieert al naar gelang het risicoprofiel van de cliënt of UBO.

Op basis van artikel 8, vijfde lid, Wwft ligt de beslissing tot het aangaan van een zakelijke relatie met een PEP of het verrichten van een transactie voor een PEP bij het hoger leidinggevend personeel.[52] Dit geldt ook voor de beslissing om een relatie te continueren met een cliënt die gedurende de relatie kwalificeert als PEP. Dit geldt ook voor (pseudo-)UBO's die kwalificeren als PEP.

52 Artikel 1 Wwft: hoger leidinggevend personeel: a. personen die het dagelijks beleid van een instelling bepalen; of b. personen werkzaam onder verantwoordelijkheid van een instelling, die een leidinggevende functie vervullen direct onder het echelon van de dagelijks beleidsbepalers en die verantwoordelijk zijn voor natuurlijke personen wier werkzaamheden van invloed zijn op de blootstelling van een instelling aan de risico's op witwassen en het financieren van terrorisme. NB: dit is niet dezelfde invulling van het begrip 'hoger leidinggevend personeel' zoals dat wordt gebruikt in het kader van onderzoek naar de UBO.

Hoe gaan instellingen het beste om met PEP's?

- Instellingen controleren bij het aangaan van de zakelijke relatie of de cliënt, of de UBO van de cliënt, een PEP is.
- Deze controle wordt daarnaast periodiek en bij signalen en wijzigingen herhaald. De PEP is onderdeel van de risicobeoordeling of vormt een aparte risicocategorie. Indien PEP's niet worden geaccepteerd, wordt dit gezien als een risicocategorie: onacceptabel risico.
- Hoger leidinggevend personeel beslist over de acceptatie van PEP's.
- Compliance is meebesluitend, meetekenend of adviserend bij dossiers met PEP's.

Instellingen die PEP's in hun cliëntenbestand hebben, kunnen hun interne procedures om doorlopend controle uit te oefenen op deze zakelijke relatie risicogebaseerd inrichten. Zo zijn kinderen van een Kamerlid in Nederland met een eenvoudige betaalrekening mogelijk minder risicogevoelig dan de echtgenote van een staatshoofd van een land met een verhoogd corruptierisico, die een private banking rekening opent. Dit neemt echter niet weg dat PEP's in de basis een hoger risico vertegenwoordigen.

Bij het cliëntenonderzoek naar PEP's accepteert de instelling niet zomaar de door de cliënt zelf verstrekte informatie, maar controleert zij deze waar mogelijk door onderzoek en toetst deze in ieder geval op geloofwaardigheid. In dat kader kan het van pas komen om te weten wat het corruptieniveau is in het land waar de persoon de functie bekleedt. Hiertoe kan bijvoorbeeld de Corruption Perception Index van Transparency International worden gebruikt.[53]

Wanneer de cliënt of een UBO gedurende de zakelijke relatie een PEP wordt of blijkt te zijn, voldoet de instelling zo snel mogelijk aan deze aanvullende maatregelen. Met name het vaststellen van de bron van het vermogen van de UBO die een PEP is, kan in bepaalde situaties moeilijk zijn, hoewel de intensiteit kan worden afgestemd op het risico. In gevallen waarin het niet lukt om de bron van het vermogen vast te stellen, moet de instelling kunnen aantonen dat er voldoende inspanningen zijn verricht om de bron van het vermogen te achterhalen.

Tot slot zal de instelling bij iemand die niet langer PEP is, op grond van artikel 8 zevende lid, Wwft de PEP procedure hanteren totdat de persoon in kwestie niet langer het hoger risico met zich brengt dat hoort bij een PEP en dat is ten minste gedurende 12 maanden.

Aanvullende informatie

- FATF, Guidance: Politically Exposed Persons (Recommendations 12 and 22), http://www.fatf-gafi.org/documents/documents/peps-r12-r22.html
- The Wolfsberg Group, FAQ over PEP's, 2008, http://www.wolfsberg-principles.com/pdf/faq/Wolfsberg_PEP_FAQs_(2008).pdf
- Transparency International, http://www.transparency.org

53 Voor meer informatie: https://www.transparency.org/research/cpi/overview.

4.9.3 Correspondentrelaties

Met de implementatie van de vierde anti-witwasrichtlijn, is het begrip 'correspondent-*bank*relatie' vervangen door correspondentrelatie.[54] Het ziet thans niet slechts op relaties tussen banken, maar ook op relaties tussen banken en andere financiële ondernemingen – zoals betaaldienstverleners – en andere financiële ondernemingen onderling.

Op grond van artikel 8 Wwft moet een instelling verscherpt cliëntenonderzoek uitvoeren indien een correspondentrelatie wordt aangegaan met een instelling die is gevestigd buiten de EU. Verwacht wordt van instellingen dat zij zich een goed beeld vormen van andere instellingen uit staten die geen EU-lidstaat zijn en waar correspondentrelaties mee aangegaan worden. Bij correspondentrelaties treedt een instelling feitelijk op als agent voor een andere instelling door het verzorgen van betalingen of het verrichten van andere diensten voor een cliënt van deze correspondentrelatie.

Vanwege het hogere risico ligt de beslissing tot het aangaan van een correspondentrelatie bij hoger leidinggevend personeel in gevolge artikel 8, vierde lid, onder c.

Alertheid is geboden op mogelijk gebruik van een correspondentrekening door (niet-geïdentificeerde) derden (transitrekening of payable-through-account), dus wanneer een cliënt van die buitenlandse instelling direct toegang heeft tot de rekening die deze instelling aanhoudt bij de Nederlandse instelling. De reden waarom aan deze categorie verhoogde aandacht geschonken dient te worden, ligt in het feit dat het gaat om dienstverlening op afstand.

Er kunnen redenen zijn om ook verscherpt cliëntenonderzoek uit te voeren bij het aangaan van een correspondentrelatie met een instelling die in een lidstaat is gevestigd. Bijvoorbeeld indien er feiten en omstandigheden zijn die kunnen duiden op een hoger risico op witwassen of terrorismefinanciering of wanneer dit op grond van de interne risicoclassificatie van de instelling wordt voorgeschreven.

Ten overvloede wordt opgemerkt dat de verplichtingen van artikel 8 Wwft, gelden in aanvulling op die van artikel 3, tweede tot en met vierde lid, Wwft. Dat betekent onder meer dat de verplichting tot voortdurende controle op de zakelijke relatie zoals vermeld staat in artikel 3 tweede lid onder d Wwft onverkort van toepassing is op correspondentrelaties.

54 Thans luidt de definitie: correspondentrelatie:
a. het verlenen van bankdiensten door een bank als correspondent aan een andere bank als respondent, met inbegrip van het verstrekken van een lopende of andere passiefrekening en aanverwante diensten, zoals contantenbeheer, internationale geldovermakingen, verwerking van cheques, transitrekeningen en valutawisseldiensten; of
b. de betrekkingen tussen banken onderling, andere financiële ondernemingen onderling, of tussen banken en andere financiële ondernemingen, waar soortgelijke diensten als bedoeld onder a door een correspondentinstelling aan een respondentinstelling worden verleend, met inbegrip van betrekkingen die zijn aangegaan voor effectentransacties of geldovermakingen;

Aanvullende informatie

- The Wolfsberg Group, aanbevelingen voor correspondentbankieren
- The Wolfsberg Group, Correspondent Banking FAQ
- FATF, Guidance on Correspondent Banking, 2016
- Basel Committee on Banking Supervision, Sound management of risks related to money laundering and financing of terrorism – annex 2 Correspondent banking, 2017

Ten aanzien van openbare bronnen is naast het gebruik van het internet op de volgende in internationale context geaccepteerde documenten te wijzen:

- De Wolfsberg Group heeft in samenwerking met Bankers Almanac een internationale database voor financiële ondernemingen opgezet, de Due Diligence Repository.
- De evaluatierapporten van internationale organisaties zoals de FATF, IMF en Wereld Bank. De instelling kan op basis van deze rapporten om bepaalde informatie aan de instelling vragen, met name ten aanzien van het toezicht dat wordt uitgeoefend.

4.10 Uitbesteding

Een instelling kan op grond van artikel 10 Wwft het cliëntenonderzoek laten verrichten door een derde. Met de wijziging van de Wwft in het kader van de implementatie van de vierde anti-witwasrichtlijn is verduidelijkt dat deze bepaling betrekking heeft op uitbesteding- of agentuurverhoudingen.[55] De bepaling ziet namelijk niet op de introductie van cliënten door andere banken of andere financiële onderneming als bedoeld in artikel 5, eerste lid, Wwft. Een instelling kan cliëntenonderzoek uitbesteden waar het gaat om het identificeren van de cliënt, de UBO, een trust of een personenvennootschap en het verifiëren van de identiteit van die personen en entiteiten, alsmede het vaststellen van het doel en de beoogde aard van de zakelijke relatie. Het monitoren van de zakelijke relatie kan alleen de instelling zelf uitvoeren.[56]

De instelling die het onderzoek heeft uitbesteed blijft verantwoordelijkheid voor het naleven van vereisten met betrekking tot het cliëntenonderzoek. Bij uitbesteding aan een derde partij moet de instelling daarom een zichtbare risico-overweging maken die mede ziet op de deskundigheid en de praktische aanpak van de derde partij tot naleving van de Wwft. Daarbij is het van belang dat de instelling niet alleen vastlegt dat de derde partij voldoet aan de Wwft en waar nodig aan de beleidsregels van de instelling, maar dat de instelling dit ook periodiek controleert, vaststelt en desgewenst hierover rapporteert aan de derde partij.

Voor meer informatie over risico's bij uitbesteding zie de DNB 'Good practices beheersing risico's bij uitbesteding' uit 2017.

55 TK, 2017-18, 34 808, nr. 3, p. 57.
56 Artikelen 3, lid 2, onderdeel d, van de Wwft wordt namelijk niet genoemd in artikel 10, lid 1, Wwft. Voor instellingen die onder de Wft vallen en waarbij de uitvoerende partij behoort tot dezelfde groep, kan deze voortdurende controle door deze partij binnen de groep worden uitgevoerd.

5 Transactiemonitoring en melden ongebruikelijke transacties

5.1 Algemeen

Financiële instellingen zijn wettelijk verplicht maatregelen te nemen om witwassen en terrorismefinanciering te voorkomen. Hierdoor moeten instellingen bijzondere aandacht besteden aan ongebruikelijke transactiepatronen en transacties[57] van cliënten, die naar hun aard een hoger risico op witwassen of het financieren van terrorisme met zich brengen. Is er aanleiding om te veronderstellen dat een (voorgenomen) transactie verband houdt met witwassen of terrorismefinanciering, dan moet de instelling deze transactie als ongebruikelijk melden bij de Financial Intelligence Unit – Nederland (FIU – NL), zie vanaf 5.5 voor informatie over het melden. Om dit te kunnen doen is het van cruciaal belang dat instellingen beschikken over een effectief transactiemonitoringsproces.

De eerste stap in het transactiemonitoringsproces is risico-identificatie. Tijdens het identificatieproces analyseren instellingen systematisch de witwas- en terrorismefinancieringsrisico's. De uitkomsten van deze analyse worden vastgelegd in de SIRA (zie ook hoofdstuk 3.2). De SIRA vormt de basis voor beleid, bedrijfsprocessen en procedures omtrent transactiemonitoring. Instellingen vertalen de in de SIRA geïdentificeerde risico's zichtbaar door naar het transactiemonitoringsproces. Ook het transactiemonitoringsproces kent een risicogebaseerd karakter.

Bij het identificeren en analyseren van de risico's hoort ook dat cliënten ingedeeld worden in risicocategorieën, bijvoorbeeld hoog, midden en laag, op grond van de risico's die de zakelijke relatie met de cliënt met zich brengt (zie ook hoofdstuk 3.4). Voor de bepaling van het risicoprofiel van een cliënt maken instellingen een transactieprofiel op basis van de verwachte transacties of het verwachte gebruik van de rekening van een cliënt of cliëntgroep. Door een transactieprofiel op te stellen kunnen instellingen in voldoende mate monitoren dat de transacties die tijdens de duur van de relatie verricht worden, overeenkomen met de kennis die de instelling heeft van de cliënt en diens risicoprofiel. Door het verwachte transactiegedrag van de cliënt in beeld te brengen kunnen instellingen toetsen of de door de cliënt uitgevoerde transacties afwijken. Het is mogelijk dat transactieprofielen van cliënten aan de hand van 'peer-grouping' worden opgesteld. Gedurende de duur van de relatie is het van belang dat de instelling periodiek toetst of de cliënt nog steeds aan het risicoprofiel voldoet en het transactiepatroon overeenkomstig de verwachtingen is. De instelling kan de frequentie en intensiteit van reviews afstemmen op de risicoclassificatie van de cliënt.

Het monitoren van de relatie met de cliënt en de transacties van de cliënt kan worden afgestemd op het soort relatie met- en het risicoprofiel van de relatie. Per sector en per product kan dit verschillend zijn. Zo kan bijvoorbeeld voor

57 Onder transactie wordt verstaan: Handeling of samenstel van handelingen van of ten behoeve van een cliënt waarvan de instelling ten behoeve van haar dienstverlening aan die cliënt heeft kennisgenomen.

Good practices transactiemonitoring

DNB biedt handvatten hoe instellingen het transactiemonitoringsproces kunnen inrichten en verbeteren. Voor deze Good practices heeft DNB gebruik gemaakt van de belangrijkste bevindingen van het in 2016 uitgevoerde thema-onderzoek "post-event transactiemonitoring".

De belangrijkste kenmerken van een adequaat transactiemonitoringssysteem:

1. Instellingen vertalen de risico's op witwassen en terrorismefinanciering die uit de SIRA voortvloeien zichtbaar door naar het transactiemonitoringsproces. Bij de bepaling van het risicoprofiel van de cliënt en/of 'cliënt peergroups' betrekken instellingen ook het verwachte transactiegedrag.
2. Instellingen hebben voldoende beleid voor transactiemonitoring opgesteld en hebben dit beleid voldoende uitgewerkt in onderliggende procedures en werkprocessen.
3. Instellingen beschikken over een (geautomatiseerd) transactiemonitoringssysteem en hebben een onderbouwde en toereikende set aan business rules (detectieregels met scenario's en grenswaarden) om witwas- en terrorismefinancieringsrisico's te detecteren. Instellingen testen deze business rules periodiek, zowel op technische aspecten als effectiviteit.
4. Instellingen beschikken over een adequaat meld- en alertafhandelingsproces. Instellingen zorgen ervoor dat voorgenomen en uitgevoerde ongebruikelijke transacties onverwijld en volledig aan de FIU-NL worden gemeld. In dit proces zijn per alert overwegingen en conclusies vastgelegd om te komen tot het sluiten dan wel escaleren van alerts.
5. Instellingen hebben hun governance ten aanzien van transactiemonitoring zodanig ingericht dat sprake is van een duidelijke functiescheiding, bijvoorbeeld via het three lines of defence model.
6. Instellingen beschikken over een toegesneden trainingsprogramma voor hun medewerkers. De medewerkers zijn zich bewust van witwas- en terrorismefinancieringsrisico's

Naast de belangrijkste kenmerken bevatten de onderstaande Good practices sectorspecifieke voorbeelden.

- Banken
- Betaaldienstverleners
- Money transfers
- Trustkantoren

Zie voor voorbeelden van Fiscale integriteitrisico's de Good practices fiscale integriteitsrisico's banken en trustkantoren (hoofdstuk 6).

levensverzekeringsproducten gedacht worden aan een periodiek controlemoment, bijvoorbeeld bij de betaling van (jaarlijkse) premies, en controlemomenten bij wijzigingen in het contract of de begunstiging. Indien er vanuit de polis een langdurige relatie met de begunstigde ontstaat (bijvoorbeeld bij annuïtaire betalingen), heeft een voortdurende controle op de uitbetalingen geen toegevoegde waarde aangezien deze betalingen door de instelling zelf worden gedaan.

5.2 Patronen en transacties herkennen

Met behulp van uw transactiemonitoringssysteem en gebruik van software analyseren instellingen hun transactiedata. Het systeem genereert op basis van business rules, zogenoemde 'alerts'. Met een alert wordt een signaal bedoeld dat duidt op een mogelijk ongebruikelijke transactie. Deze alerts worden aan onderzoek onderworpen. De bevindingen van het onderzoek naar de alerts dienen adequaat en duidelijk te worden vastgelegd. Wanneer uit de onderzoeksbevindingen blijkt dat de transactie ongebruikelijk is, meldt de instellingen deze transactie onverwijld aan de FIU-NL. De overwegingen en besluitvorming om een transactie wel of niet te melden worden voldoende inzichtelijk gemaakt en vastgelegd. Bij twijfel of een transactie ongebruikelijk is kan de transactie beter wél aan de FIU-NL gemeld worden. Op het moment dat een instelling, al dan niet opzettelijk, niet of niet tijdig voldoet aan de meldplicht, is dat een economisch delict.

Voordat transactiemonitoring plaatsvindt borgen instellingen dat alle data volledig en juist wordt meegenomen in het transactiemonitoringproces. Dit kan data betreffen over bijvoorbeeld de cliënt, de diensten en de transacties. Het begrip transactie wordt in de Wwft ruim opgevat en omschreven als 'handeling of samenstel van handelingen van of ten behoeve van een cliënt ...'. Dit betekent dat alle met de financiële transactiedata samenhangende informatie waarvan de instelling kennisneemt in het kader de dienstverlening, kan worden meegenomen. Is sprake van grotere hoeveelheden transacties, dan ligt het in de rede om de transactiemonitoring geautomatiseerd te laten plaatsvinden, om de effectiviteit, consistentie en doorlooptijd van monitoring te kunnen borgen.

In het systeem zijn op zijn minst vooraf gedefinieerde business rules opgenomen: detectieregels in de vorm van scenario's en grensbedragen. Daarnaast kunnen ook meer geavanceerde systemen gewenst zijn, en in voorkomende gevallen noodzakelijk, afhankelijk van onder meer aard en omvang van de transacties en de aard van de betreffende instelling. Zo zal bijvoorbeeld bij een kleinere instellingen met een beperkt aantal eenvoudige transacties, een zeer geavanceerd systeem minder noodzakelijk zijn. Het kan ook zijn dat een instelling het gebruik van zeer geavanceerde systemen noodzakelijk acht, bijvoorbeeld het gebruik van 'artificial intelligence'.[58] Het gebruik van geavanceerde systemen veronderstelt dat de instelling zelf voldoende kennis bezit om dit soort systemen in te

58 DNB heeft in juli 2019 richtlijnen voor het gebruik van kunstmatige intelligentie gepubliceerd zie: https://www.dnb.nl/nieuws/nieuwsoverzicht-en-archief/DNBulletin2019/dnb385020.jsp

richten en toe te passen. De kwaliteit en effectiviteit van het systeem moet aantoonbaar zijn. Door het laten uitvoeren van een modelvalidatie of audit kan een instelling de kwaliteit en effectiviteit van haar transactiemonitoring adequaat beoordelen.

De verantwoordelijkheid voor het effectief detecteren van ongebruikelijke transacties blijft hoe dan ook liggen bij de instellingen. Een instelling dient de werking van de systemen goed te begrijpen en kan daarom niet enkel steunen op door externe leveranciers aangeleverde algoritmes.

Aandachtspunten bij transactiemonitoring

- Dienen de transacties een economisch of commercieel doel?
- Gaat het om uitzonderlijk grote bedragen?
- Betreft het stortingen, opnames of overboekingen die niet in verhouding zijn tot de normale/verwachte business van de cliënt?
- Is het rekening- en transactieverloop in verhouding met de activiteiten van de cliënt?
- Zijn er transacties van en naar landen met een verhoogd risico?
- Zijn er fiscale integriteitrisico's verbonden aan de wijze waarop de transacties gestructureerd zijn?

5.3 Aandacht voor hoog-risico jurisdicties

De FATF wijst regelmatig op jurisdicties die tekortkomingen hebben in hun systeem ter bestrijding van witwassen en terrorismefinanciering. Het onderhouden van zakelijke relaties met ingezetenen van deze jurisdicties of het uitvoeren van transacties van of naar deze jurisdicties kan een hoger risico op witwassen en terrorismefinanciering met zich meebrengen, hetgeen zou kunnen leiden tot verscherpte transactiemonitoringsmaatregelen. De FATF herziet de lijsten indien daar aanleiding voor is en DNB verwijst naar deze lijsten op haar website.

Ook de Europese Commissie wijst derde landen aan die tekortkomingen hebben in hun systeem ter bestrijding witwassen en terrorismefinanciering.[59] Instellingen houden in hun transactiemonitoring rekening met deze hoog-risico landen.

Naast de waarschuwingen van de Europese Commissie, de FATF en de FATF Associate Members[60] zijn er ook andere betrouwbare bronnen over de mate van implementatie van internationale standaarden op het gebied van het bestrijden van financiële criminaliteit of terroristische activiteiten door een land of jurisdictie.

59 Op grond van artikel 9 van de vierde anti-witwasrichtlijn (2015/849) wijst de Europese Commissie derde landen aan met tekortkomingen ter bestrijding van witwassen en terrorismefinanciering.

60 FATF Associate Members zijn: Asia/Pacific Group on Money Laundering (APG), Caribbean Financial Action Task Force (CFATF), Eurasian Group (EAG), Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering measures and the Financing of Terrorism (MONEYVAL), Financial Action Task Force of Latin America (GAFILAT), Inter Governmental Action Group against Money Laundering in West Africa (GIABA) and the Middle East and North Africa Financial Action Task Force (MENAFATF).

Ook deze kunnen voor een instelling aanleiding zijn om verhoogde aandacht te geven aan de zakelijke relaties en transacties met mensen uit die landen en jurisdicties. Instellingen nemen in het kader van de monitoring de witwas- of terrorismefinancierings-risico's in bepaalde landen in acht.

Aanvullende informatie

- Europese Commissie: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:02016R1675-20181022
- VN: http://www.un.org/sc/committees/1267/index.shtml
- IMF: http://www.imf.org/external/ns/cs.aspx?id=175
- FATF: http://www.fatf-gafi.org/countries/
- OESO: http://www.oecd.org/corruption/
- Transparancy International – Corruption Perception Index: https://www.transparency.org/research/cpi/overview

5.4 Beoordeling transacties, maatregelen en vastlegging

Indien de instelling transacties aantreft die buiten het verwachte patroon en/of profiel vallen of die geen economisch of juridisch doel hebben, dan zal zij onderzoeken wat de achtergrond en doel van de transactie was. Daarbij besteedt een instelling bijzondere aandacht aan ongebruikelijke transactiepatronen en aan transacties die naar hun aard een hoger risico op witwassen of financieren van terrorisme met zich brengen. De bevindingen zullen in het cliëntendossier worden vastgelegd. Indien een transactie aanleiding geeft om te vermoeden dat deze verband houdt met witwassen of terrorismefinanciering zal de transactie onverwijld gemeld worden aan de FIU-NL op grond van artikel 16 Wwft. De overwegingen en besluitvorming om een transactie wel of niet te melden worden door de instelling vastgelegd.

Instellingen beoordelen de gevolgen van een melding aan de FIU-NL en een eventuele terugmelding van de FIU-NL voor het risicoprofiel van de cliënt en stellen vast of eventuele aanvullende beheers-maatregelen genomen moeten worden. Sluitstuk van het transactiemonitoringsproces is de bewaring van gegevens die worden verkregen in het kader van transactiemonitoring. In dit verband bewaart de instelling de gegevens van de melding van de ongebruikelijke transactie en legt deze vast, op zodanige wijze dat die gegevens opvraagbaar zijn en de desbetreffende transactie re-construeerbaar is gedurende vijf jaar na het tijdstip van het doen van de melding.

In de Good practices transactiemonitoring staat een volwassenheidsmodel opgenomen waarin alle stappen van het transactiemonitoringsproces staan omschreven met de daarbij behorende voorwaarden voor een goede inrichting.

5.5 Meldplicht ongebruikelijke transacties

Ingevolge artikel 16 Wwft meldt een instelling een verrichte of voorgenomen ongebruikelijke transactie. De bijlage van artikel 4 van het

Uitvoeringsbesluit 2018 Wwft bevat de lijst met indicatoren op grond waarvan gemeld moet worden. Deze lijst wordt gebruikt ten behoeve van de beoordeling of een transactie als ongebruikelijk moet worden aangemerkt. De indicatoren zijn onderverdeeld in objectieve indicatoren en de subjectieve indicator. De objectieve indicatoren beschrijven een situatie waarin een transactie altijd moet worden gemeld. Uit de bijlage bij het Uitvoeringsbesluit[61] wordt duidelijk welke objectieve indicatoren voor welke instellingen van toepassing zijn. Zo is bijvoorbeeld de geldtransfer-indicator van toepassing op banken, elektronischgeldinstellingen, financiële instellingen, betaaldienstagenten en betaaldienstverleners.

Bij de meldplicht ligt de nadruk echter op de subjectieve indicator. De subjectieve indicator verplicht een instelling om een transactie te melden indien er aanleiding is om te veronderstellen dat de transactie verband kan houden met witwassen of financiering van terrorisme. Deze indicator is van toepassing voor elke instelling die onder de Wwft valt. De instelling zal daarom moeten beoordelen of een bepaalde transactie wellicht melding behoeft omdat er mogelijk sprake is van witwassen of financieren van terrorisme. De instelling heeft dus een eigen verantwoordelijkheid voor het adequaat melden van ongebruikelijke transacties.

Bij indicatoren die zijn gerelateerd aan een grensbedrag beoordeelt de instelling ook of er sprake is van een verband tussen twee of meerdere transacties. Dit kan aan de hand van het soort transactie en de bedragen waar het om gaat. Indien er een verband is, zouden deze transacties onder de subjectieve indicator gemeld kunnen worden.

Met de definitie van transactie[62] is beoogd duidelijk te maken dat een ongebruikelijke transactie van de cliënt, of van een derde ten behoeve van de cliënt, altijd moet worden gemeld indien een instelling daarvan heeft kennisgenomen ten behoeve van haar dienstverlening aan die cliënt. Een direct of causaal verband tussen de ongebruikelijke transactie en de werkzaamheden van de instelling is geen vereiste. De woorden "handeling of samenstel van handelingen van of ten behoeve van een cliënt" dienen zo te worden uitgelegd dat ook een passieve betrokkenheid van de instelling (doordat zij wetenschap heeft van de transactie) de wettelijke meldplicht kan activeren.

5.5.1 Meldplicht levensverzekeraars

Levensverzekeringsproducten zijn over het algemeen producten met een lager witwas- en terrorismefinancieringsrisico. Ondanks het lagere risico blijft de kans aanwezig dat producten die worden afgenomen gefinancierd worden met opbrengsten uit financieel-economische criminaliteit.

61 Het Uitvoeringsbesluit Wwft 2018 is te raadplegen op: https://wetten.overheid.nl/BWBR0041193/2018-07-25.
62 Transactie: handeling of samenstel van handelingen van of ten behoeve van een cliënt waarvan de instelling ten behoeve van haar dienstverlening aan die cliënt heeft kennisgenomen, artikel 1 Wwft.

Ook is er een risico dat vermogen kan worden onttrokken voor het financieren van terrorisme. Op 25 oktober 2018 heeft de FATF de 'Risk-based Approach Guidance for the Life Insurance Sector' uitgebracht.[63] Met dit document worden handvatten geboden om de risicogebaseerde aanpak van levensverzekeraars vorm te geven.

Onderstaande voorbeelden zijn voorbeelden van indicatoren van transacties waarbij er voor de levensverzekeraar aanleiding zal zijn om de transactie verder te onderzoeken en te beoordelen of er factoren zijn waardoor de transactie als ongebruikelijk aangemerkt moet worden. Een aantal van die transacties zal de behandelaar reeds in het initiële werkproces opvallen. Voor een aantal andere indicatoren zal de levensverzekeraar regelmatig query's uitvoeren om te toetsen of transacties mogelijk ongebruikelijk waren.

Voorbeelden voor levensverzekeraars van indicatoren van mogelijke ongebruikelijke transacties.

- Eenmalige hoge initiële storting of hoge bijstorting op polis.
- Premiebetalingen uit een land aangemerkt als hoog-risico land.
- Verhuizing van een in Nederland gevestigde of woonachtige verzekeringnemer, begunstigde of premiebetaler naar een land aangemerkt als hoog-risico land.
- Afgekochte (koopsom)polissen die korter dan 3 jaar hebben gelopen, met een afkoopsom van [€ xx] of meer én afkoopsom bedraagt 50% of meer van de som van betaalde premies
- De verzekeringnemer, begunstigde of premiebetaler is een buitenlandse rechtspersoon of een natuurlijk persoon die niet in Nederland woonachtig of gevestigd is.
- Betalingen naar hoog-risico landen groter dan [€ xx] per jaar.
- Eenmalige uitkeringen van [€ xx] of meer.
- Periodieke uitkeringen op jaarbasis van [€ xx] of meer.
- Premierestitutie koopsom (niet zijnde verzekerde uitkering van premierestitutie) van [€ xx] of meer.
- Polissen die binnen de wettelijke opzegtermijn (30 dagen) worden opgezegd en waarbij sprake is van premiestorting of premierestitutie van [€ xx] of meer.
- Verpandingen of beleningen van de verzekering voor een bedrag van [€ xx] of meer, anders dan ten behoeve van een hypothecaire geldlening.

Meer voorbeelden

FATF, 'Risk-based Approach Guidance for the Life Insurance Sector', 2018

63 De FATF 'Risk-based Approach Guidance for the Life Insurance Sector' is te raadplegen op: http://www.fatf-gafi.org/documents/riskbasedapproach/documents/rba-life-insurance.html?hf=10&b=0&s=desc(fatf_releasedate).

5.5.2 Meldplicht credit Cards

Voor creditcard transacties kunnen onderstaande 'red flags' ondersteuning bieden bij het detecteren van ongebruikelijke transacties.

Voorbeelden van indicatoren van mogelijke ongebruikelijke transacties bij credit card transacties.

Funding van de kaart

1. Contante stortingen op een betaalrekening, waarbij het doel is om de uitgaven van de creditcard te betalen
2. Funding door een derde partij (niet zijnde de kaarthouder) en vanuit het buitenland

Gebruik van de kaart

- Excessief ATM-gebruik of retourboekingen naar een andere rekening door natuurlijke personen zonder een duidelijke ratio
- Excessieve aanschaf van andere card of stored value (vouchers) producten
- Frequente en aanzienlijke transacties bij casino's
- Frequente en/of aanzienlijke transacties bij non-profitorganisaties (donaties)
- (Vermeende) levering van niet-tastbare goederen of diensten
- Concentratie van frequente hoogwaardige transacties door een kleine groep kaarthouders bij bepaalde merchants (aanschaf luxe producten)
- Gestructureerd gebruik maken van gestolen creditcards bij E-commerce merchants

Overige signalen

- Identificatie en/of verificatieproblemen (aanvrager en/of UBO)
- Afhankelijkheid merchant van bepaalde kaarthouders door omzet (volume)
- Relaties tussen kaarthouder(s) en merchant(s) (criminele organisatie en anoniem gebruik)
- Valsheid in geschrifte
- Cybercrime (onder andere door phishing, skimming en inzet van malware)

5.6 FIU meldprocedure

Het is inherent aan de meldplicht van artikel 16 Wwft dat instellingen processen en procedures hebben om het ongebruikelijke karakter van transacties te herkennen en te melden. Instellingen melden (voorgenomen) ongebruikelijke transacties onverwijld bij FIU-NL nadat het ongebruikelijke karakter van de transactie bekend is geworden. Verder ligt het in de rede, zoals ook in de bijlage bij het Uitvoeringsbesluit Wwft 2018 is vermeld, dat transacties die in verband met witwassen of terrorismefinanciering aan politie of Openbaar Ministerie worden gemeld, ook aan de FIU-NL worden gemeld; er is immers een vermoeden van witwassen of terrorismefinanciering.

De Wwft geeft een opsomming van de gegevens die bij een melding moeten worden verstrekt. Deze gegevens zijn voor de FIU-NL van essentieel belang om een ongebruikelijke transactie te kunnen analyseren. Indien een instelling stelselmatig bepaalde gegevens niet aanlevert, kan de FIU-NL deze omissie in het meldgedrag aan de toezichthouder doorgeven en zou de toezichthouder de instelling een aanwijzing kunnen geven om interne procedures en controles ter voorkoming van witwassen en terrorismefinanciering te ontwikkelen.

Meldprocedure FIU

Instellingen die onder meldplicht vallen zoeken contact met FIU Nederland om toegang te krijgen tot het meldportaal. Meer informatie is te vinden op de website van de FIU.

5.7 Vrijwaringen

De Wwft kent een strafrechtelijke vrijwaring in artikel 19 Wwft en een civielrechtelijke vrijwaring in artikel 20 Wwft. De strafrechtelijke vrijwaring ziet er op toe dat gegevens of inlichtingen die de instelling te goeder trouw bij melding verstrekt, niet kunnen worden gebruikt ten behoeve van een opsporingsonderzoek of strafrechtelijke vervolging van de instelling ter zake van witwassen of financieren van terrorisme. De wet breidt deze vrijwaring uit tot degene die de melding heeft gedaan. Gedacht kan worden aan een medewerker van een bank die voor de melding heeft zorg gedragen of die aan het opstellen van het meldingsbericht heeft meegewerkt.

De civielrechtelijke vrijwaring houdt in dat een instelling niet civielrechtelijk aansprakelijk is voor de schade die iemand anders (de cliënt of een derde) als gevolg van een melding lijdt wanneer is gehandeld in de redelijke veronderstelling dat uitvoering wordt gegeven aan de meldplicht. Hierbij kan gedacht worden aan eisen gesteld in een civielrechtelijke procedure op grond van wanprestatie, indien de instelling heeft besloten een transactie niet uit te voeren en deze te melden. Ook is een actie op grond van een onrechtmatige daad voorstelbaar, wegens eventuele schade die mogelijk is ontstaan ten gevolge van de melding door een instelling.

Uiteraard gelden deze vrijwaringen alleen indien de melding te goeder trouw en op correcte wijze, conform de vereisten van de Wwft heeft plaatsgevonden.

5.8 Geheimhouding Wwft

De Wwft kent een geheimhoudingsplicht voor instellingen ingevolge artikel 23 Wwft. Instellingen zijn onder andere verplicht geheim te houden dat een artikel 16 Wwft melding is gedaan. Uitzonderingen hierop zijn mogelijk voor zover dat uit de wet voortvloeit. De uitzonderingen op de geheimhoudingsplicht staan de instelling toe om informatie uit te wisselen met – kort gezegd – onderdelen van de eigen organisatie of het netwerk elders en/of andere instellingen die onder de reikwijdte van de Wwft of gelijkwaardig regelgeving vallen, in het kader van de doelstelling van deze wetgeving. Zonder deze uitzonderingen zouden bestaande waarschuwingssystemen tussen de financiële instellingen kunnen worden belemmerd, zoals het interbancaire waarschuwingssysteem.

Op basis van artikel 23a Wwft zijn instellingen gehouden om artikel 16 Wwft meldingen binnen de groep te delen tenzij door de FIU anders wordt bepaald.

5.9 Rechtsvorderingen en geheimhouding Wwft

Instellingen kunnen geconfronteerd worden met een vordering van het Openbaar Ministerie om cliëntinformatie te verstrekken in het kader van een strafrechtelijk onderzoek naar een cliënt (of naar derden). Voor de instelling geldt een geheimhoudingsplicht.

Een vordering kan voor de instelling aanleiding zijn om nader (verscherpt) cliëntenonderzoek in te stellen en de transacties van de cliënt extra te monitoren. De uitkomsten van het nadere cliëntenonderzoek kan voor instellingen aanleiding zijn om beheersmaatregelen treffen of ongebruikelijke transacties te melden aan de FIU, zonder de vordering te bespreken met de cliënt. Wanneer het Openbaar Ministerie vanwege het onderzoek niet wil dat de cliënt op enige wijze te weten komt dat er een onderzoek loopt, dan zal dat expliciet bij de vordering worden aangeven. Dit betekent dat indien de instelling beheersmaatregelen treft dat het onmogelijk is dat deze worden opgemerkt door de cliënt.

Een vordering van het Openbaar Ministerie hoeft voor een instelling geen aanleiding te zijn om de cliëntrelatie op basis van de Wwft of Wft te beëindigen of de dienstverlening op te schorten. Een instelling kan op basis van door haar verricht cliëntenonderzoek tot de conclusie komen dat de cliënt onacceptabele risico's met zich brengt en dat er grond bestaat om afscheid te nemen van de cliënt. Indien wel sprake is van onacceptabele risico's of indien niet kan worden voldaan aan de eisen van het cliëntenonderzoek, dient de instelling de cliëntrelatie bij de eerstvolgende mogelijkheid te verbreken.

Echter, indien het strafrechtelijk onderzoek vergt dat de cliëntrelatie en de transacties worden gecontinueerd, dan doet deze mogelijkheid zich nog niet voor. Het verzoek om de cliëntrelatie en de transacties te continueren zal door de OvJ, bij de vordering, worden gedaan.

In die situatie bieden een verscherpte monitoring van de klant en zijn transacties en een zorgvuldige vastlegging van de relevante feiten en omstandigheden in het cliëntdossier, de nodige waarborgen om de risico's het hoofd te bieden. Instellingen mogen alleen afscheid nemen van een klant op basis van de vordering wanneer het Openbaar Ministerie toestemming geeft.

Tot slot geldt dat in bovengenoemde situaties de verplichting tot het melden voor ongebruikelijke transacties door of ten behoeve van de personen waarop de vordering betrekking heeft, onverkort blijft gelden.

6 De Verordening betreffende bij geldovermakingen te voegen informatie (Wire Transfer Regulation 2)

6.1 Algemeen

De EU-Verordening bij geldovermakingen te voegen informatie, ook bekend als de Wire Transfer Regulation 2 (WTR2) bevat bepalingen ten aanzien van de traceerbaarheid van geldovermakingen om witwassen en terrorismefinanciering te voorkomen, op te sporen en te onderzoeken. De verordening verplicht instellingen informatie bij geldovermakingen te voegen en controles uit te voeren op ontvangende overmakingen, zodat informatie over de betaler en de begunstigde in de betaalketen herleidbaar blijft. DNB houdt toezicht op de onder haar toezicht staande instellingen op de nakoming van de verplichtingen die o.a. voorvloeien uit de Wwft.[64]

6.2 Achtergrond van de WTR2

Op 26 juni 2017 is de EU-Verordening (2015/847) 'betreffende bij geldovermaking te voegen informatie' in werking getreden. Deze Verordening is de opvolger van de ingetrokken Wire Transfer Regulation (WTR1, EG-Verordening nr. 1781/2006). De WTR1- en WTR2-Verordeningen hebben beiden als doel om de traceerbaarheid van informatie bij geldovermakingen te verbeteren ter ondersteuning van de voorkoming van, de opsporing van, en het onderzoek naar, het witwassen van geld en terrorismefinanciering.

De WTR1 bevatte verplichtingen over het vastleggen van informatie over de betaler bij geldovermakingen. De WTR2 breidt de verplichtingen uit ten aanzien van het vastleggen van informatie bij geldovermakingen. De kern hierbij is dat naast informatie over de betaler ook informatie over de begunstigde moeten worden vastgelegd. Deze pagina geeft een kort overzicht van de inhoud van de WTR2.

6.3 Toepassingsbereik

De WTR2 is van toepassing op geldovermakingen verzonden of ontvangen door betalingsdienstaanbieders of intermediaire betalingsdienstaanbieders in de Europese Unie (Artikel 2). Het toepassingsbereik is breed geformuleerd, maar er gelden een aantal uitzonderingen (artikel 2 WTR2). Er zijn bijvoorbeeld uitzonderingen voor krediet- of debetkaarten, geldovermakingen met elektronisch geld en geldovermakingen die via een mobiele telefoon of een ander digitaal of Informatie Technologie-toestel worden verricht.

6.4 Verplichtingen van (intermediaire) betalingsdienstaanbieders

Het tweede hoofdstuk van WTR2 heeft twee delen, waarbij één onderdeel gewijd is aan de verplichtingen van de betalingsdienstaanbieder van de betaler en het andere onderdeel aan die van de begunstigde. Kortgezegd draagt de betaaldienstverlener van de betaler zorg voor een adequate informatievastlegging. De betalingsdienstaanbieder van de begunstigde controleert of de informatie die hij ontvangt, compleet is. Welke informatie bij de

64 Artikel 1d, tweede lid, Wwft,

geldovermaking wordt vastgelegd en bijgevoegd staat omschreven in artikel 4 van de WTR2. Hierbij is van invloed of geldovermaking binnen de Europese Unie, van buiten de EU naar binnen de EU óf van binnen de EU naar buiten de EU plaatsvindt (artikel 5 en 6 van de WTR2). De intermediaire betalingsdienstaanbieder zorgt ervoor dat alle informatie over de betaler en begunstigde wordt bewaard en bijgevoegd.

6.5 Opsporen en beoordelen van onvolledige informatie

Betalingsdienstaanbieders van de begunstigde stellen procedures in om te onderzoeken en te beoordelen of de meegestuurde informatie volledig is (artikel 8). Deze procedures moeten op een risico-gebaseerde manier worden uitgevoerd. Indien geconstateerd wordt dat informatie onvolledig is, dan moet de geldovermaking opgeschort of geweigerd worden. Welke actie wordt ondernomen is afhankelijk van welke informatie ontbreekt. Ten aanzien van intermediaire betalingsdienstaanbieders gelden specifieke regels (artikel 10, 11 en 12 van de WTR2). Hierbij is van invloed of de geldovermaking binnen, vanaf of naar de Europese Unie plaatsvindt. De European Banking Authority (EBA) heeft over dit onderwerp nadere Richtsnoeren (Guidelines) uitgebracht.

6.6 EBA Richtsnoeren

Op 22 september 2017 hebben de Europese toezichthoudende autoriteiten (EBA, EIOPA en ESMA) Gemeenschappelijke Richtsnoeren (Joint Guidelines) gepubliceerd over de WTR2. Dit document bevat richtsnoeren over hoe financiële ondernemingen om dienen te gaan met ontbrekende informatie over de betaler of de begunstigde en welke procedures zij dienen in te voeren voor het omgaan met geldovermakingen waarbij informatie ontbreekt. [65]

6.7 FIU meldingen

Het ontbreken van informatie van betaler of begunstigde bij geldovermakingen kan reden zijn tot het doen van een melding van een ongebruikelijke transactie bij de Financial Intelligence Unit (FIU). Dit geldt voor zowel de betalingsdienstaanbieders als de intermediaire betalingsdienstaanbieders (artikel 9 en 13 WTR2). In de Gemeenschappelijke Richtsnoeren staan aanvullende factoren beschreven die kunnen worden meegewogen. Te denken valt aan overmakingen van en naar risicogebieden, afwijkend hoge geldbedragen en anonieme overmakingen. Zie hierbij punt 30 van de Gemeenschappelijke Richtsnoeren voor meer informatie.

65 Gemeenschappelijke richtsnoeren uit hoofde van artikel 25 van Verordening (EU) 2015/847 over de maatregelen die betalingsdienstaanbieders dienen te nemen om ontbrekende of onvolledige informatie over de betaler of de begunstigde op te sporen, en de procedures die zij dienen in te voeren voor het omgaan met geldovermakingen waarbij de vereiste informatie ontbreekt

6.8 Integriteitstoezicht Wwft

De WTR2 verplichtingen moeten gezien worden in het licht van de geldende verplichtingen ten aanzien van Wwft. Van financiële instellingen wordt verwacht dat de WTR2 verplichtingen in procedures worden opgenomen.

Gemeenschappelijke richtsnoeren – Wire Transfer Regulation 2

Zie voor een nadere uitwerking van de verordening 'de gemeenschappelijke richtsnoeren' van de European Supervisory Authorities (EBA, ESMA en EIOPA).

7 Sanctieregelgeving

7.1 Algemeen

De Leidraad van het ministerie van Financiën geeft uitgebreid informatie omtrent de sanctiemaatregelen. In aanvulling daarop worden hieronder het toezicht door DNB op de naleving van de Sanctiewet 1997 (SW) en de meldprocedure beschreven.

Met betrekking tot het financieel verkeer zijn de AFM en DNB belast met het toezicht op de naleving van de Sw. Daartoe hebben de beide toezichthouders gezamenlijk de Regeling Toezicht Sanctiewet 1977 (Rtsw) vastgesteld. Deze Regeling schrijft voor dat een instelling maatregelen treft om te controleren of relaties van de instelling voorkomen op één of meerdere sanctielijsten (zoals de EU besluiten en/of Verordeningen, besluiten van de minister van Buitenlandse Zaken op basis van de Sanctieregeling Terrorisme 2007-II – ook wel de 'Nationale Terrorismelijst' genaamd'[66] – of VN Veiligheidsraad Resoluties). In de Verordeningen van de Europese Unie en nationale sanctieregelingen zijn verschillende financiële sancties te onderscheiden:

- een gebod tot het bevriezen van tegoeden en activa van aangewezen personen of organisaties
- een verbod om rechtstreeks dan wel niet rechtstreeks middelen ter beschikking te stellen aan deze personen of organisaties
- een verbod of restricties op het verlenen van financiële diensten (t.a.v. personen, entiteiten of goederen)

Van een instelling wordt verwacht dat ze een eigen risico-inschatting maakt op basis waarvan zij maatregelen treft ter uitvoering van de sanctieregelingen. Een adequate risicoanalyse van de organisatie is daartoe noodzakelijk en dit kan vormgegeven worden binnen de systematiek van de SIRA (zie hoofdstuk 3.2).

Een instelling moet daarbij continu kunnen detecteren of haar relaties voorkomen in, dan wel of haar diensten en transacties betrekking hebben op de sanctieregelingen. Ook moet een instelling DNB daarover onverwijld (kunnen) informeren op grond van artikel 3 Regeling toezicht Sanctiewet 1977. Deze eis kan niet risicogebaseerd worden ingevuld, de instelling kan dus niet kiezen óf de sanctieregelingen nageleefd worden en afzien van het continue screenen van relaties.

Een effectief screeningsproces stelt een instelling in staat sanctieregelingen na te leven en kenmerkt zich door een frequente screening. De screeningsmomenten zijn zodanig ingericht dat instellingen continu kunnen detecteren of haar relaties voorkomen in- of haar diensten en transacties betrekking hebben op – de sanctieregelingen. Het risico op het overtreden van sanctieregelingen kan worden verkleind door te screenen bij acceptatie, bij relevante wijzigingen aan de kant van de cliënt, bij wijzigingen op de sanctielijsten en bij transacties.

66 Zie voor de Nederlandse sanctielijst van personen en organisatie met bevroren tegoeden, https://www.rijksoverheid.nl/onderwerpen/internationale-sancties/sanctiemaatregelen/landen-organisaties-en-personen-waartegen-sancties-gelden

Belangrijke screeningsmomenten

- acceptatie
- relevante wijzigingen aan de kant van de cliënt
- wijzigingen op de sanctielijsten
- transacties

7.2 Administratieve organisatie en interne controle (AO/IC)

DNB beoordeelt en handhaaft als toezichthouder de effectiviteit van de door de instellingen getroffen procedures en maatregelen die zijn gericht op de naleving van de sanctiewetgeving. Praktisch gezien kan een instelling voor het treffen van maatregelen aansluiting zoeken bij bestaande administratieve organisatie en interne controle (AO/IC) voorschriften, die voortvloeien uit andere regelgeving zoals de Wft of de Wwft. Bij het vormgeven van de AO/IC door de financiële instelling is het uitgangspunt dat zij handelt in lijn met de doelstellingen van de sanctieregelgeving. Kort gezegd, instellingen zijn in staat hun administratie zodanig te controleren dat gesanctioneerde relaties, goederen en transacties kunnen worden opgemerkt. De financiële middelen moeten direct bevroren kunnen worden en/of voorkomen moet worden dat financiële middelen en/of diensten ter beschikking worden gesteld.

Er mag geen afscheid worden genomen van een bestaande klant en in sommige gevallen kan een ontheffing bij het ministerie van Financiën aangevraagd worden. Als de instelling constateert dat de identiteit van een relatie overeenkomt met een (rechts)persoon of entiteit als bedoeld in de sanctieregelgeving (zogenaamde 'hit'[67]), dan dient de instelling dit direct aan DNB te melden. De wijze waarop een hit aan DNB gemeld moet worden is verder toegelicht in paragraaf 8.5.

DNB kijkt in haar beoordeling van de AO/IC naar o.a. de volgende elementen

- De sanctierisico's die de instelling loopt zoals vastgelegd in de SIRA
- De opzet van het sanctiebeleid, de procedures en de gedragslijnen
- De toepassing van het eigen sanctiebeleid in de cliëntendossiers
- Het screeningsproces (incl. afhandeling en vastlegging van hits)
- Training, opleiding en awareness

67 Bij controle tegen de sanctielijsten zal een instelling vele mogelijke hits tegenkomen. Deze worden allemaal gecontroleerd op overeenkomst met de diverse lijsten. Alleen daadwerkelijke hits worden gemeld. Zogenaamde 'false positives' worden niet gemeld.

7.3 Het 'relatie'-begrip

Het begrip 'relatie'

De Regeling geeft een ruime definitie van het begrip 'relatie', namelijk een ieder die betrokken is bij een financiële dienst of een financiële transactie. Hieronder vallen onder andere:

- cliënten
- vertegenwoordigers of gemachtigden
- UBO's van de cliënten
- begunstigden van een product (bijvoorbeeld bij een uitkering op een levensverzekering) of (internationale) overboeking van gelden
- wederpartij bij een financiële transactie/ product (bijvoorbeeld bij uitkering van een schadeverzekering)
- betrokkene(n) bij een financiële transactie waarbij een doelvennootschap van een trustkantoor partij is
- bestuurders van cliënten en aan cliënten gerelateerde partijen

Het begrip 'relatie' is zo ruim gedefinieerd omdat zowel het direct als het indirect ter beschikking stellen van financiële middelen of diensten onder de sanctiemaatregelen valt. In april 2013 zijn voor de "Richtsnoeren inzake de implementatie en evaluatie van de beperkende maatregelen (sancties) in het kader van het gemeenschappelijk buitenlands en veiligheidsbeleid van de EU" nieuwe elementen toegevoegd. Deze nieuwe elementen geven aan dat het beschikbaar maken van gelden aan personen of entiteiten die niet op de sanctielijsten staan, maar die onder de zeggenschap staan of eigendom zijn van personen of entiteiten die wel op de sanctielijsten staan in principe wordt beschouwd als het indirect beschikbaar maken van gelden aan de gesanctioneerde persoon of entiteit.[68]

Er is sprake van indirect ter beschikking stellen van financiële middelen of diensten in het geval dat er 50% of meer eigendomsrechten zijn van een persoon in een structuur of in het geval dat een persoon (bijvoorbeeld een bestuurder) zeggenschap heeft (waarbij zeggenschap in de Richtsnoeren zeer ruim gedefinieerd is). Wanneer de persoon met 50% of meer eigendom of de persoon met zeggenschap op een sanctielijst voorkomt, moeten ook tegoeden van de rechtspersoon bevroren worden en mogen er geen gelden naar die rechtspersoon gaan. In de praktijk kunnen instellingen ook bij eigendomspercentages onder 50% de UBO in kaart brengen. Zo is het aan te raden dat instellingen gebruik maken van de definitie van UBO in de Wwft en derhalve alle UBO's die 25% of meer eigendomsrechten hebben, kennen. Immers, het is ook verboden om tegoeden ter beschikking te stellen aan personen of entiteiten, waarover een gesanctioneerde persoon zeggenschap heeft. Voor zeggenschap is het niet nodig om 50% of meer van de aandelen in handen te hebben. Het risico bestaat dat UBO's via verschillende entiteiten binnen een structuur toch zeggenschap hebben.

68 Richtsnoeren inzake de implementatie en evaluatie van beperkende maatregelen (sancties). Te raadplegen op: https://data.consilium.europa.eu/doc/document/ST-5664-2018-INIT/nl/pdf

Voor cliënten die slechts gedeeltelijk beursgenoteerd zijn is het, in het kader van de naleving van de sanctieregelgeving, van belang dat voor het niet-beursgenoteerde gedeelte de UBO bekend te zijn.

Bij de acceptatie van een cliënt worden alle relaties vastgesteld en vastgelegd in het relatiebestand. Naast de cliënt betreft dit ook andere personen en entiteiten die bij de financiële dienst of transactie betrokken zijn, zoals de UBO('s) van de cliënt, vertegenwoordigers, bestuurders, gemachtigden en begunstigden (voor zover bekend). Aangezien de definitie van 'relatie' heel ruim is, dient een instelling bij het in kaart brengen van alle relaties te bekijken in hoeverre een bepaalde relatie eigendom of zeggenschap heeft of kan krijgen over de gelden.

Bij het identificeren worden gegevens vastgesteld zoals naam, geboortedatum, woonplaats en vestigingsadres van deze personen en entiteiten. Aan de hand van deze gegevens kan een instelling een goede controle doen. Het ontbreken van bijvoorbeeld geboortedatum of woonplaats kan het beoordelen van een hit bemoeilijken. Voor rechtspersonen kan hierbij over het algemeen worden volstaan met een check aan de gegevens zoals opgenomen in het Handelsregister bij de Kamer van Koophandel en voor natuurlijke personen met een check aan het (kopie) paspoort om zo een adequate screening aan de sanctieregelgeving mogelijk te maken.

Bij relevante wijzigingen aan de kant van de cliënt, bijvoorbeeld gewijzigde relaties of een wijziging van de UBO's, dient een instelling haar relatiebestand te actualiseren. Voor wat betreft de relaties die kwalificeren als hoog-risico (bijvoorbeeld die relaties die handelen met sanctielanden) wordt van een instelling een actievere rol verwacht bij het achterhalen van wijzigingen. Dit kan bijvoorbeeld door periodiek te informeren of er wijzigingen zijn in de relevante relaties. Het volledige relatiebestand dient vervolgens meegenomen te worden in het screeningsproces.

Eveneens wordt onderzocht of er bij de financiële dienst of transactie sprake is van een verbod of restrictie inzake bepaalde landen en gebieden en/of bepaalde goederen (embargo's). Door de instelling dient dit op toegankelijke wijze te zijn vastgelegd.

Aandacht voor strategische goederen en proliferatie.

In een aantal sanctieregimes gelden er verboden of restricties op het verlenen van financiële diensten ten behoeve van goederen. Het gaat bijvoorbeeld om militaire goederen, 'dual-use' goederen, strategische diensten (bijv. programmatuur en technologie) en goederen die gebruikt kunnen worden voor interne repressie (foltergoederen).

Meer informatie over deze goederen.

7.4 De controle van transacties

Het uitgangspunt is dat bij transacties de betrokken partijen (relaties) worden getoetst tegen de sanctielijsten. De instelling zorgt er voor dat haar AO/IC zodanig is ingericht dat ook bij betalingen verricht met behulp van derde partijen wordt voldaan aan de sanctieregelgeving.

Indien er voldoende afspraken ter naleving van de sanctieregelgeving zijn gemaakt met de derde partijen kan de instelling erop vertrouwen dat deze indien nodig gelden zullen bevriezen. De afspraken zouden onder meer moeten behelzen dat instellingen elkaar op de hoogte stellen van transacties die bevroren worden en dat buitenlandse derde partijen bij het screenen ook gebruik maken van Nederlandse sanctielijsten. De instelling zorgt ervoor dat haar AO/IC zodanig is ingericht dat ook bij betalingen aan derden wordt voldaan aan de doelstellingen van de Sanctieregelgeving.

Hoe filtert een instelling transacties tegen sanctielijsten?

Minimale informatie of velden waar tegen gecontroleerd wordt:

- opdrachtgever
- begunstigde
- plaatsnamen
- land
- omschrijving

Instellingen die actief zijn in het betalingsverkeer filteren de SWIFT MT-series en velden (inclusief de n99 berichten) en SEPA-berichten en velden die de instelling op basis van een gedocumenteerde risico-afweging heeft bepaald.

Voor trustkantoren, verzekeraars en instellingen met beperkt betalingsverkeer wordt bij uitbetaling aan begunstigden gecontroleerd of de (rechts)persoon op de sanctielijsten voorkomt.

7.5 Melden aan DNB

Bij een 'hit' meldt de instelling aan de toezichthouder:

- identificerende gegevens (naam, alias, woonplaats, geboorteplaats en -datum)
- de aard en omvang van de bevroren tegoeden of activa
- de actie ondernomen door de instelling
- de toepasselijke sanctieregeling(en)

Instellingen maken gebruik van het door de AFM en DNB opgestelde meldformat om bij een 'hit' naar DNB te versturen.[69] DNB beoordeelt de van financiële instellingen ontvangen meldingen op compleetheid. Instellingen melden de gevallen waarin er daadwerkelijk sprake is van een 'hit'. Indien een instelling twijfelt of een 'hit'-melding een daadwerkelijke 'hit' oplevert doet de instelling nader onderzoek om vast te stellen of uit te sluiten dat er sprake is van overeenkomst met de sanctielijsten.

In sommige gevallen (dit kan per sanctieregeling verschillen) zijn ontheffingen mogelijk. De minister van Financiën is bevoegd om hierover te beslissen. Een gemotiveerd verzoek tot ontheffing kan worden gericht aan het ministerie.

69 Zie ook de DNB website: http://www.toezicht.dnb.nl/2/50-221960.jsp.

Voorbeeldcasus ontheffingverlening

Een bijzondere casus is in dit geval een aansprakelijkheidsverzekering. Bijvoorbeeld, een cliënt van een verzekeraar die een aansprakelijkheidsverzekering heeft afgesloten veroorzaakt een aanrijding. Bij toekenning van de claim moet de verzekeraar betalen aan het slachtoffer/begunstigde. Indien bij controle van de sanctielijsten echter blijkt dat de begunstigde op deze lijsten voorkomt, is de verzekeraar op grond van de sanctieregelgeving gehouden de tegoeden te bevriezen terwijl op grond van andere regelgeving een verplichting tot uitbetaling kan bestaan. De instelling bevriest in een dergelijk geval de gelden en doet een melding overeenkomstig het meldformat aan DNB, die deze melding vervolgens doorzet aan de minister van Financiën. Op basis van een gemotiveerd verzoek tot ontheffing kan de minister vervolgens besluiten of een ontheffing kan worden verleend. Ook bij andere verzekeringen waar de begunstigde onbekend is, moet de verzekeraar op het moment dat een claim wordt ingediend bekijken of de sanctieregelingen van toepassing zijn.

7.6 'Hit'-meldingen, FIU-meldingen en termijnen

Van instellingen wordt verwacht dat wanneer zij op basis van een 'hit' op de sanctielijsten tegoeden bevriest, zij ook naar het transactieverleden kijken om te beoordelen of er mogelijk transacties hebben plaatsgevonden waarbij er aanleiding is om te veronderstellen dat die transacties verband kunnen houden met witwassen of financiering van terrorisme. Bij een vermoeden van witwassen of terrorismefinanciering melden instellingen dat vervolgens aan de FIU op grond van artikel 16 Wwft.

Tegoeden moeten bevroren blijven totdat de desbetreffende sanctieregeling gewijzigd wordt en de verplichting om te bevriezen ophoudt te bestaan, ontheffing wordt verleend of anderszins tegenbericht van de minister van Financiën of DNB wordt ontvangen. Indien de instelling niets verneemt, dient er van uit gegaan te worden dat het tegoed als een daadwerkelijke 'hit' moet worden beschouwd en dat het bevroren dient te blijven tot nader bericht.

Gemelde gegevens moeten worden bewaard tot 5 jaar nadat de betreffende sanctieregeling niet meer van kracht is of buiten werking is gesteld.

Aanvullende informatie

Rijksoverheid – Internationale sancties
http://www.rijksoverheid.nl/onderwerpen/internationale-sancties

Ministerie van Buitenlandse Zaken – Overzichtspagina sancties – Beperkende EU-maatregelen
https://ecer.minbuza.nl/ecer/dossiers/buitenlands-en-veiligheidsbeleid/sancties.html

DNB – Sanctiewet 1977
https://www.toezicht.dnb.nl/4/6/50-204700.jsp

DNB – Q&A Naleving Sanctiewet 1977 binnen SEPA
https://www.toezicht.dnb.nl/3/50-230317.jsp

DNB – Q&A Sanctiewet voor schadeverzekeraars
https://www.toezicht.dnb.nl/binaries/50-235745.pdf

DNB – Handreiking Sanctiewet voor Pensioenfondsen
https://www.toezicht.dnb.nl/binaries/50-235742.pdf

8 Vastlegging, bewaarplicht en de Algemene verordening gegevensbescherming (AVG)

Uit diverse wetgeving[70] volgt dat instellingen gegevens omtrent de cliënten en de transacties moeten bewaren. Het betreft alle gegevens die zijn verkregen tijdens het CDD proces, zoals kopieën van de identiteitsdocumenten, rekeninggegevens, correspondentie, gespreksnotities over en met de cliënt, transacties van en andere dienstverlening aan die cliënt. Uit het dossier blijkt ook hoe het besluitvormingsproces rond de cliëntacceptatie tot stand gekomen is, bijvoorbeeld in het geval van hoog-risico cliënten.

Bij rechtspersonen worden ook de gegevens vastgelegd van de personen die bij de instelling optreden voor de rechtspersoon. Van de UBO wordt de identiteit van de UBO en de wijze waarop deze identiteit is geverifieerd, vastgelegd. Indien een cliënt handelt als trustee legt een instelling ook op opvraagbare wijze gegevens vast van de instellers, de trustees en de UBO's. Indien een cliënt handelt als vennoot van een personenvennootschap legt een instelling gegevens vast van de vennoten, de personen die bevoegd zijn inzake het beheer van de personenvennootschap en de personen die in belangrijke mate invloed kunnen uitoefenen of belangen hebben.

Het doel van de bewaarplicht is onder andere dat de autoriteiten inzicht kunnen krijgen in de activiteiten van een cliënt, bijvoorbeeld in het geval van een (strafrechtelijk) onderzoek. De diverse dossiers en bestanden zijn dan ook goed toegankelijk voor de toezichthouder. Hierbij maakt het niet uit of de gegevens in elektronische vorm of als fysiek document worden bewaard.

In de Richtsnoeren 'Identificatie en verificatie van persoonsgegevens' van het College Bescherming Persoonsgegevens, de huidige Autoriteit Persoonsgegevens, staat opgenomen dat een financiële instelling – als bewijs van de identificatieverplichting (reconstructieplicht) – ook een kopie van het gecontroleerde identiteitsdocument kan vastleggen. Op grond van de Wwft, artikel 33, bestaat er geen verplichting om het Burgerservicenummer (BSN) vast te leggen.[71]

In de huidige Wwft is rekening gehouden met de Algemene Verordening Gegevensbescherming (AVG). Een belangrijk uitgangspunt van de AVG is de 'doelbinding', dit is uitgewerkt in artikel 34a eerste lid Wwft. Persoonsgegevens die uit hoofde van de Wwft zijn verzameld kunnen in beginsel alleen verwerkt worden in het kader van het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld, te weten de naleving van de Wwft met het oog op het voorkomen van witwassen en financieren van terrorisme.

Naast de doelbinding is in artikel 34a tweede lid Wwft bepaald dat instellingen cliënten informeren over de wettelijke verplichting voor verwerking van persoonsgegevens op grond van de Wwft. Hierbij kan gedacht worden aan het informeren van cliënten over het doel van de verwerking van de gegevens en de wettelijke bewaartermijn die geldt ten aanzien van deze gegevens.

70 Artikel 33, 34 en 34a Wwft, artikel 14 Bpr, artikel 10 Boek 2 BW, artikel 52 AWR.
71 Te raadplegen op: https://wetten.overheid.nl/BWBR0033181/2012-07-12.

De Nederlandsche Bank N.V.
Postbus 98, 1000 AB Amsterdam
020 524 91 11
dnb.nl