

Memorandum Privacy First inzake het wetsvoorstel plan van aanpak witwassen

Bijlage bij brief Privacy First aan Tweede Kamer d.d. 2 december 2022, SPF20221202.

T.a.v.:

- vaste commissie Financiën, Tweede Kamer
- vaste commissie Justitie en Veiligheid, Tweede Kamer
- vaste commissie Digitale Zaken, Tweede Kamer

Geachte Kamerleden,

Met grote zorgen heeft Stichting Privacy First kennisgenomen van het op 21 oktober 2022 ingediende voorstel *Wet plan van aanpak witwassen*¹, waarin wordt voorgesteld een aantal wijzigingen in de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) aan te brengen die grote consequenties voor de grondrechten van burgers zullen hebben. In dit memorandum zetten wij onze zorgen nader voor u uiteen.

Desgewenst zijn wij graag bereid om e.e.a. verder toe te lichten.

Hoogachtend,

Vincent Böhre
directeur Privacy First

¹ <https://www.rijksoverheid.nl/documenten/kamerstukken/2022/10/21/kamerbrief-bij-wetsvoorstel-plan-van-aanpak-witwassen>

Inhoudsopgave:

1. Inleiding - criminaliteitsbestrijding is belangrijk maar moet wel goed gebeuren	4
<i>Mislukking van witwasbestrijding door banken</i>	4
<i>Campagne gegevens delen</i>	4
<i>Te hoge verwachtingen van IT</i>	5
<i>Schade burgers, discriminatie en uitsluiting</i>	6
<i>Bancair sleepnet en andere voorstellen</i>	7
2. Ons commentaar	8
<i>2.1 Introductie</i>	8
<i>2.2 Navraagplicht</i>	9
Algemeen	10
Hoog risico is een te ruime categorie	10
Onderbouwing ontbreekt	11
Conclusie	12
Enige details	12
In artikel 3b dient een tijdsbepaling te worden opgenomen	12
Aanpassing van de reikwijdte hoort in de wet thuis (artikel 3b lid 6)	12
De cliënt en alle betrokkenen op wie de navraag betrekking heeft dienen vooraf te worden geïnformeerd over het risicoprofiel, over de gronden voor navraag en over de wijze van navraag	12
Rechtsbescherming	13
<i>2.3 Verwerking bijzondere persoonsgegevens (artikel 34a lid 1, 5 tot en met 7 Wwft)</i>	14
<i>2.4 Het bancaire sleepnet</i>	15
Algemene opmerkingen	15
Inleiding	15
Onderbouwing ontbreekt, andere Wwft-plichtigen willen hetzelfde	15
Voordeel voor de klant	15
Governance	16
Europese aanbestedingsplicht en inkoop Europese IT	16
Enige details	17
Uitzondering alleen voor consumenten	17
Risico-indicatoren en kunstmatige intelligentie: een black box	17
Risico-indicatoren	17
Hoog-risicosector	18
“afkomstig is uit een hoog-risico jurisdictie”	18
Verantwoording afleggen is nodig	19
Tot slot	19
<i>2.5 Rechtsbescherming, verantwoordingsmechanismen en toezicht</i>	20
Rechtsbescherming	20
3. Tot slot	22

<u>Bijlage 1 – Een andere inleiding over bestrijding van witwassen en terrorismefinanciering in Nederland</u>	23
<u>Groot aantal Wwft-plichtigen met verschillend karakter</u>	23
<u>Ontbrekend toezicht op gegevensverwerking</u>	23
<u>Gereguleerde sectoren</u>	24
<u>Kwaliteit gegevensverwerking</u>	24
<u>One-size-fits-all</u>	25
<u>Effectiviteit</u>	25
<u>Uitsluiting & de-risking</u>	26
<u>Rechtsbescherming</u>	27
<u>Bijlage 2 – Hoog risico volgens DNB</u>	28
<u>IRAP-formulier</u>	28
<u>Hoog risico wegens structuur of rechtsvorm (rubriek ‘Structuren*/eigenschappen doelvennootschappen’)</u>	28
<u>Hoog risico algemeen (rubriek ‘Doelvennootschappen algemeen’)</u>	29
<u>Activiteiten in hoog risico sectoren</u>	29
<u>Voorbeeld compliance dienstverlener</u>	31
<u>Bijlage 3 – Hoog risico factoren volgens Annex III bij AMLD4</u>	32
<u>(1) Customer risk factors:</u>	32
<u>(2) Product, service, transaction or delivery channel risk factors:</u>	32
<u>(3) Geographical risk factors:</u>	33

1. Inleiding - criminaliteitsbestrijding is belangrijk maar moet wel goed gebeuren

Privacy First tekent allereerst aan dat wij voorstander zijn van een krachtige bestrijding van criminaliteit.² Dat dient echter wel op een proportionele wijze te gebeuren en als daar private ondernemingen voor worden ingeschakeld, dienen dat private partijen te zijn die daar geschikt voor zijn en is essentieel dat de grondrechten van de klanten worden gerespecteerd.

Het is op dit moment pijnlijk zichtbaar dat het systeem van criminaliteitsbestrijding door private partijen ('witwasbestrijding') niet goed functioneert.

Mislukking van witwasbestrijding door banken

Uit de gang van zaken bij banken wordt duidelijk dat de privatisering van de witwasbestrijding is mislukt. Een en ander terwijl het systeem van de Wwft met cliëntenonderzoek en transactiemonitoring door de Financial Action Task Force (FATF), de internationale criminaliteitsbestrijdingswetgever, juist voor banken is ontworpen. Door middel van hoge boetes die aan banken worden opgelegd worden zij gestimuleerd de Wwft na te leven.

Hoewel werd verondersteld dat banken door middel van transactiemonitoring criminaliteit zouden kunnen ontdekken, is het systeem zeer kostbaar en ineffectief gebleken. Uit de literatuur blijkt dat de geautomatiseerde detectie van 'ongebruikelijke transacties' een zeer hoog percentage vals positieven oplevert, meer dan 95%, waaruit op een arbeidsintensieve wijze de echte ongebruikelijke transacties moeten worden gefilterd.³ De ineffectiviteit van het systeem wordt door FATF in haar publicaties erkend.

Als het de banken al niet lukt om criminaliteit te detecteren, dan is de vraag welke verwachtingen we kunnen hebben van de overige Wwft-plichtigen. De gang van zaken bij banken zou reden moeten zijn om te bekijken of het systeem van de Wwft wel klopt. Echter, dat gebeurt niet.

Campagne gegevens delen

Momenteel is een krachtige campagne inzake het delen van gegevens ten behoeve van de misdaadbestrijding aan de gang. Daaraan wordt niet alleen deelgenomen door het kabinet, dat nog steeds graag de *Wet gegevensverwerking door samenwerkingsverbanden* (WGS) door het parlement wil trekken. Ook Wwft-plichtigen, zoals de Nederlandse Vereniging van

² Witwassen en terrorismefinanciering omvatten alle criminaliteit waaruit een financieel voordeel voortvloeit, zodat het een zeer breed terrein is en iedere klant van een Wwft-plichtige onderneming geraakt kan worden.

³ Zie ook de opinie van Tjalling Tiemstra in het FD, 'Witwasbestrijding vereist wel degelijk fundamentele herziening', <https://fd.nl/opinie/1453862/witwasbestrijding-vereist-wel-degelijk-fundamentele-herziening>, 25 oktober 2022, die schrijft: "De controle van 10 miljard transacties door 12.000 bankmedewerkers, ten koste van naar schatting €1,5 mrd, leidde in 2021 tot de identificatie van slechts 0,0005% (50.000) 'verdachte transacties'. Een ruime meerderheid hiervan had een waarde van gemiddeld minder dan €1.700 per transactie."

Banken (NVB) en diverse anderen met eigen belangen bij het witwasbestrijdingssysteem⁴ zijn actief aan het campagnevoeren.

Privacy First is van mening dat de positie van de burger en de klant te weinig aandacht krijgt. Allereerst zal de vraag beantwoord moeten worden of en wanneer het gegevens delen nodig, nuttig en proportioneel is. Vervolgens zal moeten worden nagegaan hoe schade voor burgers wordt voorkomen, waarbij onder andere van belang is dat een volwaardig toezicht en goede rechtsbescherming wordt gecreëerd. In het voorstel van het kabinet ontbreekt daar aandacht voor.

Te hoge verwachtingen van IT

Kenmerkend voor de 'datagedreven' overheid, is dat men de hoop heeft gericht op het gebruik van digitale middelen en de risico's en schade onderschat. In het onderhavige wetsvoorstel komt dat tot uitdrukking, aangezien men uit is op een gedetailleerde analyse van grote hoeveelheden data van iedere Nederlander.

De aanbieders van IT-oplossingen prijzen hun oplossingen aan omdat het percentage vals positieven volgens hen verlaagd zou kunnen worden door middel van *machine learning*. Het komt er op neer dat transactiepatronen en klantengedrag diepgaand worden geanalyseerd. Daarvoor is nodig dat het systeem 'getraind' wordt met zeer grote hoeveelheden gegevens van alle klanten (zowel financiële transactiegegevens als elders digitaal te verkrijgen gegevens). De kunstmatige intelligentie ('artificial intelligence', AI) moet daarmee worden 'opgeleid'. Praktisch betekent dit een financiële surveillance van iedere burger, zoals ook in het wetsvoorstel tot uitdrukking komt.

Dergelijke financiële surveillance is riskant, zoals ook uit de literatuur blijkt. Zo schrijft Canhoto⁵ dat er geen aandacht is voor de nadelen van het gebruik van *machine learning* en AI:

Given the scale of continued expansion of customer surveillance by commercial organisations for their own strategic purposes (Zuboff, 2015), or on behalf of governments (Ball et al., 2015), the possibility of errors and associated consequences is hugely magnified. Yet, by and large, the cost of those errors are not part of the discussions or calculations of the cost and benefits of using AI. Further research could conceptualise the value of using AI in ways which not only consider the characteristics of these technologies, but also the context where they are used, and the consequences of their deployment for a broad range of stakeholders impacted by their use (Newell & Marabelli, 2015), including the possibility of discrimination and victimisation of certain groups, or the erosion of privacy.

⁴ Zoals het IFFC, <https://www.iffc.nl/>.

⁵ Zie Ana Isabel Canhoto, *Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective*, oktober 2020, <https://www.sciencedirect.com/science/article/pii/S0148296320306640>, p. 9.

Die financiële surveillance komt boven op de surveillance waar iedere burger al mee te maken heeft zoals de surveillance door advertentiebedrijven⁶ en door de geheime diensten.⁷ Daar komen nieuwe ontwikkelingen bij, zoals de analyse door aanbieders van messaging-diensten op kinderporno⁸, waardoor het communicatiegeheim bedreigd wordt en waarbij commerciële partijen gedetailleerde persoonsgegevens van hun gebruikers zullen verkrijgen. Officieel mag het niet voor andere doelen worden gebruikt, maar controle en handhaving blijven achter.

Een jaar of vijf geleden verschenen de eerste publicaties waarin werd geconstateerd dat het systeem van transactiemonitoring door individuele financiële instellingen niet functioneert en dat gewenst is dat gezamenlijk wordt geanalyseerd. Ook bij FATF landde die gedachte, wat in 2021 uitmondde in de 'High Level Roundtable for Data Pooling, Analysis and Data Protection'.⁹ In juli 2021 werd de 'Stocktake on Data Pooling, Collaborative Analytics and Data Protection'¹⁰ gepubliceerd en in juli dit jaar verscheen 'Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing'.¹¹

Voor zover ons bekend is Nederland het eerste land dat de aanbevelingen van FATF gaat uitvoeren.

Wij zijn van mening dat grote voorzichtigheid moet worden betracht met toepassingen die financiële surveillance (analyse van zeer gedetailleerde gegevens van iedere klant) met zich meebrengen, zoals hierna zal worden toegelicht.

Schade burgers, discriminatie en uitsluiting

Intussen levert de naleving van de Wwft in toenemende mate schade voor burgers op, schade die niet altijd zichtbaar is. Klachten van consumenten komen op allerlei verschillende plaatsen terecht, zoals bij de Consumentenbond, Radar of Kassa, of op security.nl. De Nederlandse Vereniging van Banken spreekt eufemistisch over 'hinder voor klanten'.¹²

Oudheidkundige Jona Lendering publiceerde in oktober 2020 een voor banken leerzaam blog onder de titel '*Verdachte transactie*'¹³, over het cliëntenonderzoek dat plaatsvond door een grootbank naar aanleiding van een betaling van een paar tientjes waarbij de vermelding stond "*nine photos of several Persia-related themes*". Het stuk geeft aan wat er mis kan gaan; het is een klein voorval en het topje van de ijsberg.

⁶ Google, Facebook, Twitter en vele anderen.

⁷ Voorstel voor de Tijdelijke Wet op Inlichtingen- en Veiligheidsdiensten 2022, zie ook <https://berthub.eu/articles/posts/uitleg-over-de-wiv-2/>.

⁸ Het EU chatcontrol voorstel, zie https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2976.

⁹ [https://www.fatf-gafi.org/publications/digitaltransformation/roundtable-data-pooling-analysis-protection.html?hf=10&b=0&s=desc\(fatf_releasedate\)](https://www.fatf-gafi.org/publications/digitaltransformation/roundtable-data-pooling-analysis-protection.html?hf=10&b=0&s=desc(fatf_releasedate))

¹⁰ [https://www.fatf-gafi.org/publications/digitaltransformation/documents/data-pooling-collaborative-analytics-data-protection.html?hf=10&b=0&s=desc\(fatf_releasedate\)](https://www.fatf-gafi.org/publications/digitaltransformation/documents/data-pooling-collaborative-analytics-data-protection.html?hf=10&b=0&s=desc(fatf_releasedate))

¹¹ [https://www.fatf-gafi.org/publications/digitaltransformation/partnering-in-the-fight-against-financial-crime.html?hf=10&b=0&s=desc\(fatf_releasedate\)](https://www.fatf-gafi.org/publications/digitaltransformation/partnering-in-the-fight-against-financial-crime.html?hf=10&b=0&s=desc(fatf_releasedate))

¹² Banken: hinder voor klanten door witwasaanpak verminderen, 26 september 2022, <https://www.nvb.nl/nieuws/banken-hinder-voor-klanten-door-witwasaanpak-verminderen/>.

¹³ <https://mainzerbeobachter.com/2020/10/23/verdachte-transactie/>

De Wwft-naleving door financiële instellingen zorgt voor zeer veel ergernis bij klanten, die door hen soms als verdachten van criminaliteit bejegend worden en onder dreiging van blokkering van de rekening informatie moeten verschaffen.¹⁴ Daarbij komt regelmatig voor dat de informatie- en bewijsleveringsverzoeken van financiële instellingen niet terecht zijn. Degenen die genoeg geld hebben kunnen procederen tegen hun bank, wat heeft geleid tot vele uitspraken. Die uitspraken geven aan hoe ernstig het probleem is. Velen kunnen zich zo'n procedure niet veroorloven en moeten het gedrag van de financiële instelling daarom slikken.

Een schadelijke ontwikkeling is dat financiële instellingen er in toenemende mate voor kiezen volledige klantgroepen uit te sluiten. Dit wordt ook wel 'de-risking' genoemd. Daar zijn inmiddels zeer veel voorbeelden van.¹⁵ Zo wordt beweerd dat de gehele non-profit sector een verhoogd risico op criminaliteit met zich mee zou brengen.¹⁶

Deze uitsluitingspraktijken zijn sterk toegenomen en zijn een gevolg van de wijze waarop overheden risicoprofilering voorschrijven aan Wwft-plichtigen.¹⁷ Zowel FATF als de Nederlandse overheid erkennen de schade die ontstaat door de witwasbestrijding, maar menen te kunnen volstaan met 'mitigating the unintended consequences'¹⁸ en weigeren te erkennen dat het systeem van witwasbestrijding niet juist is.

Bancair sleepnet en andere voorstellen

Het kabinet wenst dat een bancaire sleepnet wordt getrokken over alle financiële transacties van alle Nederlanders. Privacy First is van mening dat dit een onverstandig en ondoordacht voorstel is.

Ook de overige voorstellen zijn naar onze mening onverstandig.

¹⁴ Een voorbeeld zijn de vele klachten die bij de Consumentenbond zijn binnengekomen over Robeco. Zie het artikel 'Controle op witwassen. Banken doen aan megalomane gegevensverzameling', Geldgids oktober / november 2021.

¹⁵ Zie over defensiebedrijven <https://www.nidv.eu/nieuws/enquete-nidv-toegang-financiele-diensten-steeds-moeilijker/>.

¹⁶ Zie het overzicht van hoog-risico sectoren van DNB in bijlage 2, waarin stichtingen als hoog risico worden gekwalificeerd.

¹⁷ Zelfs FATF signaleerde dit in hun beoordeling van Nederland, die augustus 2022 is bekendgemaakt, al is jammer dat zij niet inzien dat dit een gevolg is van hun concept. Zie <https://www.rijksoverheid.nl/documenten/rapporten/2022/08/24/mutual-evaluation-report-netherlands-2022>, o.a. p. 125, waar wordt opgemerkt onder punt 5: "The Netherlands should consider the growing incidences of de-risking and ensure that AML obligations are not being used as a reason to exit particular sectors or groups."

¹⁸ Zie <https://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/unintended-consequences-project.html>.

2. Ons commentaar

2.1 Introductie

In ons commentaar bespreken wij de navolgende onderwerpen uit het voorstel:¹⁹

- [1] Het voorstel dat alle ondernemingen die op grond van de Wwft misdaad moeten opsporen en melden (Wwft-plichtigen), verplicht zijn om bij andere ondernemingen van hetzelfde type informatie inzake een toekomstige cliënt op te vragen (artikel 3b nieuw Wwft), hierna: '**de navraagplicht**'.
- [2] Verwerking **bijzondere persoonsgegevens** door alle Wwft-plichtigen (voorstel voor artikel 34a lid 1, 5 tot en met 7 Wwft).
- [3] Het voorstel dat banken samen transacties mogen monitoren (artikelen 10 en 34b nieuw Wwft), hierna: '**het bancaire sleepnet**'.

In verband met deze onderwerpen vragen wij verder uw aandacht voor:

- [4] De gebrekkige **rechtsbescherming** van klanten (consumenten en mkb) tegen het optreden van Wwft-plichtige ondernemingen en **het ontbreken van verantwoordingsmechanismen**, die gewenst zijn als overheidstaken worden geprivatiseerd.
- [5] De noodzaak van krachtige **toezichthouders** die er voor zorgen dat Wwft-plichtige ondernemingen de grondrechten van hun klanten (consumenten en mkb) respecteren bij het uitvoeren van het cliëntenonderzoek op grond van de Wwft, met inbegrip van toezicht op risicoprofilering en toezicht op *machine learning/artificial intelligence*. Deze toezichthouder dient over voldoende middelen te beschikken om onderzoeken te kunnen instellen en boetes te kunnen opleggen.

¹⁹ Beperking van contante betalingen door handelaren onderling komt niet aan de orde.

2.2 Navraagplicht

Op dit moment valt een zeer groot aantal ondernemingen onder de Wwft ('Wwft-plichtigen', door de wetgever 'instellingen' genoemd), zie ook [bijlage 1](#). Al deze ondernemingen moeten grote hoeveelheden persoonsgegevens inzake hun cliënten en aan de cliënten gerelateerde personen verwerken, met grote risico's voor de persoonlijke levenssfeer van de betrokkenen. Daarnaast is sprake van verwerking van andere vertrouwelijke gegevens, waarvoor eveneens geldt dat als die gegevens in verkeerde handen komen, er risico's zijn voor betrokkenen, organisaties of soms zelfs voor de nationale veiligheid.

In het wetsvoorstel wordt een nieuw artikel 3b Wwft voorgesteld, op grond waarvan alle Wwft-plichtigen verplicht zijn om bij 'hoog risico' op witwassen of terrorismefinanciering navraag te doen bij andere Wwft-plichtigen uit dezelfde categorie.

Dit systeem zal leiden tot nog meer gegevensbeschermingsrisico's voor burgers en is disproportioneel, omdat er zeer snel van hoog risico sprake is, zoals hierna wordt toegelicht.

Hierna stellen we het navolgende aan de orde:

- De categorie 'hoog risico' is veel te ruim.
- De noodzaak voor gegevensuitwisseling tussen alle Wwft-plichtigen is niet onderbouwd.

Daarna bespreken we nog enige details:

- Het ontbreken van een tijdsbepaling.
- Aanpassing van de reikwijdte hoort in de wet thuis.
- De cliënt en alle betrokkenen dienen vooraf over de navraag worden geïnformeerd, inclusief het vermeende risicoprofiel.
- De rechtsbescherming dient te worden verbeterd.

Algemeen

Hoog risico is een te ruime categorie

Anders dan gesuggereerd wordt in de memorie van toelichting, is er zeer snel sprake van hoog risico op witwassen en terrorismefinanciering. Volgens het voorstel is er 'hoog risico' (en moet er navraag worden gedaan) als:

- a. de zakelijke relatie of transactie naar haar aard indicaties van een hoger risico op witwassen of financieren van terrorisme met zich brengt;
- b. de risicofactoren, bedoeld in bijlage III bij de vierde anti-witwasrichtlijn, van toepassing zijn; of
- c. de instelling het cliëntenonderzoek als bedoeld in artikel 8 verricht.

Ad a. Naar de aard indicaties hoog risico

Dit is een vage omschrijving die in de praktijk zeer veel problemen zal opleveren en er toe kan leiden dat Wwft-plichtigen veiligheidshalve maar altijd navraag gaan doen. Er zijn geen algemeen bekend gemaakte en onderbouwde categorieën die aan deze kwalificatie voldoen.

De enige houvast die Wwft-plichtigen hebben, komt van de overheid, bijvoorbeeld De Nederlandsche Bank (DNB). Als bijlage 2 is een overzicht toegevoegd van categorieën die DNB als hoog risico aanmerkt. Deze hoog risico kwalificaties worden door DNB niet onderbouwd en zijn voor mensen van belang als zij betrokken zijn bij een organisatie (bijvoorbeeld als aandeelhouder of bestuurder) of als zij in bepaalde sectoren actief zijn (bijvoorbeeld de horeca). Het is een hoogst merkwaardige opsomming, waar een groot deel van het bedrijfsleven en overige organisaties tot hoog risico worden bestempeld.

Nog bonter maakt een compliance-dienstverlener het in haar overzicht van 'verhoogd risico Wwft'²⁰ waarin o.a. de hele landbouw, de hele e-commerce, alle kappers en alle toeristenwinkels tot hoog risico worden verklaard. Als het waar is, is ongeveer iedereen hoog risico.

Ad b. Risicofactoren bijlage III AMLD4

De risicofactoren van bijlage III AMLD4 zijn zeer algemeen geformuleerd, zie bijlage 3, terwijl een toelichting ontbreekt. De aanwezigheid van een risicofactor betekent echter niet dat de betreffende cliënt ook hoog risico is en ook niet dat er altijd aanvullend onderzoek moet worden ingesteld. Daartoe zou de nieuwe navraagplicht echter wel dwingen.

Ad c. Als verscherpt cliëntenonderzoek is voorgeschreven

Het verscherpte cliëntenonderzoek van artikel 8 Wwft vindt niet alleen plaats in situaties dat er daadwerkelijk hoog risico is.

²⁰ <https://www.fbn.nl/wp-content/uploads/2022/06/Visueel-overzicht-branches-met-verhoogd-risico-1-juni-2022.pdf>

Met name het cliëntenonderzoek naar politiek prominente personen ('PEP's')²¹ omvat een grote groep personen die in het geheel geen hoog risico zijn. Ten eerste is hoogst twijfelachtig dat er een verhoogd risico aanwezig is bij alle personen die in Nederland PEP zijn (binnenlandse PEP's), zoals leden van de Tweede Kamer en de Eerste Kamer (de 'primaire PEP's'). Nog erger wordt het dat ook ouders, kinderen en levenspartner, alsmede 'personen bekend als naaste geassocieerde'²² van de binnenlandse PEP's geacht worden hoog risico te zijn. Het begrip 'naaste geassocieerde' is zeer ruim, zo leidt de aanwezigheid van een primaire PEP in een bestuur van een stichting ertoe dat alle mede-bestuurders zelf ook 'PEP' zijn geworden en dus een hoog risico op witwassen en terrorismefinanciering zouden zijn.

Wij zijn van mening dat de PEP-definitie veel te ruim is en dat ook andere vermeende hoog risico situaties in werkelijkheid geen hoog risico hoeven te zijn.

Als er een navraagplicht zou komen, is ongewenst dat het begrip 'hoog risico' zo ruim is als thans omschreven.

Onderbouwing ontbreekt

Voorts ontbreekt in de memorie van toelichting een analyse die de noodzaak voor gegevensuitwisseling tussen alle Wwft-plichtigen onderbouwt. Voor een deel van de Wwft-plichtigen uit het mkb is het voor een groot deel van hen al moeilijk om überhaupt te begrijpen wat er van hen verlangd wordt en om de Wwft op een zorgvuldige en veilige wijze na te leven. De navraagplicht maakt dit nog lastiger. Daarbij speelt ook een rol dat een deel van de Wwft-plichtigen niet is gereguleerd en dat er een gebrekkige rechtsbescherming is als er iets mis gaat.

Wij kunnen ons voorstellen dat een navraagplicht of een alternatief nuttig is voor specifieke sectoren, waarbij te denken valt aan banken (omdat zij veel transacties zien) en notarissen (omdat zij aandelen- en vastgoedtransacties verzorgen). Maar ook bij notarissen is de vraag of een navraagplicht wel praktisch uitvoerbaar is.²³

Er zijn diverse alternatieven denkbaar. Zo kan ten aanzien van het notariaat worden gedacht aan een mogelijkheid om personen te verifiëren via Dienst Justis (met een nee/ja systeem). Uit de memorie van toelichting blijkt niet dat alternatieven zijn onderzocht.

²¹ Zie voor de definitie

<https://wetten.overheid.nl/jci1.3:c:BWBR0041193¶graaf=2&artikel=2&z=2021-04-01&g=2021-04-01>. Een overzicht van functies is op https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/brochures_en_publicaties/wwft-prominente-publieke-functies te vinden.

²² Lees over naaste geassocieerden: <https://ellentimmer.com/2021/12/30/wwft-601/>.

²³ Zoals door Henry Pot op LinkedIn wordt signaleerd, "Ik begrijp waar ze naar toe willen. Maar praktisch haalbaar? (...) Een cliënt zal niet zo snel aangeven dat hij bij (bijvoorbeeld) een notaris niet geaccepteerd is om compliance technische redenen. Om dit risico te mitigeren zou de notaris zijn ongeveer 1200 collega notarissen moeten contacteren om te kijken of de potentiële cliënt al bij die notaris geprobeerd heeft een zakelijke relatie aan te gaan".

Conclusie

Privacy First is van mening dat de noodzaak van de navraagplicht niet is onderbouwd. Als die onderbouwing er zou komen, vinden wij dat pas een navraagplicht in de Wwft kan worden opgenomen als:

- is nagegaan of er **alternatieven** zijn die minder belastend zijn voor de klanten en die minder risico's voor de gegevensbescherming opleveren;
- is nagegaan voor welke Wwft-plichtigen dit daadwerkelijk **noodzakelijk** is;
- de navraagplicht wordt beperkt tot **specifiek aangewezen risico's**;
- aangetoond wordt dat **de burger er op vooruit** gaat door de invoering van deze maatregel.

Enige details

Voorts hebben we nog een aantal andere opmerkingen, die hierna volgen.

In artikel 3b dient een tijdsbepaling te worden opgenomen.

Het is niet afdoende dat in de memorie van toelichting wordt verwezen naar de bewaartermijn van de Wwft (vijf jaar na het beëindigen van de dienstverlening) aangezien een deel van de Wwft-plichtigen (onder meer in de financiële sector) doorlopende diensten verricht. Dit zou betekenen dat in sommige gevallen gegevens van twintig jaar geleden moeten worden opgediept.

In het kader van de dataminimalisatie dient in artikel 3b een tijdsbepaling te worden opgenomen, bijvoorbeeld in de zin dat er alleen wordt gevraagd naar informatie van maximaal vijf jaar geleden.

Aanpassing van de reikwijdte hoort in de wet thuis (artikel 3b lid 6).

In artikel 3b lid 6 wordt nu voorgesteld dat bij algemene maatregel van bestuur de navraagplicht kan worden beperkt respectievelijk uitgebreid. Vanwege de grote consequenties voor de grondrechten, hoort dit onderwerp in de wet thuis en niet in een algemene maatregel van bestuur.

De cliënt en alle betrokkenen op wie de navraag betrekking heeft dienen vooraf te worden geïnformeerd over het risicoprofiel, over de gronden voor navraag en over de wijze van navraag.

Op dit moment hoeven overheidstoezichthouders en Wwft-plichtigen geen verantwoording af te leggen over het risicoprofiel dat aan cliënten wordt toegekend. Het is dringend nodig dat die verantwoording wel wordt afgelegd, zodat betrokkenen weten waar zij aan toe zijn en zij commentaar kunnen leveren en verweer kunnen voeren.

Voorts laten Wwft-plichtigen meestal na om de betrokkenen²⁴ te informeren over de persoonsgegevens die zij verwerken in het cliëntenonderzoek dat zij doen als de cliënt geen natuurlijke persoon is²⁵, terwijl dat wel door artikel 14 AVG wordt voorgeschreven.

Voorbeeld: als cliëntenonderzoek naar een besloten vennootschap wordt gedaan kunnen de betrokkenen zijn:

- de statutair bestuurders;
- de natuurlijke personen die aandelen of certificaten in de bv houden ('uiteindelijk belanghebbenden');
- andere personen betrokken bij de bv (vooral relevant voor sanctieregelgeving).

In de praktijk krijgen deze mensen niet te horen dat er onderzoek naar hen is gedaan en op welke manier (bijvoorbeeld welke handelaren in persoonsgegevens²⁶ zijn geraadpleegd). Hoewel handelaren in persoonsgegevens (datahandelaren) de betrokkenen over de verwerking dienen te informeren, gebeurt dat in de praktijk niet. Ter voorkoming van fouten is het essentieel dat betrokkenen zowel door Wwft-plichtigen als door datahandelaren over de verwerking worden geïnformeerd en dat op naleving van deze verplichting wordt gehandhaafd.

Als de navraagplicht door zou gaan, vinden wij dat expliciet in de Wwft moet worden opgenomen:

- [i] dat de cliënt en alle betrokkenen vooraf over het vermeende risicoprofiel dienen te worden geïnformeerd, waarbij de Wwft-plichtige zorgt voor een adequate onderbouwing;
- [ii] dat de cliënt en de betrokkenen door de Wwft-plichtige in staat worden gesteld om commentaar te leveren op het vermeende risicoprofiel;
- [iii] dat de cliënt en alle betrokkenen vooraf moeten worden geïnformeerd bij wie navraag wordt gedaan.

Het is belangrijk dat hier sprake is van transparantie en dat de Wwft-plichtige verantwoording aflegt. Voorts is verbetering van de rechtsbescherming gewenst, zie hierna.

Rechtsbescherming.

Bij ingrijpende bevoegdheden zoals de navraagplicht hoort een volwassen rechtsbescherming. Die is er nu niet, wat er toe leidt dat alleen degenen die het kunnen betalen hun 'recht' kunnen halen bij de onafhankelijke rechter. Zie voor onze voorstellen hierna onder 'rechtsbescherming'.

²⁴ 'Betrokkenen' in de zin van de AVG.

²⁵ Opvallend is dat in de memorie van toelichting zorgvuldig om deze verplichting 'heen' wordt geschreven.

²⁶ Er zijn diverse gespecialiseerde handelaren in persoonsgegevens ten behoeve van de criminaliteitsbestrijding, voorbeelden zijn WorldCheck en Experian.

2.3 Verwerking bijzondere persoonsgegevens (artikel 34a lid 1, 5 tot en met 7 Wwft)

Het tekstvoorstel voor artikel 34a lid 1, 5 tot en met 7 Wwft is relevant voor alle Wwft-plichtigen. Zoals al in bijlage 1 bij dit memorandum is uiteengezet, zijn er vele soorten Wwft-plichtigen en is niet gegarandeerd dat iedereen de gegevensbeschermingsverplichtingen goed kan/zal naleven.

Privacy First acht het ongewenst dat alle soorten Wwft-plichtigen in staat worden gesteld bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard te verwerken, zoals nu voor artikel 34a lid 1 Wwft wordt voorgesteld, zeker nu een behoorlijke rechtsbescherming van betrokkenen tegen het optreden van de Wwft-plichtige ontbreekt en de Autoriteit Persoonsgegevens geen capaciteit of middelen heeft om toezicht uit te oefenen.

Wij stellen voor dat specifieke sectoren worden aangewezen en dat wordt gezorgd voor goede rechtsbescherming.

Verder is belangrijk dat in de memorie van toelichting wordt verduidelijkt dat het informeren van de cliënt over de verwerking van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard (artikel 34a lid 6 Wwft) onverlet laat dat betrokkenen op grond van artikelen 13/14 AVG eveneens door de Wwft-plichtige worden geïnformeerd. Nu wordt in de memorie van toelichting gesuggereerd dat met het informeren van de cliënt kan worden volstaan.

Voorts achten wij het ongewenst dat gegevensbeschermingsregels in relatie tot artikel 34a lid 1 nieuw kunnen worden ingesteld bij of krachtens een algemene maatregel van bestuur (amvb), zoals wordt voorgesteld in de tekst voor artikel 34b lid 7 nieuw Wwft. Het risico is aanwezig dat via een amvb afbreuk wordt gedaan aan de gegevensbescherming waarop betrokkenen recht hebben. Vanwege de grote impact op de gegevensbescherming van burgers van artikel 34b lid 1 Wwft nieuw, horen die bepalingen bij wet te worden gegeven, door middel van de Uitvoeringswet Algemene verordening gegevensbescherming.

2.4 Het bancaire sleepnet

Algemene opmerkingen

Inleiding

In de inleiding heeft Privacy First al geconstateerd dat het systeem van de Wwft is mislukt, wat zichtbaar is aan de gang van zaken bij banken, voor wie het systeem is ontworpen en die onder dreiging van hoge boetes tot naleving worden bewogen. In de literatuur is al eerder geconstateerd dat de individuele transactiemonitoring door banken weinig oplevert en zeer veel geld kost.

De kosten worden op dit moment aan alle klanten van banken doorberekend, terwijl de banken geen verantwoording verschuldigd zijn over de wijze waarop zij de overheidstaak op grond van de Wwft uitvoeren en de rechtsbescherming onvoldoende is. Op de rechtsbescherming gaan wij hierna afzonderlijk in.

Onderbouwing ontbreekt, andere Wwft-plichtigen willen hetzelfde

Dit voorstel vinden wij onacceptabel, in de eerste plaats omdat niet wordt onderbouwd dat het gezamenlijk monitoren tot betere resultaten zou leiden dan het individueel monitoren. Voorts zijn wij van mening dat de gezamenlijke monitoring een ernstige inbreuk op de persoonlijke levenssfeer maakt van Nederlandse inwoners.

Dat banken zo graag samen willen monitoren geeft ook aan dat het concept van de witwasbestrijding niet klopt. Het kabinet beweert steeds dat banken (en andere Wwft-plichtigen) in zo'n goede positie zouden verkeren om misdaad te voorkomen en te detecteren. Dat blijkt niet waar te zijn bij banken en geldt waarschijnlijk ook voor andere Wwft-plichtigen. Er zijn al signalen dat andere Wwft-plichtigen (bijvoorbeeld notarissen) het voorbeeld van de banken willen volgen en ook gezamenlijk willen monitoren of gegevens uitwisselen.

Nu al is gevaarlijk dat banken zich als een pseudo-overheid gaan gedragen, terwijl zij geen verantwoording hoeven af te leggen over hun optreden, bijvoorbeeld over de informatie die zij van klanten verlangen en over de enorme tariefsverhogingen die zij vanwege de witwasbestrijding hebben doorgevoerd bij alle klanten.

Wij zijn van mening dat onvoldoende is gekeken naar alternatieven voor het bancaire sleepnet. Er bestaan op allerlei terreinen digitale registratiesystemen, die een rol kunnen spelen in het detecteren van criminaliteit. Een voorbeeld zijn de digitale systemen op het gebied van transport van producten. Er wordt te eenzijdig gefocust op het betalingssysteem.

Voorts is van belang dat criminaliteit wordt bestreden aan de bron en niet aan het einde van de keten (bij de betaling).

Voordeel voor de klant

Als Nederland al zou willen kiezen voor het bancaire sleepnet, zoals nu wordt voorgesteld, is dat alleen acceptabel als de effectiviteit groot is en de risico's, lasten en nadelen die de witwasbestrijding nu voor burgers opleveren afnemen. Verder is essentieel dat een en ander zorgvuldig is vormgegeven en een volwassen rechtsbescherming wordt opgetuigd, zodat Wwft-plichtigen worden gestimuleerd tot maatschappelijk betamelijk gedrag.

Governance

Bij die zorgvuldige vormgeving hoort dat wordt nagegaan welke juridische positie de entiteit inneemt die de transactiemonitoring uitvoert. Wij achten het ongewenst dat die entiteit een deelneming is van financiële instellingen, zoals nu met Transactie Monitoring Nederland BV (TMNL) het geval is.

Als er al zo'n entiteit komt, zijn wij van mening dat deze entiteit zo moet worden ingericht dat de belangen van de klanten (met name consumenten en mkb) van de financiële instellingen worden behartigd en hun grondrechten (inclusief gegevensbeschermingsrechten) worden gerespecteerd. Dit hoort te betekenen dat de entiteit geen deelneming dient te zijn van de financiële instellingen wier transacties worden geanalyseerd en dat de entiteit wordt geleid door mensen met kennis van grondrechtenproblematiek in de IT en van gegevensbeschermende techniek.

Het zou een zelfstandige privaatrechtelijke entiteit kunnen zijn, waarop de Wet Normering Topinkomens (WNT) van toepassing is.²⁷

Europese aanbestedingsplicht en inkoop Europese IT

De entiteit die het bancaire sleepnet uitvoert (ongeacht of het TMNL is of een andere entiteit) is een publiekrechtelijke instelling in de zin van de Aanbestedingswet 2012²⁸ aangezien zij ten doel heeft te voorzien in behoeften van algemeen belang, anders dan van industriële of commerciële aard en het beheer van de entiteit is onderworpen aan toezicht door de Nederlandse staat.²⁹

Dat betekent dat de entiteit Europees moet aanbesteden, waarbij het ons verstandig lijkt om – gelet op de veiligheidsbelangen en het bevorderen van digitale onafhankelijkheid van Europa – voor te schrijven dat uitsluitend Europese producten mogen worden ingekocht. Daarmee kan beter worden gewaarborgd dat de Europese beginselen van gegevensbescherming en mensenrechten worden nageleefd.

²⁷ Wij blijven het overigens bijzonder vinden dat op topfunctionarissen van DNB de WNT-norm niet van toepassing is.

²⁸ Artikel 1.1 Aanbestedingswet 2012.

²⁹ Voor aanbestedingsplicht is niet relevant dat een entiteit privaat is gefinancierd, zie de uitspraak van het Hof van Justitie van de Europese Unie van 3 februari 2021 inzake de Italiaanse voetbalbond, zaken C-155/19 en C-156/19.

Enige details

Wij hebben principiële bezwaren tegen het bancaire sleepnet. Zonder die bezwaren prijs te geven hebben we ook opmerkingen bij enige details van het voorstel.

Uitzondering alleen voor consumenten

In artikel 34b staat een beperkte uitzondering voor consumenten. Volgens lid 4 van het voorgestelde artikel worden transacties onder € 100 tussen consumenten (privérekeningen) niet gecombineerd in het bancaire sleepnet. Transacties onder € 100 tussen een privé-rekening en een zakelijke rekening worden wel via het bancaire sleepnet geanalyseerd maar met een beperkte set van gegevens inzake de consument.³⁰

Natuurlijke personen die zakelijk handelen, bijvoorbeeld als eenmanszaak of als vennoot van een personenvennootschap, vallen volledig met alle transacties onder het bancaire sleepnet, terwijl ook zij gegevensbeschermingsrechten hebben op grond van de AVG.

Het is verder hoogst merkwaardig dat de consumentenuitzondering alleen geldt voor transacties tot € 100. In de praktijk zal dit betekenen dat een groot deel van de consumententransacties mee gaan in het bancaire surveillance systeem en dat via het bancaire sleepnet een gedetailleerd beeld van iedere rekeninghouder kan ontstaan.

Wij zijn van mening dat alle consumententransacties onder een hoge (nader te bepalen) drempel buiten het bancaire sleepnet dienen te blijven en dat er beneden deze drempel ook geen gegevens horen te worden meegestuurd (anders dan in lid 4 sub b. voorgesteld).

Risico-indicatoren en kunstmatige intelligentie: een black box

Op grond van artikel 34b lid 3 sub d. kan bij algemene maatregel van bestuur worden vastgesteld dat door de bank “reeds vastgestelde risico-indicatoren” mogen worden verwerkt in het kader van de gezamenlijke transactiemonitoring. Uit lid 6 van artikel 34b blijkt dat geen sprake is van geautomatiseerde besluitvorming en dat bij de geautomatiseerde gegevensanalyse geen algoritmes worden gehanteerd waarvan de uitkomsten niet navolgbaar en controleerbaar zijn.

Hier spreekt een ongerechtvaardigd geloof in de techniek uit. Als dit systeem door zou gaan (wat we niet hopen) dienen er veel hogere eisen aan te worden gesteld.

Overigens is er wel degelijk sprake van geautomatiseerde besluitvorming, aangezien het systeem vermeende criminaliteitssignalen zal selecteren en aan de individuele banken zal sturen, die vervolgens na een vooronderzoek hun cliënten zullen benaderen met vragen. Dat betekent overlast (en soms kosten) voor die cliënten als de signalen ten onrechte geselecteerd blijken te zijn.

Risico-indicatoren

De risico-indicatoren van artikel 34b lid 3 sub d. worden vrijwel niet toegelicht in de memorie van toelichting. Er wordt in vage termen gesproken over “door de instelling reeds vastgestelde risico-indicatoren” en over “reeds geïdentificeerde risico’s”. Hier dient nadere informatie over te worden verschaft. Wat is de kwaliteit van de huidige risico-indicatoren en zijn deze onafhankelijk getoetst?

³⁰ Alleen het IBAN-nummer, het BIC-nummer en de landencode.

De ervaringen met SyRI en de toeslagenaffaire hebben ons geleerd dat het vaststellen van risico's en het maken van een risicoprofiel gecompliceerd is en snel leidt tot onjuiste conclusies. Wij zijn er niet van overtuigd dat het huidige systeem in de witwasbestrijding goed werkt en vragen ons af of het niveau van degenen die bij de overheid en bij de banken met het onderwerp bezig zijn wel hoog genoeg is om tot goede analyses te komen.³¹

Wij zijn van mening dat het systeem van risico-indicatoren en vaststelling van risicoprofielen van klanten in de witwasbestrijding getoetst moet worden door onafhankelijke deskundigen zonder belangen in de financiële sector of de criminaliteitsbestrijding.³² Onze indruk is dat de wijze waarop wordt omgegaan met vermeende risico's onvoldoende kwaliteit heeft, met als gevolg dat klanten van Wwft-plichtigen onnodig worden lastig gevallen.

In het kader van de navraagplicht maakten wij al de opmerking dat wat de regelgever als 'hoog risico' beschouwt zeer vaag en ruim is, zodat de kans zeer groot is dat nette burgers in de ogen van financiële instellingen hoog risico zijn.

Ook de memorie van toelichting geeft daar blijk van, waar wordt opgemerkt:

Teneinde hieraan tegemoet te komen, kunnen deze risico-indicatoren bij algemene maatregel van bestuur vastgesteld worden. Deze indicatoren dienen generiek te worden omschreven en niet herleidbaar te zijn tot personen. Voorbeelden hiervan zijn indicatoren dat een cliënt actief is een bepaalde hoog-risicosector, afkomstig is uit een hoog-risico jurisdictie of onderdeel uitmaakt van een ondoorzichtige bedrijfsstructuur.

Hoog-risicosector

Er wordt gesproken over een 'hoog-risicosector': wie bepaalt dat? Is, zoals DNB meent, zie bijlage 2, sprake van hoog risico bij iedere:

- adviseur
- restauranteigenaar
- autohandelaar
- transporteur
- aannemer

(en blijven er dan nog organisaties en personen over die geen hoog risico zijn)?

Het is hoog tijd dat de overheid en financiële instellingen verantwoording gaan afleggen over de manier waarop zij burgers, organisaties en bedrijven 'profilieren'.

"afkomstig is uit een hoog-risico jurisdictie"

Betekent dit dat iedereen die in Iran is geboren hoog risico is? Wij denken dat dit een ongerechtvaardigd onderscheid naar geboorteplaats (mogelijk ook naar nationaliteit is).

³¹ Zie bij de overheid bijvoorbeeld het AMLC artikel 'Misbruik van rechtsvormen' <https://www.amlc.nl/misbruik-van-rechtsvormen/> dat vol staat met fouten, die worden besproken in <https://ellentimmer.com/2022/10/13/wwft-736/>.

³² Ook bepaalde wetenschappers die regelmatig overheidsopdrachten op het gebied van de witwasbestrijding uitvoeren, vallen in deze categorie.

Verantwoording afleggen is nodig

Wij zijn van mening dat overheid en financiële instellingen verantwoording behoren af te leggen over de wijze waarop zij omgaan met risico-indicatoren in risicoprofilering. Dat betekent dat aan een vaststelling van de risico-indicatoren die door de sleepnet entiteit gehanteerd mogen worden, een grondige onafhankelijke analyse vooraf dient te gaan.

Datzelfde geldt voor de algoritmen die worden gebruikt bij de geautomatiseerde gegevensanalyse (artikel 34b lid 6 sub c.). Als het sleepnet er komt, dient de sleepnet entiteit aan het publiek en aan een gespecialiseerde overheidstoezichthouder (niet DNB) verantwoording af te leggen over de wijze waarop de gegevensanalyse plaatsvindt.

Verder is essentieel dat in het systeem (danwel in het systeem van de bank die dat teruglevert aan de sleepnet entiteit) wordt ingebouwd dat de hinder en overlast voor de klanten worden vastgesteld en in de analyse meegenomen.³³ Bijvoorbeeld dat aan de klanten om nadere informatie is gevraagd, of en in welke mate dit overlast heeft veroorzaakt (bijvoorbeeld doordat de klant kosten moest maken of doordat onnodige inbreuk op de privésfeer heeft plaatsgevonden). Zoals de financiële transacties worden gemonitord, moet ook de schade die het systeem oplevert worden gemonitord. Daarom is een volwassen governance essentieel.

Tot slot

In dit onderdeel is de rechtsbescherming van de burger nog niet aan de orde gekomen. Daar gaan we in 2.5 op in.

Wij zijn van mening dat het huidige sleepnet voorstel grote risico's voor alle Nederlanders met zich meebrengt en dat een volwassen governance ontbreekt. Het voorstel in deze vorm mag niet doorgaan. Of een gewijzigd voorstel acceptabel is, zal volledig van de onderbouwing afhangen en van de inrichting van het systeem.

³³ Zie Canhoto over het ontbreken van belangstelling voor de klant en de bij de klant betrokkenen die worden onderzocht: *“Given the scale of continued expansion of customer surveillance by commercial organisations for their own strategic purposes ([Zuboff, 2015](#)), or on behalf of governments ([Ball et al., 2015](#)), the possibility of errors and associated consequences is hugely magnified. Yet, by and large, the cost of those errors are not part of the discussions or calculations of the cost and benefits of using AI.”*

2.5 Rechtsbescherming, verantwoordingsmechanismen en toezicht

Op dit moment ontbreekt een volwassen rechtsbescherming tegen optreden van overheid en Wwft-plichtigen op het gebied van de bestrijding van criminaliteit (inclusief terrorisme-financiering). Die noodzaak is er zowel voor wat betreft de navraagplicht als met betrekking tot het bancaire sleepnet.

Als het bancaire sleepnet er zou komen is essentieel dat er een correcte governance is, de Europese aanbestedingsregels worden nageleefd, er uitsluitend van Europese IT gebruik wordt gemaakt, er een verantwoordingsmechanisme wordt gecreëerd en er streng toezicht wordt uitgeoefend door een toezichthouder die oog heeft voor de belangen van de burger. Daarop is hiervoor al ingegaan.

Bij ingrijpende bevoegdheden van Wwft-plichtigen hoort een volwassen onafhankelijke rechtsbescherming, die er voor kan zorgen dat Wwft-plichtigen schadelijk gedrag achterwege laten.

Rechtsbescherming

Privacy First denkt aan het volgende:

- [i] de Wwft-plichtige informeert de cliënt en de betrokkenen over het toegekende risicoprofiel en voor zover van toepassing over het navraagvoornemen en stelt hen in de gelegenheid commentaar te geven;
- [ii] als de Wwft-plichtige de cliënt om informatie en/of bewijs in verband met het cliëntenonderzoek verzoekt, licht de Wwft-plichtige op verzoek toe waarom het verzoek redelijk en proportioneel is;
- [iii] als de cliënt en/of een betrokkene het niet eens zijn met de Wwft-plichtige, kunnen zij op een laagdrempelige manier het geschil aan een **onafhankelijke rechter** (bijvoorbeeld een kantonrechter) voorleggen;
- [iv] de cliënt en de betrokkene kunnen zich wenden tot een nieuw te creëren **financiële ombudsman** die ook bevoegdheden zal krijgen als het om de witwasbestrijding door anderen dan financiële instellingen gaat. Die ombudsman dient een onafhankelijke positie te krijgen, vergelijkbaar met de Nationale Ombudsman voor de overheid.

Ad [iii] Onafhankelijke rechter

Hierbij kan worden aangetekend dat het Kifid niet de onafhankelijkheid en de kwaliteit heeft om goed voor de belangen van burgers op te komen, zoals ook zaken uit het verleden hebben geleerd, zoals ernstige mislag in de zaak over de Accidental American die door de geschillencommissie van Kifid werd veroordeeld voor valsheid in geschrifte³⁴. Niet voor niets dringt lid van de Tweede Kamer Alkaya aan op wijzigingen bij Kifid³⁵, maar wij denken dat herziening van Kifid niet voldoende is.

³⁴ Zie de uitspraak van 27 mei 2019, <https://www.kifid.nl/wp-content/uploads/2020/07/Uitspraak-2020-630.pdf>. Het oordeel over valsheid in geschrifte werd door de kort geding rechter van tafel geveegd, zie ECLI:NL:RBMNE:2020:5647. De bodemrechter kwam in een daarna gevolgde procedure ook voor het overige tot een ander oordeel, zie <https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Midden-Nederland/Nieuws/Paginas/Volksbank-mag-rekeningen-onbedoelde-Amerikaan-niet-sluiten.aspx>.

³⁵ Zie dossier 35727, <https://zoek.officielebekendmakingen.nl/dossier/35727>.

Het is van belang dat de rechtsbescherming inzake de witwasbestrijding wordt geconcentreerd bij een laagdrempelige gespecialiseerde onafhankelijke rechter, die bevoegd is bij geschillen met financiële instellingen en alle overige Wwft-plichtigen. Dit biedt meteen de gelegenheid om daar ook alle andere voor burgers belangrijke geschillen met financiële instellingen te concentreren, bijvoorbeeld over kredietregistratie (BKR), plaatsing op zwarte lijsten en klachten over onzorgvuldig optreden van financiële instellingen.

Voors is van belang dat deze rechtsbescherming zowel voor consumenten als voor eenmanszaken en het mkb geldt. Ook bij organisaties betrokken natuurlijke personen (bijvoorbeeld de uiteindelijk belanghebbende of bestuurder)³⁶ dienen op die onafhankelijke rechter een beroep te kunnen doen.

Ad [iv] Financiële ombudsman

De financiële sector en de witwasbestrijding spelen een belangrijke rol in het leven van burgers. In de verhouding tussen financiële instellingen en de burger gaat het nodige mis. Op dit moment is er geen onafhankelijke overheidsinstantie die signalen kan oppakken op de manier dat de Nationale Ombudsman het op dit moment bij de overheid doet.

Wij zijn van mening dat zo'n ombudsman dringend nodig is, vanwege de belangrijke beslissingen die financiële instellingen en Wwft-plichtigen nemen, bijvoorbeeld over kredietregistratie (BKR), plaatsing op de zwarte lijst en het cliëntenonderzoek op grond van de Wwft. De bejegening van klanten is niet altijd correct. Een financiële ombudsman kan signalen in ontvangst nemen en naar aanleiding daarvan onderzoek doen en bevindingen openbaar maken.

³⁶ Dat is van belang omdat het voorkomt dat een bank een bestuurder van een rechtspersoon op de zwarte lijst zet, omdat de bank van mening is dat die bestuurder verantwoordelijk is voor het niet-nakomen door de rechtspersoon van verplichtingen in verband met het cliëntenonderzoek op grond van de Wwft.

3. Tot slot

Onder verwijzing naar het voorgaande verzoekt Privacy First u om er bij het kabinet op aan te dringen het wetsvoorstel in te trekken en met een ander voorstel te komen.

Bijlage 1 – Een andere inleiding over bestrijding van witwassen en terrorismefinanciering in Nederland

Sinds 1 februari 1994 zijn financiële instellingen verplicht om cliëntenonderzoek te doen, transacties te monitoren en vermoedens van criminaliteit te melden bij de overheid (melding van ' ongebruikelijke transacties', tegenwoordig bij FIU-Nederland).³⁷ Na 1994 is de regelgeving regelmatig gewijzigd en is de Wwft tot stand gekomen. Voorts is de reikwijdte van de Wwft sterk uitgebreid.³⁸

Nederland heeft de Wet MOT / Wid en later de Wwft ingevoerd op grond van Europese verplichtingen.

Kenmerkend voor de Wwft is het dubbele werk: alle Wwft-plichtigen die een relatie met dezelfde cliënt hebben, moeten hetzelfde cliëntenonderzoek doen. Dat maakt de Wwft een zeer kostbare wet, terwijl niet is gebleken dat het cliëntenonderzoek het beoogde effect oplevert.

Groot aantal Wwft-plichtigen met verschillend karakter

Op dit moment valt een zeer groot aantal ondernemingen onder de Wwft ('Wwft-plichtigen', door de wetgever 'instellingen' genoemd). Al deze ondernemingen moeten grote hoeveelheden persoonsgegevens inzake hun cliënten en aan de cliënten gerelateerde personen verwerken, met grote risico's voor de persoonlijke levenssfeer van de betrokkenen. Daarnaast is sprake van verwerking van andere vertrouwelijke gegevens, waarvoor eveneens geldt dat als die gegevens in verkeerde handen komen, er risico's zijn voor betrokkenen, organisaties of soms zelfs voor de nationale veiligheid.

Ontbrekend toezicht op gegevensverwerking

Daarbij valt op dat de Wwft-plichtigen maar voor een beperkt deel vallen onder gereuleerde ondernemingen met een vorm van integriteitstoezicht. Hoewel het in veel parlementaire stukken lijkt alsof alleen banken en andere financiële instellingen³⁹ zich aan de Wwft moeten houden, geldt de Wwft ook voor een grote groep niet-gereuleerde ondernemingen/ organisaties, die voor een belangrijk deel tot het midden- en kleinbedrijf behoren.

Dit betreft:

- safeloket aanbieders;⁴⁰
- leasemaatschappijen en andere aangewezen ondernemingen;⁴¹

³⁷ Destijds gebaseerd op de Wet melding ongebruikelijke transacties (Wet MOT) en de Wet identificatie bij dienstverlening (Wid).

³⁸ De huidige groep ondernemingen is te vinden in artikel 1a Wwft.

³⁹ Zie artikel 1a lid 2 en 3 Wwft, waarin de financiële ondernemingen worden opgesomd.

⁴⁰ Artikel 1a lid 3 sub a. Wwft.

⁴¹ Artikel 1a lid 3 sub a. Wwft, daarin wordt gesproken over ondernemingen die werkzaamheden verrichten die zijn opgenomen onder de punten 2, 3, 5, 6, 9, 10, 12 en 14 van bijlage I bij de richtlijn kapitaalvereisten.

- belastingadviseurs en administratiekantoren;
- juridisch adviseurs als zij bedrijfsmatig advies geven of bijstand verlenen op specifieke terreinen, onder meer bij vastgoedtransacties en fusie en overname;⁴²
- degenen die bedrijfsmatig een adres of postadres ter beschikking stellen (domicilieverleners);⁴³
- makelaars;⁴⁴
- handelaars (zowel verkopers als kopers) die goederen (ver)kopen als de koopprijs 10.000 euro of meer bedraagt;⁴⁵
- makelaars bij koop en verkoop van voertuigen, schepen, kunstvoorwerpen, antiquiteiten, edelstenen, edele metalen, sieraden of juwelen;⁴⁶
- handelaars (zowel verkopers als kopers) van kunstvoorwerpen als de prijs 10.000 euro of meer is⁴⁷, wat onder meer musea omvat;
- taxateurs van onroerende zaken.⁴⁸

Gereguleerde sectoren

Er zijn een aantal Wwft-plichtigen die niet tot de financiële sector behoren, waarvoor een vorm van toezicht geldt:

- beroepsmatige statutair bestuurders ('trustkantoren');⁴⁹
- accountants;⁵⁰
- advocaten en notarissen als zij bedrijfsmatig advies geven of bijstand verlenen op specifieke terreinen, onder meer bij vastgoedtransacties en fusie en overname;⁵¹
- aanbieders van wisseldiensten en bewaarportemonnees voor virtuele valuta;⁵²
- bepaalde kansspelaanbieders.⁵³

Kwaliteit gegevensverwerking

Dit betekent echter niet dat er voldoende toezicht is op de kwaliteit van de verwerking van persoonsgegevens en de naleving van de AVG. Nog riskanter wordt het als de Wwft-plichtigen in verband met de naleving gebruik maken van externe leveranciers, zoals

⁴² Zie artikel 1a lid 4 sub c. en d. Wwft. De wet geldt niet als rechtsbijstand wordt verleend, zie artikel 1a lid 5.

⁴³ Artikel 1a lid 4 sub g. Wwft.

⁴⁴ Artikel 1a lid 4 sub h. Wwft.

⁴⁵ Artikel 1a lid 4 sub i. Wwft.

⁴⁶ Artikel 1a lid 4 sub j. Wwft.

⁴⁷ Artikel 1a lid 4 sub k. Wwft.

⁴⁸ Artikel 1a lid 4 sub o. Wwft.

⁴⁹ Artikel 1a lid 4 sub f. Wwft.

⁵⁰ Artikel 1a lid 4 sub b. Wwft.

⁵¹ Zie artikel 1a lid 4 sub c. en d. Wwft. De wet geldt niet als rechtsbijstand wordt verleend, zie artikel 1a lid 5.

⁵² Zie artikel 1a lid 4 sub l. en m. Wwft. Zij dienen over een vergunning van DNB te beschikken op grond van hoofdstuk 3A van de Wwft.

⁵³ Artikel 1a lid 4 sub n. Wwft.

compliance dienstverleners, datahandelaren en IT-leveranciers. Via die externe leveranciers kunnen persoonsgegevens en andere vertrouwelijke gegevens weglekken.

Aan deze compliance dienstverleners, datahandelaren en IT-leveranciers worden geen integriteitseisen gesteld en er is onvoldoende of geen toezicht op de wijze waarop zij de persoonsgegevens en andere vertrouwelijke gegevens van de klanten van Wwft-plichtigen verwerken.

Gevolg is dat de gegevensverwerking door Wwft-plichtigen grote risico's voor burgers met zich meebrengt.

Privacy First is zeer bezorgd over datalekken en andere incidenten bij Wwft-plichtigen, bijvoorbeeld accountantskantoren en notariskantoren, die zeer veel vertrouwelijke gegevens verwerken.

One-size-fits-all

Kenmerkend voor de Wwft is dat voor alle Wwft-plichtigen dezelfde regels gelden, terwijl het systeem is ontworpen voor banken. De verschillen zijn groot.

Zo is onder andere de informatiepositie van de hiervoor beschreven niet-financiële Wwft-plichtigen onderling heel verschillend en verschilt die sterk van banken. Ook ziet niet iedereen evenveel transacties. Een aanbieder van safeloketten en een domicilieverlener zien helemaal geen transacties van hun klanten (behalve dan de transacties met henzelf). Sommige Wwft-plichtigen zien maar weinig transacties, zeker in vergelijking met betaalinstanties/banken (bijvoorbeeld juristen) of zien de transacties pas achteraf (zoals administratiekantoren en accountants).

Het kennisniveau van de verschillende soorten Wwft-plichtigen is heel verschillend, terwijl van allen hetzelfde onderzoek naar de organisatiestructuur en de uiteindelijk belanghebbende van de cliënt wordt verwacht.

Kenmerkend voor de Wwft is dat de regelgevers de verschillen tussen de soorten Wwft-plichtigen volledig negeren en het doen voorkomen dat zij hun cliënten kunnen kennen en een risicoprofiel kunnen maken aan de hand waarvan de transacties respectievelijk de zakelijke relatie kunnen worden getoetst. De juistheid van deze stelling is nog nooit onderbouwd.

Effectiviteit

Het is van algemene bekendheid dat de effectiviteit van het huidige systeem van witwasbestrijding en bestrijding van terrorismefinanciering zeer gering is. Dat komt niet alleen doordat de overheid onvoldoende capaciteit heeft om de meldingen van ongebruikelijke transacties op te volgen.

In opdracht van de Stichting Maatschappij en Veiligheid schreef een commissie van deskundigen het rapport 'Poortwachters tegen witwassen'⁵⁴, waarin wordt geconstateerd

⁵⁴ Zie <https://maatschappijveiligheid.nl/poortwachtersfunctie-banken/>, 20 juni 2022.

dat de misdaadbestedingsactiviteiten van banken zeer kostbaar zijn en weinig opleveren. De huidige transactiemonitoring door banken bij hun eigen klanten is al een financiële surveillance van burgers die zeer ingrijpend is, waarvan niet vaststaat dat deze op een juiste manier plaatsvindt; voorts zijn de activiteiten van banken zeer kostbaar en leveren hinder en overlast voor de klanten op.⁵⁵

De klanten van banken ervaren het optreden van deze financiële instellingen regelmatig als hinderlijk, soms vanwege de onkunde die uit de vragen blijkt, maar ook vanwege de wantrouwende houding en de bancaire uitvluchten (doen alsof de vragen worden gesteld vanwege de veiligheid van de klant, terwijl de bank in werkelijkheid wil weten of de klant crimineel is).

Een boekhoudster schreef in 2021:



Yvonne Krul · 1ste
Administrator / advisor

2 d ...

Het is bijna onmogelijk een bankrekening te hebben en te behouden. En de compliance afdelingen stellen de meest onbenullige en idiote vragen. Het ontbreekt hen ten enenmale aan fundamentele kennis over wet en regelgeving. Het zijn cowboys en compliance is het wilde westen.

Uitsluiting & de-risking

Een schadelijke ontwikkeling is dat de witwasbestrijding leidt tot uitsluiting van burgers en organisaties, de zogenaamde 'de-risking'. Dit fenomeen wordt veroorzaakt door de vermeende hoge witwas- en terrorismefinancieringsrisico's die bepaalde groepen klanten opleveren (waarbij ook de sanctieregelgeving en de dienstverlening aan de overheid een rol spelen).

Het de-risken is nu al pijnlijk zichtbaar, bijvoorbeeld doordat banken diensten weigeren aan mensen met de Amerikaanse nationaliteit en mensen die in de Verenigde Staten of Iran geboren zijn. Organisaties en bedrijven hebben er meer last van, zo willen veel banken geen rekeningen meer openen voor stichtingen en verenigingen en hebben bepaalde ondernemingssectoren de grootste moeite om rekeningen te openen. Inmiddels zijn er al vele berichten in de media verschenen over allerlei vormen van uitsluiting.⁵⁶

⁵⁵ De banken realiseren zich dat, zie het artikel 'Banken: hinder voor klanten door witwasaanpak verminderen', 26 september 2022, <https://www.nvb.nl/nieuws/banken-hinder-voor-klanten-door-witwasaanpak-verminderen/>. Maar ze komen met de verkeerde oplossing.

⁵⁶ Zie bijvoorbeeld:

- 'Door de jacht op terroristen en fout geld kunnen ook de brave vrijwilligers hun geld nergens kwijt', de Volkskrant 29 november 2021, <https://www.volkskrant.nl/economie/door-de-jacht-op-terroristen-en-fout-geld-kunnen-ook-de-brave-vrijwilligers-hun-geld-nergens-kwijt~b4ed7ac9/>;
- Uitsluiting van defensiebedrijven <https://www.nidv.eu/nieuws/enquete-nidv-toegang-financiele-diensten-steeds-moeilijker/>, 22 juni 2021;
- 'Rabobank sluit kleine autodealers uit vanwege risico op witwassen', FD 1 juli 2021.

Ook de Europese Banken Autoriteit (EBA) heeft gesignaleerd dat het met de-risking de spuigaten uitloopt en beloofde maatregelen⁵⁷, al zijn de effecten van die maatregelen niet te zien.

Deze uitsluitingspraktijken zijn een gevolg van de wijze waarop overheden risicoprofilering voorschrijven aan Wwft-plichtigen, waarvan de oorsprong ligt bij FATF. FATF signaleerde in hun beoordeling van Nederland, die in augustus 2022 is bekend gemaakt⁵⁸, zie onder andere pagina 125, waar wordt opgemerkt onder punt 5:

The Netherlands should consider the growing incidences of de-risking and ensure that AML obligations are not being used as a reason to exit particular sectors or groups.

FATF erkent de schade die ontstaat door de witwasbestrijding, maar menen te kunnen volstaan met ‘mitigating the unintended consequences’⁵⁹ en weigert te erkennen dat het systeem van witwasbestrijding niet juist is. Nederland volgt dezelfde redenering. Wij vinden dat het hoog tijd is dat het systeem en de gevolgen voor de burgers van Nederland ter discussie wordt gesteld.

Rechtsbescherming

Anders dan het kabinet in het de memorie van toelichting bij het wetsvoorstel veronderstelt, is de rechtsbescherming van burgers op dit moment volstrekt onvoldoende.

Het is nu al gewenst dat de rechtsbescherming wordt verbeterd van iedereen die discussies of problemen met financiële instellingen en andere Wwft-plichtigen heeft over de witwasbestrijding.

-
- brandbrieven van onder andere de Beroepsvereniging Bewindvoerders WSNP (BBW), zie de reactie van Financiën, 1 juli 2021, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z12357&did=2021D26600;
 - brandbrief Insolad, vereniging insolventierecht advocaten, aan de minister van Financiën c.s., <https://www.internetconsultatie.nl/wijzigingalgemeneleidraadwwft/reactie/168572/bestand>;
 - boze klant van DeGiro, die afscheid neemt van iedereen die geen natuurlijke persoon is, <https://www.linkedin.com/pulse/extreme-derisking-bij-degiro-dirk-de-lange/>.

⁵⁷ The EBA takes steps to address ‘de-risking’ practices, 22 maart 2022, <https://www.eba.europa.eu/eba-takes-steps-address-%E2%80%98de-risking%E2%80%99-practices>.

⁵⁸ <https://www.rijksoverheid.nl/documenten/rapporten/2022/08/24/mutual-evaluation-report-netherlands-2022>

⁵⁹ Zie <https://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/unintended-consequences-project.html>.

Bijlage 2 - Hoog risico volgens DNB

IRAP-formulier

Volgens het IRAP-formulier voor trustkantoren dat in het voorjaar van 2022 door DNB bekend is gemaakt ⁶⁰ zijn dit hoog risico sectoren:

Hoog risico wegens structuur of rechtsvorm (rubriek 'Structuren*/eigenschappen doelvennootschappen')

DNB noemt:

- *Doelvennootschappen met private structuur***
- *Doelvennootschappen met kwalificatie BFI*
- *Doelvennootschappen met > 5 lagen in de structuur****
- *Doelvennootschappen dat onderdeel is van een structuur met één of meer nomineer shareholders*
- *Doelvennootschappen waarbij sprake is van een structuur met één of meer commanditaire vennootschappen dan wel buitenlandse rechtspersonen die qua eigenschappen/kenmerken vergelijkbaar zijn met een Nederlandse commanditaire vennootschap.*
- *Doelvennootschappen die kwalificeren als coöperatie/coöperatieve vereniging*
- *Doelvennootschappen die onderdeel zijn van een structuur waarin één (of meer) (Angelsaksische) trust(s) is (zijn) opgenomen*
- *Doelvennootschappen die onderdeel zijn van een structuur waarin één (of meer) stichting(en) is (zijn) opgenomen*
- *Doelvennootschappen die zelf kwalificeren als stichting*
- *Doelvennootschappen met één (of meer) buitendirecteuren die alleen/zelfstandig bevoegd is (zijn)*
- *Doelvennootschappen waarbij sprake is van back-to-back**** leningen bij de doelvennootschap en/of haar deelneming(en)*

⁶⁰ https://www.dnb.nl/media/yjinxjdp/2022-04-05_irap_vragenlijst_trustkantoren_peildatum_31-12-2021_v2022-01.xlsx,
aankondiging: <https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2022/uitvraag-periodieke-rapportage-voor-trustkantoren/>.

Er hoort de volgende toelichting door DNB bij:

** Structuur: het gaat hierbij om de eigendomsstructuur en de formele zeggenschapsstructuur van de doelvennootschap, alsmede de relevante delen van de structuur van de groep waartoe de doelvennootschap behoort.*

*** Een private structuur is een structuur die (al dan niet middellijk) gehouden wordt door een of enkele natuurlijke personen, dan wel waar sprake is van feitelijke of bijzondere zeggenschap door een of enkele natuurlijke personen. Het betreft geen beursgenoteerde onderneming en geen staatsbedrijf.*

**** NB: bij het bepalen van het aantal lagen dienen zowel de lagen onder als boven de doelvennootschap in acht te worden genomen (incl. de dv).*

***** Een back-to-back lening is een kredietinstrument waarbij de kredietnemer geld of financiële instrumenten ter beschikking krijgt. De kredietverstrekker ontvangt daarvoor een zekerheid, direct of indirect, uit eigen liquide middelen van de kredietnemer bijvoorbeeld in de vorm van een deposito, garantiestelling of (in depot) ontvangen financiële waarden.*

Hoog risico algemeen (rubriek 'Doelvennootschappen algemeen')

Hier worden door DNB genoemd:

- *Doelvennootschappen gerelateerd aan vastgoed* (o.a.: projectontwikkeling, het doen van vastgoedtransacties, exploitatie van vastgoed)*
- *Doelvennootschappen waaraan ook een ander trustkantoor trustdiensten verleent*
- *Inactieve doelvennootschappen (> 1 jaar geen transactie/activiteit (anders dan instandhouding))*

Toelichting DNB:

** Hierbij gaat het om de hoofdactiviteit van de structuur waar de doelvennootschap onderdeel van is.*

Activiteiten in hoog risico sectoren

DNB geeft de volgende lijst:

- *Grondstoffen, mineralen, mijnbouw*
- *Olie, gas, energie*
- *Militaire goederen/defensie*

- *Handelaren in edelmetalen*
- *Handelaren in losse diamanten*
- *Juweliers*
- *Handelaren in kunst*
- *Veilinghuizen*
- *Handelaren en/ of handelsplatformen en/of aanbieders van bewaarportemonnees in crypto's*
- *Uitgevers van cryptotokens (uitgegeven via een Initial Coin Offering)*
- *Crowdfunding*
- *(Online) kansspelen*
- *Bouw, infrastructuur, offshore & dredging***
- *Commercieel vastgoed*
- *Coffeeshops, growshops*
- *Profsport**
- *Relaxbedrijven, prostitutie, adult industry (incl. internet)*
- *Religieuze instellingen & charitatieve instellingen (o.a. stichtingen)*
- *Transport, shipping*
- *Adviesdienstverlening, consultancy*
- *Intellectueel eigendom/patenten/royalty's*
- *Money transfer organisaties en payment service providers*
- *Farmaceutische industrie*
- *Cash intensieve sectoren (bijv. taxi branch, car wash / parking / wasserettes)*
- *Schroothandel*
- *Autohandelaren*
- *Horeca*
- *Online shops*
- *Handel in luxe / waardevolle producten (leer / bont, antiek, vee)*
- *Telecom (belwinkels etc.)*

Toelichting DNB:

** Het gaat om (o.a.) spelers, intermediairs, zaakwaarnemers, nationale en internationale bonden (zoals KNVB, FIFA, UCI en IOC), teams/clubs, en eigenaren van teams/clubs.*

*** (zee)kustgerelateerde bouw- en engineeringactiviteiten, baggeren en dreggen*

Voorbeeld compliance dienstverlener

Een compliance dienstverlener heeft een nog ruimer overzicht van 'verhoogd risico Wwft' waarin o.a. de hele landbouw, de hele e-commerce, alle kappers en alle toeristenwinkels tot hoog risico worden verklaard. Zie onderstaand recent overzicht op de website van deze dienstverlener:

BRANCHES VERHOOGD RISICO WWFT

DIT SCHEMA IS BIJGEWERKT T/M 1 JUNI 2022



 AFVAL- VERWERKING	 AMBTENAREN OVERIG	 AUTOHANDEL, -SCHADE, -VERHUUR, -WASSTRAAT, -EXPORT OUDE LEASE	 BELWINKELS	 BEMIDDELAAR SUBSIDIES	 BLOEMEN- HANDEL	 BOUW, AANNEMERS, SLOOP	 CASINO
 COFFEESHOPS, GROWSHOPS	 CROWD- FUNDING	 DOUANE, POLITIE, JUSTITIE	 E-COMMERCE	 (EDEL)METALEN ZOALS PLATINA, KOPER EN NIKKEL	 ELEKTRONICA	 EMISSIE- HANDEL	 ENERGIE, OLIE, GAS
 EVENEMENTEN, ZAALVERHUUR	 EXPORT NAAR CASHLANDEN	 FOTO-, VIDEO-, EN AUDIO- APPARATUUR EN -DRAGERS	 FRUIT- HANDEL	 GELDWISSEL- KANTOREN	 HAVEN- BEDRIJVEN	 HORECA	 INFRA- STRUCTUUR
 JUWELIERS, GOUDINKOOP	 KAPPERS	 KLEDING- BOETIEKJES	 KRINGLOOP- WINKELS	 KUNST- EN ANTIETK	 LANDBOUW	 MASSAGE- SALONS	 NAGEL- STUDIO'S
 PAARDEN- HANDEL	 PLEZIER- VAARTUIGEN	 SCHOONHEIDS- SALONS	 SEKS- BRANCHE	 TABAKS- PRODUCTEN	 TAXI- BEDRIJVEN	 TOERISTEN- WINKELS	 TRUST- SECTOR
 UITZEND- BUREAUS	 VEILING- HUIZEN	 VERHUUR, BEMIDDELING, VASTGOED, KAMERS	 VIRTUELE VALUTA	 VISSERIJ	 VOETBAL- CLUBS	 ZONNEBANK- STUDIO'S	 ZORG- BEDRIJVEN

 **BEKIJK HET ACTUELE OVERZICHT MET BRANCHES IN DATABANK WWFT**

Bron: <https://www.fbn.nl/wp-content/uploads/2022/06/Visueel-overzicht-branches-met-verhoogd-risico-1-juni-2022.pdf>

Bijlage 3 – Hoog risico factoren volgens Annex III bij AMLD4

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02015L0849-20210630#tocId108>

ANNEX III

The following is a non-exhaustive list of factors and types of evidence of potentially higher risk referred to in Article 18(3):

(1) Customer risk factors:

- (a) the business relationship is conducted in unusual circumstances;
- (b) customers that are resident in geographical areas of higher risk as set out in point (3);
- (c) legal persons or arrangements that are personal asset-holding vehicles;
- (d) companies that have nominee shareholders or shares in bearer form;
- (e) businesses that are cash-intensive;
- (f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;

▼M1

(g) customer is a third country national who applies for residence rights or citizenship in the Member State in exchange of capital transfers, purchase of property or government bonds, or investment in corporate entities in that Member State.

▼B

(2) Product, service, transaction or delivery channel risk factors:

- (a) private banking;
- (b) products or transactions that might favour anonymity;

▼M1

(c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic identification means, relevant trust services as defined in Regulation (EU) No 910/2014 or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities;

▼B

(d) payment received from unknown or unassociated third parties;

(e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;

▼M1

(f) transactions related to oil, arms, precious metals, tobacco products, cultural artefacts and other items of archaeological, historical, cultural and religious importance, or of rare scientific value, as well as ivory and protected species.

▼B

(3) Geographical risk factors:

- (a) without prejudice to Article 9, countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;
- (b) countries identified by credible sources as having significant levels of corruption or other criminal activity;
- (c) countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;
- (d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

Over Privacy First

Privacy First is een onafhankelijke stichting met als doel het behouden en bevorderen van het recht op privacy alsmede de persoonlijke vrijheid van leefomgeving. Privacy First zet zich in voor het behoud en de versterking van het recht op:

- Privacy en eerbiediging van de persoonlijke levenssfeer.
- Bescherming van persoonsgegevens.
- Vertrouwelijke communicatie.
- Lichamelijke integriteit.

Privacy First heeft als doel deze rechten op een gedegen manier te laten vastleggen in de wet en treedt hierin actief op in de vorm van politieke lobby, juridische actie en rechtszaken, informatieverstrekking en acties voor het grote publiek.

Zie voor onze standpunten en activiteiten op het terrein van financiële privacy <https://www.privacyfirst.nl/aandachtsvelden/financiele-privacy.html> .

Amsterdam, 2 december 2022