

aan Ministerie van Financiën
Ministerie van Justitie en Veiligheid
Ministerie van Economische Zaken
via
<https://www.internetconsultatie.nl/implementatiewetvoorkomingvanwitwassenenterrorismefinanciering/b1>

ons kenmerk SPF20250829

datum 29 augustus 2025

onderwerp Consultatie Implementatiewet ter voorkoming van witwassen en terrorismefinanciering

Geachte heer/mevrouw,

Stichting Privacy First maakt graag gebruik van de mogelijkheid te reageren op het voorstel voor de *Implementatiewet ter voorkoming van witwassen en terrorismefinanciering* ('Iwt'). Met deze wet zal het Europese antiwitwaspakket ('AML Package') worden geïmplementeerd.

De bestrijding van witwassen en terrorismefinanciering en het bestrijden van de niet-naleving van gerichte sancties zal hierna ook als 'AML/CFT' worden aangeduid. De Europese antiwitwasverordening zal als 'AMLR' worden aangeduid en de Europese antiwitwasrichtlijn als 'AMLD6'. Het consultatievoorstel duiden wij als 'Iwt' aan. De bedrijven die de antiwitwastaken moeten uitvoeren noemen we 'witwasbestrijdingsplichtigen'.

Een zeer grote groep van witwasbestrijdingsplichtige bedrijven, variërend van banken tot boekhouders, moeten dezelfde AML/CFT-regels toepassen, die kortgezegd inhouden dat zij een risicoprofiel van zichzelf en van iedere klant moeten maken, moeten zorgen voor procedures en alle transacties en activiteiten van hun klanten moeten monitoren. Dit alles heeft tot doel dat zij de opsporing kunnen assisteren door vermoedens van criminaliteit of crimineel geld ¹ te melden aan een onderdeel van de politie, FIU-Nederland ('FIU-NL'). Dit duiden wij ook aan als privatisering van de misdaadbestrijding. Deze privatisering levert veel problemen op, die vooral aan het licht zijn gekomen in de financiële sector, maar die ook elders zichtbaar zijn.

De privatisering van de misdaadbestrijding brengt op dit moment al grote maatschappelijke schade toe en het schaadt het vertrouwen van burgers in de financiële sector en in de overheid. Het heeft geleid tot schuldbekentenissen van de financiële sector

¹ Artikel 96 AMLR.

en van de minister van Financiën. In **bijlage 1** bij deze consultatiereactie lichten wij de problematiek nog een keer toe. Met de voornoemde schuldbekentenissen zijn we er nog niet, zoals wij hierna zullen toelichten.

In deze consultatiereactie doen wij voorstellen voor de Nederlandse implementatie van de Europese antiwitwasregelgeving, wat niet betekent dat wij akkoord zijn met de inhoud van het AML Package. Het doel van onderhavig commentaar is om de schadelijke effecten van die regelgeving zoveel mogelijk te beperken, waarbij wij ons het recht voorbehouden om te ageren tegen elementen van die regelgeving die in strijd zijn met de AVG, het Europees Handvest of andere grondrechten.

Privacy First benadrukt dat zij niet gekant is tegen het betrekken van bedrijven bij de misdaadbestrijding. Haar bezwaren richten zich tegen het toebedelen van taken aan bedrijven die daar niet geschikt voor zijn, tegen de disproportionele kosten die witwasbestrijdingsplichtigen moeten maken en aan de klant worden doorberekend, en tegen het niet respecteren van de grondrechten van burgers, midden- en kleinbedrijf en kleine en middelgrote non-profit organisaties.

Privacy First benadrukt dat niet alleen consumenten geraakt worden door deze regelgeving. Mkb en de kleine en middelgrote non-profit organisaties staan even onmachtig tegenover de overheid en de grote witwasbestrijdingsplichtigen zoals banken.

In deze consultatiebijdrage doen wij daarom voorstellen om te schade door de privatisering van de misdaadbestrijding te beperken.

De opbouw van deze consultatiereactie is als volgt:

- In deel A gaan we in op de onderwerpen die in het consultatievoorstel ontbreken.
- Deel B bevat commentaar op een aantal elementen van het consultatievoorstel.

Inhoudsopgave

A.	Onderwerpen die in de lwt ontbreken	5
A1.	<i>Het AML/CFT systeem: foutencorrectie en informatie</i>	<i>5</i>
A2.	<i>Bestrijden van discriminatie en de-risking / handhaving op schending grondrechten</i>	<i>7</i>
A3.	<i>Verplichting tot aanbieden basisdiensten en verbod doorberekening CDD- kosten</i>	<i>9</i>
A4.	<i>Gegevensverwerking</i>	<i>10</i>
A5.	<i>Openbaarmaking van persoonsgegevens via het ubo-register</i>	<i>15</i>
A6.	<i>Rechtsbescherming en optreden tegen grondrechtenschendingen</i>	<i>16</i>
A7.	<i>Gegevens delen door witwasbestrijdingsplichtigen (artikel 75 AMLR) en uitbesteding</i>	<i>17</i>
A8.	<i>Open finance verbod</i>	<i>18</i>
A9.	<i>Verwijzingsportaal banken</i>	<i>19</i>
A10.	<i>Schrappen bestaande nationale regels die afwijken van de EU-regels</i>	<i>20</i>
B.	Detailonderwerpen uit het voorstel voor de lwt	22
	<i>Artikel 1.3 lid 2 lwt – nieuwe verordeningen inzake AML/CFT</i>	<i>22</i>
	<i>Hoofdstuk 3 – de governance van FIU NL</i>	<i>22</i>
	<i>Artikel 3.6 lwt – Opschorting van transacties in opdracht van FIU-Nederland</i>	<i>23</i>
	<i>Artikel 2.3 lwt – Personentoetsing bij alle witwasbestrijdingsplichtigen</i>	<i>25</i>
	<i>Artikel 2.4 – Verscherpt cliëntenonderzoek voor aanbieders van trustdiensten of vennootschapsrechtelijke diensten</i>	<i>26</i>
	<i>Artikel 3.13 – Verschillende definities basisdelicten</i>	<i>27</i>
	Tot slot	28

Bijlage 1 – De schaduwkant van de privatisering van de misdaadbestrijding 29

Naleving grondrechten is nodig om het vertrouwen van burgers te verdienen 29

De problemen spelen al langer en zijn bekend..... 29

Gegevensbeschermingsrisico's..... 33

Bijlage 2 – Samenwerking tussen de banken 39

A. Onderwerpen die in de lwt ontbreken

In het consultatievoorstel ontbreken een aantal elementen die naar het oordeel van Privacy First nodig zijn om de risico's verbonden aan het AML Package te beperken.

Wij geven bij de onderdelen een korte toelichting op de achtergrond en zijn desgewenst bereid nadere informatie te verschaffen.

A1. Het AML/CFT systeem: foutencorrectie en informatie

Achtergrond:

- De praktijk leert dat er fouten en onvolkomenheden voorkomen in nadere regelgeving (zowel Nederlands als Europees) en in de opvattingen en aanpak door toezichthouders en bij witwasbestrijdingsplichtigen. Dit komt onder meer tot uitdrukking in de witwastypologieën en -indicatoren en het gebruik daarvan, zowel door witwasbestrijdingsplichtigen als door de overheid.² De nadere regelgeving en de uitvoeringspraktijk wordt nu ontwikkeld zonder de vertegenwoordigers van de klanten er bij te betrekken.³
- Doordat de overheid (onder andere door middel van de bijlagen bij AMLR, de risicobeoordeling van de Europese Commissie (SNRA), de nationale risicobeoordelingen (NRA's) en uitingen en standpunten van de toezichthouder ⁴) bepaalde klantgroepen als 'hoog risico' aanmerkt, worden deze klantgroepen door witwasbestrijdingsplichtigen geweigerd dan wel worden witwasbestrijdingsplichtigen met hoge nalevingskosten geconfronteerd, die zij zullen doorberekenen.
- In de huidige Nederlandse NRA's staan ernstige fouten. Op grond van het AML Package zullen de NRA's een semi-wettelijke status krijgen en daarom is het onaanvaardbaar als er onjuistheden in staan.
- Het AML/CFT systeem is nu al ingewikkeld en het zal door het AML Package nog ingewikkelder worden, onder andere omdat er zowel sprake is van EU-regels als Nederlandse regels. De EU zal met zeer veel nadere regels ('RTS', richtsnoeren, enzovoorts) komen. In de consultatietoelichting wordt gemeld: "*Het gehele pakket kent meer dan 40*

² Zie onder andere de kritiek in dit Vaklunch artikel: <https://vaklunch.nl/witwasindicatoren-als-startpunt-geen-sluitstuk/>.

³ Voorbeeld: het rondetafelgesprek met brancheorganisaties van witwasbestrijdingsplichtigen, https://www.tweedekamer.nl/debat_en_vergadering/commissievergaderingen/details?id=2025A02441.

⁴ Zoals de aanvraagformulieren van DNB en AFM, die voorheen als excel bestand gedownload konden worden. Voorheen plaatste DNB onder andere in de hoog risico categorie: adviesdienstverlening en consultancy, religieuze & charitatieve instellingen (onder andere stichtingen), telecom, online winkels, horeca, autohandelaren en cash intensieve sectoren. Een hoog risico kwalificatie kan ook in de privé-sfeer gevolgen hebben.

grondslagen voor de AMLA om nadere regelgeving uit te werken, plus een algemene grondslag voor de AMLA om richtsnoeren op te stellen over niet voorgeschreven onderwerpen." (pagina 3)

- In artikel 1.2 Iwt is opgenomen dat de krachtens de AMLR door de Europese Commissie en AMLA gestelde regels worden gelijkgesteld met krachtens de Nederlandse wet gestelde regels. Als die nadere regels fouten of onvolkomenheden bevatten, zal dat schadelijke gevolgen hebben voor Nederlandse burgers.
- Het AML/CFT systeem is zeer kostbaar, onder meer door de ingewikkeldheid en het dubbele werk dat wordt gedaan. Een serieuze toetsing van de uitvoerbaarheid, de effectiviteit en het nut om overheidstaken aan bedrijven uit te besteden die daar niet geschikt voor zijn, heeft nog nooit plaatsgevonden.⁵
- Op dit moment is de informatie over AML/CFT versnipperd en verspreid over verschillende bronnen (EU, Nederlandse overheid, toezichthouders, FIU NL). Dat maakt het voor klanten moeilijk om na te gaan of de witwasbestrijdingsplichtige correct handelt.

Commentaar:

Vragen:

- Stel dat er ernstige fouten in de Europese of Nederlandse regels staan: hoe worden die gesignaleerd? Is er een correctiemogelijkheid? Is er een laagdrempelige mogelijkheid om de onjuistheid van de nadere regels aan de kaak te stellen?
- Hoe wordt er voor gezorgd dat onjuiste praktijken bij witwasbestrijdingsplichtigen aan het licht komen? Immers, alles is (opsporings)geheim, wat een onafhankelijke toetsing belemmert (zie rechtbank Den Haag 9 september 2024, <https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2024:14477>). Hoe wordt tegenspraak georganiseerd? Hoe kunnen getroffen burgers mogelijke fouten onmiddellijk rechtzetten zonder dat zij hierover jarenlang moeten procederen?

Aanbevelingen:

- Beperk de nationale regels zoveel mogelijk. Schrap alle overbodige bepalingen uit de Iwt en overige Nederlandse regelgeving.
- Creëer tegenwicht bij totstandkoming NRA's en voorlichtingsuitingen FIU-Nederland / AMLC c.s. aangezien daar fouten en onvolkomenheden in voorkomen. Bijvoorbeeld door middel van een instituut dat onafhankelijk is van de financiële sector en van de ministeries van Financiën en Justitie en Veiligheid.
- Creëer een systeem waarin het mogelijk wordt om fouten en onvolkomenheden onmiddellijk te signaleren en te corrigeren, zowel voor klanten van witwasbestrijdingsplichtigen als de witwasbestrijdingsplichtigen zelf. Zorg voor onafhankelijke tegenspraak.

⁵ De evaluaties gaan tot nu toe alleen over deelonderwerpen.

- Vanwege de ingewikkeldheid van de regelgeving is het essentieel dat er één goed toegankelijke database wordt ontwikkeld waarin alle informatie is te vinden en die ook voor niet-gespecialiseerde burgers toegankelijk is en waarin voor alle detailonderwerpen is na te gaan wat de onderbouwing van de regels is. Neem daarin alle uitingen van de Nederlandse en Europese overheid op en ook alle Nederlandse toezichthouders en FIU-NL. Privacy First verzoekt de Nederlandse regering zo'n database tot stand brengen. Dit is nodig voor klanten van witwasbestrijdingsplichtigen en kan ook voor witwasbestrijdingsplichtigen zelf van nut zijn.
- Wij verzoeken de Nederlandse regering te zorgen voor een voorlichtingscampagne waarin het publiek goed wordt geïnformeerd over de ingrijpende wijzigingen die het AML Package met zich meebrengt, met inbegrip van de extra maatregelen die zijn genomen om excessen (zoals zich onder de huidige antiwitwasregels voordoen) te voorkomen.
- Wij verzoeken onafhankelijk onderzoek in te laten stellen naar de vraag of de witwasbestrijdingsplichtigen de huidige en nieuwe regelgeving wel begrijpen (doenvermogen) en of zij gelet op hun kennis en vaardigheden wel in staat zijn tot naleving. In dat onderzoek dient ook te worden betrokken wat de werkelijke nalevingskosten zijn en of de opbrengst (voorkoming crimineel geld respectievelijk detecteren en melden crimineel geld) opweegt tegen de kosten. In het onderzoek dient te worden nagegaan of de regels leiden tot discriminatie en de-risking, of de diensten van witwasbestrijdingsplichtigen duurder worden als gevolg van de AML/CFT verplichtingen, of het leidt tot vermindering van het aanbod en of toegang tot basisdiensten wordt beperkt als gevolg van de AML/CFT verplichtingen.

A2. Bestrijden van discriminatie en de-risking | handhaving op schending grondrechten

Achtergrond:

- Discriminatie en de-risking zijn goedkoper dan mitigerende maatregelen. Naar verwachting zullen discriminerende praktijken onder het AML Package verder toenemen. Dat is onder meer een gevolg van de veel bredere meldingsplicht inzake criminaliteitsvermoedens (artikel 69 AMLR). Daan Doorenbos schreef in zijn artikel over de nieuwe meldplicht: *"In mijn optiek hoort een zo ver opgerekte opsporingstaak niet thuis bij de meldingsplichtige entiteiten die onder de verordening vallen. Het is principieel en praktisch onwenselijk dat private partijen worden belast met de algemene opdracht de handel en wandel van hun eigen cliënten te toetsen aan commune en bijzondere strafwetgeving. Daar zijn zij niet voor opgeleid en dat leidt tot groot ongemak respectievelijk onderling wantrouwen".*⁶

⁶ Daan Doorenbos, *De meldingsplicht uit de nieuwe antiwitwasverordening*, tijdschrift Ondernemingsrecht juni 2025, pagina 431-436.

- Daar komt bij dat AMLR afwijkende definities van witwassen en terrorismefinanciering kent, daarin wordt verwezen naar artikel 3, leden 1 en 5, van Richtlijn (EU) 2018/1673, respectievelijk artikel 11 van Richtlijn (EU) 2017/541 en wordt vervolgens van alles toegevoegd, waarbij ook nog een passage inzake kleurloos opzet is opgenomen (bij witwassen: "*medeweten, bedoeling of opzet, vereist als bestanddeel van die gedragingen, kunnen worden afgeleid uit objectieve feitelijke omstandigheden*"). Dit betekent dat er zeer snel witwassen of terrorismefinanciering moet worden aangenomen, waardoor grote schade voor de beschuldigde kan ontstaan.
- Soms is de 'hoog risico' kwalificatie op de AMLR gebaseerd, een voorbeeld daarvan is de veel te brede definitie van PEPs (deze omvat ook ouders, kinderen en naaste geassocieerden), terwijl maar een zeer klein deel van de PEPs, hun aanverwanten en naaste geassocieerden een criminaliteitsrisico vormt (naar de mening van Privacy First is dit onrechtmatige Europese regelgeving). Het is belangrijk dat de Nederlandse wetgever maatregelen neemt om de schade van de PEP-definitie te mitigeren.
- Nationaliteitsdiscriminatie wordt in het AML Package gelegaliseerd, terwijl er geen verband is tussen nationaliteit en criminaliteit / crimineel geld. De Commissie Meijers adviseerde in januari 2024 "*to prohibit the use of sensitive and potential discriminatory data such as nationality, religious affiliation, country of birth, country of residence*"⁷, maar daar is door de Europese wetgever niets mee gedaan. Ook hier zijn mitigerende maatregelen nodig.
- Risicoprofilering met AI op persoonsniveau is de kern van het AML/CFT systeem. Of dat werkelijk mogelijk is, is de vraag. Zie in dat verband het advies van de Wetenschappelijke Adviesraad Politie (WARP) van juni 2025, <https://www.wetenschappelijkeadviesraadpolitie.nl/uploads/publications/Navigeren-in-niemandslan.pdf>, waarin de Raad opmerkt: "*De conclusie lijkt daarom gerechtvaardigd dat het voorspellen van crimineel gedrag op persoonsniveau geen vanzelfsprekende ambitie zou moeten zijn. Dit in tegenstelling tot de verdere inzet van data- en AI-toepassingen bij het analyseren van criminaliteitsfenomenen en – patronen op basis van historische en in sommige gevallen mogelijk real time data.*". Om die reden komt WARP tot dit advies: "*De Raad adviseert de politie niet verder in te zetten op (algoritmische) toepassingen die gericht zijn op het voorspellen van (crimineel) gedrag op persoonsniveau en dat ook publiekelijk kenbaar te maken*". Dit is ook relevant voor witwasbestrijdingsplichtigen.
- Witwasbestrijdingsplichtigen zijn criminaliteitsbestrijdingsamateurs, daarbij speelt ook dat de antiwitwas-compliance een hoge kostenpost vormt, mede door de bureaucratische eisen (de witwasbestrijdingsplichtige moet bewijzen dat de wet is nageleefd). Door dit amateurisme worden fouten gemaakt en wordt gediscrimineerd.

⁷ <https://www.commissie-meijers.nl/wp-content/uploads/2024/01/240112-Meijers-Committee-comment-CM2401-EU-Anti-Money-Laundering-AML-package.pdf>

Commentaar:

- Dring bij de Europese wetgever aan op aanpassing van artikel 69 AMLR en op aanpassing van de PEP-definitie zodat de grondrechtenschendingen worden beperkt. Dring bij de Europese wetgever aan op verwijdering van andere onjuiste hoogrisico kwalificaties uit de AMLR.
- Neem in de lwt expliciet op dat de toezichthouder er op toeziet dat de eisen die aan witwasbestrijdingsplichtigen worden gesteld beter aansluiten bij het doenvermogen van de respectievelijke soorten ondernemingen en dat geen irreële eisen worden gesteld aan witwasbestrijdingsplichtigen uit het mkb.
- Neem in de lwt op dat toezichthouders verplicht zijn om bij het voorbereiden van handhavende maatregelen na te gaan of die maatregelen de-risking en/of discriminatie en/of andere grondrechtenschendingen tot gevolg zullen hebben. Neem in de lwt op dat boetes alleen worden opgelegd als niet-naleving van voorschriften er daadwerkelijk toe heeft geleid dat crimineel geld niet is ontdekt ⁸ of na herhaling.
- Er dienen aanvullende mechanismen te worden gecreëerd die de antiwitwastoezichthouders en andere overheidsinstanties er toe bewegen de risico's op schending van grondrechten te beperken. Bijvoorbeeld doordat hun optreden onderzocht kan worden door een onafhankelijke financiële ombudsman of door een onafhankelijk kennisinstituut, die signalen kunnen oppakken en de toezichthouders kunnen aanzetten tot verbetering van hun optreden.
- Niet alleen compliance-gebreken maar ook discriminatoire praktijken en de-risking moeten actief door de antiwitwastoezichthouders worden bestreden. Neem in de lwt op dat de toezichthouder kan handhaven als de witwasbestrijdingsplichtige zich schuldig maakt aan overtreding van de gegevensbeschermingsvoorschriften, discriminatie en de-risking.

A3. Verplichting tot aanbieden basisdiensten en verbod doorberekening CDD-kosten

Achtergrond:

- Vanwege de hoge kosten van het systeem en de ingewikkeldheid gaan witwasbestrijdingsplichtigen over tot *cherry picking* (want dat is goedkoper) en de-risking. Dat betekent dat ook gewone mensen zonder goede redenen worden uitgesloten, met 'ondernemersvrijheid' als alibi. Voorbeelden: geen mensen met Amerikaanse

⁸ Anders dan in de zaak ECLI:NL:CBB:2025:369, die ging over een administratiekantoor dat iets moest melden wat al bij de opsporing bekend was.

nationaliteit wegens FATCA, want dat is te duur (Aegon, Knab), en veel banken willen geen VvE's bedienen.

Commentaar:

- Voor zover witwasbestrijdingsplichtigen een basisdienst ⁹ leveren (zoals bijvoorbeeld een bankrekening en een eenvoudige spaarrekening), dienen zij verplicht te worden deze dienst te leveren, behoudens uitzonderingen (zoals een strafrechtelijke veroordeling), waarbij de overheid eventueel ondersteuning biedt ter beperking van de kosten.¹⁰ Hier is wetgeving voor nodig, aangezien betrokken witwasbestrijdingsplichtigen dit niet uit zichzelf zullen doen. Privacy First adviseert hiertoe een bepaling in de lwt op te nemen.
- Creëer een verbod voor witwasbestrijdingsplichtigen om de CDD-kosten voor basisdiensten door te berekenen aan natuurlijke personen, mkb en kleine en middelgrote nonprofit organisaties.¹¹ Basisdiensten dienen bereikbaar te blijven tegen kosten zonder CDD-opslag.

A4. Gegevensverwerking

Achtergrond:

- Op grond van het AML Package en de daarop gebaseerde lwt zal zeer grootschalige gegevensverwerking plaatsvinden, zowel bij de overheid als bij grote witwasbestrijdingsplichtige ondernemingen. Niet alleen nationaal maar ook internationaal (onder andere uitwisseling bankrekeninggegevens via BARIS).
- In misdaadbestrijdingsland lijkt men soms te denken dat gegevensbescherming alleen maar 'hinderlijk' is, terwijl het gaat over de grondrechten van mensen en organisaties, zoals dat je niet wordt lastig gevallen als daar geen reden voor is en dat er goed met je persoonsgegevens wordt omgegaan.

Overheid

- Privacy First maakt zich ernstige zorgen over de ruime toegang die een onoverzichtelijk veld van overheidsinstanties krijgt tot veel meer persoonsgegevens dan nu het geval is, terwijl veel Nederlandse overheidsinstanties nu al niet voldoen aan de

⁹ In wetgeving zal moeten worden gedefinieerd wat basisdiensten zijn.

Niet alle witwasbestrijdingsplichtigen (huidige lijst: <https://www.fiu-nederland.nl/home/meldergroepen/>) verlenen diensten waar geen consument, mkb-onderneming of kleine of middelgrote nonprofit zonder kunnen.

¹⁰ Bijvoorbeeld door een stoplichtsysteem, waarbij de witwasbestrijdingsplichtige alleen aan de overheid hoeft te vragen of er iets aan de hand is.

¹¹ Zoals nu wel gebeurt, bijvoorbeeld bij sommige banken gebaseerd op type rechtspersoon en aantal bestuurders. Deze methode is willekeurig, nu een relatie tussen het organisatietype en het risico op witwassen en terrorismefinanciering ontbreekt.

gegevensbeschermingsregels. Voorbeelden zijn de Belastingdienst (AP: Belastingdienst moet systemen met privacyrisico's stopzetten

<https://www.autoriteitpersoonsgegevens.nl/actueel/ap-belastingdienst-moet-systemen-met-privacyrisicos-stopzetten>), de Douane en de politie (AP: politie kan gegevens niet langer bewaren dan wettelijk toegestaan <https://www.autoriteitpersoonsgegevens.nl/actueel/ap-politie-kan-gegevens-niet-langer-bewaren-dan-wettelijk-toegestaan>).

- Uit de recente beslissing van DNB inzake bunq¹² maakt Privacy First op dat DNB op grote schaal transactiegegevens van Nederlandse banken in haar bezit heeft en dat zij op basis daarvan een *outlier*-detectiemodel heeft ontwikkeld.¹³ Dit sluit ook aan bij de mededeling van DNB-bestuurder de heer Maijoor, door ons geciteerd in onze reactie tijdens de consultatie Wet rapportage hypotheekmarkt DNB.¹⁴ Privacy First heeft in de reactie aangegeven ernstige bedenkingen te hebben bij de vraag of de toezichtbepalingen wel een grondslag in de zin van de AVG bieden voor een dergelijk grootschalige, gedigitaliseerde verwerking van de betaalgegevens van miljoenen Nederlanders.
- Voor zover Privacy First bekend is, heeft nog nooit een gegevensbeschermingsonderzoek naar DNB of andere actoren in het AML/CFT-systeem, zoals FIU NL, plaatsgevonden. Het is essentieel dat belangrijke overheidsactoren in het AML/CFT-systeem worden geaudit.
- In artikel 5.6 Iwt worden dertien verschillende autoriteiten benoemd met wie de toezichthouders onder de Iwt en FIU NL informatie kunnen delen. Niet alleen de hoeveelheid potentieel betrokken instanties is zorgelijk, maar nog zorgelijker is dat niet helder is om welke instanties het exact gaat. Wij benoemen hieronder de meest diffuse definities: [a] bevoegde autoriteiten als bedoeld in artikel 2, eerste lid, punt 44, van de antiwitwasverordening; [b] de bevoegde autoriteiten uit andere lidstaten; [c] andere toezichthouders; [d] toezichthoudende instanties. De definitie van *Bevoegde autoriteiten als bedoeld in artikel 2, eerste lid, punt 44, van de antiwitwasverordening* is open en hiermee niet duidelijk. Volgens AMLR gaat het om: *een financiële-inlichtingeneenheid (FIE), een toezichthoudende autoriteit, een overheidsinstantie die belast is met het onderzoeken of vervolgen van witwassen, daarmee verband houdende basisdelicten of terrorismefinanciering of met het opsporen, in beslag nemen of bevriezen en confisqueren van criminele activa en een overheidsinstantie waaraan taken zijn toegewezen op het gebied van de bestrijding van witwassen of terrorismefinanciering.* Het is onduidelijk wie dit exact zijn. De bepaling is te ruim, zodat nadere duiding noodzakelijk is. Dit geldt ook voor autoriteiten hierboven genoemd onder [b] tot en met [c]. De ruime definiëring leidt tot overlap, wat ook weer vragen oproept. Wat is het

¹² Bekendgemaakt op 25 augustus jl., nieuwsbericht: <https://www.dnb.nl/algemeen-nieuws/handhavingsmaatregel-2025/boete-voor-bunq-b-v-wegens-onvoldoende-clientenonderzoek/>, beslissing: <https://www.dnb.nl/media/cr2ajxmx/bestuurlijke-boete-wwft-bunq-b-v.pdf>.

¹³ Paragrafen 41/42, pagina's 10/11 van het besluit.

¹⁴ <https://www.internetconsultatie.nl/rapportagehypotheekmarkt/reactie/c263celf-5df9-42a1-994e-e3539187c19b>, zie pagina 5.

verschil tussen andere toezichthouders en toezichthoudende instanties? Voor zover bedoeld is dat de bevoegde instanties ook buitenlandse instanties zijn, komt de vraag op hoe wordt voorkomen dat deze autoriteiten info opvragen via de FIU NL die naar Nederlands recht niet opvraagbaar is.

- Privacy First maakt zich ernstige zorgen over het gebrek aan afbakening van de relevante entiteiten. Dit zal ertoe leiden dat velerlei instanties gevoelige informatie van burgers uitwisselen, zonder dat duidelijk is of die instanties voldoen aan basisvoorwaarden omtrent geheimhouding of cybersecurity. Het moet te allen tijde duidelijk blijven hoe data in bepaalde systemen van instanties terecht zijn gekomen om burgers in staat te stellen zich te verweren tegen overheidshandelingen waarbij die data mogelijk ten onrechte gebruikt worden. Dergelijke gevallen komen nu al voor, maar zullen naar verwachting veel vaker voorkomen als data door gebrek aan duidelijkheid over wie wat in het systeem gebracht heeft ontbreekt. Burgers kunnen hier ernstige en fatale gevolgen van ondervinden. Privacy First verwijst bijv. naar het geval waarbij een Nederlandse burger om onduidelijke redenen door de Spaanse overheid vastgehouden werd: <https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2023:18764>.
- Onduidelijke afbakening zal naar verwachting ook leiden tot extra informatie-uitvragen van overheidsinstanties bij meldingsplichtige entiteiten. Wij zien in het wetsvoorstel geen enkele waarborg dat overlappende informatie-uitvragen uitgesloten zijn, bijvoorbeeld door coördinatie tussen de relevante autoriteiten.
- Privacy First wijst op artikel 62 AMLD6, die vergt dat de lidstaten een lijst van bevoegde autoriteiten doorgeven aan de Europese Commissie en AMLA. Een lijst van relevante nationale autoriteiten dient dus beschikbaar te zijn.

Witwasbestrijdingsplichtigen

- AMLR maakt grootschalige gegevensdeling tussen witwasbestrijdingsplichtigen onderling en met de overheid mogelijk (vooral relevant voor de grote witwasbestrijdingsplichtigen), grotendeels op AMLR gebaseerd (artikelen 48, 75 AMLR, voor banken en betaaldienstverleners ook op PSR/PSD3 te baseren). Privacy First is gekant tegen dergelijke gegevensdeling nu dat een vorm van financiële surveillance van grote aantallen burgers en organisaties zal inhouden, zonder dat zij verdacht zijn of aannemelijk is dat zij een hoger criminaliteitsrisico vormen ('bancair sleepnet'). Zie daarover nader onder A7.
- In de praktijk worden betrokkenen¹⁵ als ze zelf geen klant zijn (bijvoorbeeld ubo's, bestuurders) door witwasbestrijdingsplichtigen, AML/CFT-datahandelaren en overheidsinstanties niet geïnformeerd over de verwerking van hun gegevens. Dat is in strijd met de AVG.
- Uitermate riskant is dat alle witwasbestrijdingsplichtigen (dus niet alleen gereguleerde partijen zoals banken) op grond van de AMLR verplicht zullen zijn om **het BSN** van klant-natuurlijke persoon en uiteindelijk begunstigten te verwerken. Verder zijn alle witwasbestrijdingsplichtigen verplicht om de complete geboortedatum en het

¹⁵ Hier wordt de 'betrokkene' in de zin van de AVG bedoeld.

woonadres van de ubo te administreren. Dit zal zeer grote risico's voor betrokkenen opleveren.

- Witwasbestrijdingsplichtigen houden er regelmatig onveilige praktijken op na als het gaat om communicatie met de klant. Zo hebben banken nog steeds niet standaard een beveiligd kanaal ten behoeve van het stellen van CDD vragen, het geven van CDD-antwoorden en het sturen van kopieën van documenten.

Toezicht en handhaving

- Het gegevensbeschermingstoezicht en -handhaving blijft achter, onder andere door capaciteitsgebrek, terwijl de risico's voor burgers exponentieel toenemen.

Commentaar:

- Privacy First adviseert u bij de Europese wetgever te verzoeken om aanpassing van de AMLR-bepalingen inzake de te verwerken persoonsgegevens door witwasbestrijdingsplichtigen. De verplichte verwerking van het BSN (/TIN) dient vanwege de risico's voor burgers beperkt te worden tot gereguleerde financiële instellingen en een selectie van relevante andere witwasbestrijdingsplichtigen (bijvoorbeeld notarissen).

Privacy First is voorts van mening dat er Nederlandse wetgeving nodig is:

- Er vindt in de lwt een heldere afbakening plaats van de actoren die gegevens mogen uitwisselen en de grondslag voor die uitwisseling. Verduidelijkt wordt dat alleen mag worden uitgewisseld als de andere partij haar gegevensbescherming aantoonbaar op orde heeft. Er vindt periodiek een risicobeoordeling van het gegevensdelingslandschap binnen de overheid plaats.
- Alle partijen in het AML/CFT-systeem, zowel de overheid als de witwasbestrijdingsplichtigen, zijn verplicht om interne mechanismen te creëren om risico's van onder andere risicoprofilering en algoritmische analyse te signaleren. Dit omvat bij de overheid zowel FIU NL, de toezichthouders, als alle partijen waarmee zij op grond van de lwt of andere regelgeving gegevens mogen delen.
- In de lwt wordt opgenomen dat zover AI wordt ingezet, wordt aangesloten bij de werkwijzen die op grond van de AI Act verplicht zijn. Van die mechanismen maakt een FRIA deel uit. Voorts dient bij het inzetten van AI bij risicoprofilering sprake te zijn van een risicomanagementverplichting tijdens de *life cycle* van de software, een onafhankelijke conformiteitsbeoordeling, penetratietesten, hackathons en dergelijke.
- Alle witwasbestrijdingsplichtigen dienen verplicht te zijn een beveiligd kanaal ter beschikking te stellen voor de gegevensuitwisseling met klanten in het kader van het CDD. Dit geldt ook als de klant door een gemachtigde of advocaat wordt vertegenwoordigd.
- Het door witwasbestrijdingsplichtigen verplichtstellen van gebruik van de EUDI-wallet ten behoeve van de verificatie van de identiteit wordt wettelijk verboden. De EUDI-wallet

moet vrijwillig blijven – in lijn met wat de Nederlandse wetgever heeft toegezegd – en mag niet de keuze beperken.

- Een systeem van periodieke audits op de gegevensverwerking dient verplicht te worden gesteld, zowel bij alle witwasbestrijdingsplichtigen als bij FIU en de toezichthouders. De resultaten van de onderzoeken bij de AML/CFT actoren uit de overheid worden openbaar gemaakt. Er worden consequenties verbonden aan tekortkomingen, zoals het tijdelijk stopzetten van informatieverwerking voor bepaalde doeleinden.
- Er wordt een recht gecreëerd om het optreden van een witwasbestrijdingsplichtige te laten toetsen door de financiële ombudsman.
- Betrokkenen behoren door iedereen die hun gegevens verwerkt direct en zonder dat zij er om verzoeken geïnformeerd te worden, behoudens bijzondere omstandigheden.¹⁶ Bij bijzondere omstandigheden gebeurt het op een later tijdstip, behoudens beperkte uitzonderingen.
- Er komt een onafhankelijk systeem van signalering van fouten en onvolkomenheden bij gegevensverwerking in het kader van AML/CFT, dat ook meldingen door medewerkers van witwasbestrijdingsplichtigen, klanten en andere betrokkenen (zoals ubo's, bestuurders) mogelijk maakt. De opzet kan vergelijkbaar zijn aan het klokkenluiderssysteem.
- Er dient een vergunningplicht te komen voor de datahandel in de witwasbestrijding en financiële sector, inclusief personentoetsing en toetsing van technische systemen. Ook de datahandelaar Bureau Kredietregistratie (BKR) zal in dit vergunningensysteem worden opgenomen, zoals wij al eerder hebben voorgesteld in de consultatie over het BKR.
- Misbruik van persoonsgegevens uit de witwasbestrijding c.a. (inclusief Handelsregister / ubo-register), en het door witwasbestrijdingsplichtigen niet of niet correct naleven van de AVG wordt gehandhaafd door de antiwitwastoezichthouders in samenwerking met de Autoriteit Persoonsgegevens. Dit wordt expliciet in de Iwt geregeld.

Voorts verzoeken wij u het volgende te bewerkstelligen:

- De capaciteit van de Autoriteit Persoonsgegevens (AP) wordt flink uitgebreid, vanwege de grote risico's die het AML Package gaat opleveren. De budgetten van de AP groeien minimaal mee met de groei van de financiële AML/CFT toezichthouders. De AP gaat zo spoedig mogelijk audits uitvoeren bij FIU NL en de AML/CFT-toezichthouders en maakt de resultaten daarvan openbaar.

¹⁶ Bijvoorbeeld als een misdadavermoeden wordt gemeld.

A5. Openbaarmaking van persoonsgegevens via het ubo-register

Achtergrond:

- Witwasbestrijdingsplichtigen zijn verplicht grote hoeveelheid gegevens over hun klant-natuurlijke persoon en over de uiteindelijk begunstigden (ubo's) van hun klanten die geen natuurlijke persoon zijn te verzamelen. Een zeer grote groep mensen is of wordt ubo, niet alleen mensen met een economisch belang bij een entiteit maar ook mensen met 'zeggenschap', zoals statutair bestuurders en het hoogste management (topfunctionarissen).¹⁷
- Appartementseigenaren van kleine VvE's komen mogelijk in het ubo-register en via de naam van de VvE kan hun adres worden achterhaald. Bij die kleine VvE's kunnen aan de hand van het adres, dat in de naam van de VvE zit, via het ubo-register de personalia van de appartementseigenaren worden achterhaald. Dit is ongewenst en maakt het nodig dat er maatregelen worden genomen.
- Er is sprake van grootschalige gegevensuitwisseling tussen renseigneringsplichtigen (onder andere financiële instellingen en cryptovaluta aanbieders) en de overheid, waarbij ook ubo's moeten worden doorgegeven. Deze gegevens worden ook internationaal tussen overheden uitgewisseld. De ubo-gegevens worden onder andere internationaal uitgewisseld via het Europese ubo-register BORIS, waartoe het publiek toegang zal krijgen.
- Een belangrijk deel van de private partijen die toegang krijgen tot het ubo-register en BORIS worden niet op integriteit getoetst (onder andere datahandelaren, een deel van de witwasbestrijdingsplichtigen, journalisten en non-profit-organisaties).

Commentaar:

Vanwege de verhoging van de risico's voor ubo's, zijn naast de algemene versterking van het gegevensbeschermingstoezicht, extra maatregelen nodig:

- Alle private partijen en personen die toegang krijgen tot het ubo-register, dienen op integriteit te worden getoetst, ook de witwasbestrijdingsplichtigen die niet tot een gereguleerde beroepsgroep behoren.
- Iedere ubo moet onmiddellijk worden geïnformeerd over elke private raadpleging van het register. Dit moet in de Nederlandse wet worden vastgelegd. Op die manier kan een ubo controleren of op juiste gronden het register is geraadpleegd en of de gegevens op juiste gronden worden verwerkt.
- VvE's moeten worden uitgezonderd van de ubo-register plicht. Voor zover dat niet mogelijk zou zijn dient de Nederlandse regering op aanpassing van AMLR aan te dringen,

¹⁷ Een statutair bestuurder kan 'zeggenschaps'-ubo zijn dan wel pseudo-ubo. In het laatste geval zijn ook topfunctionarissen ubo.

dan wel moeten andere maatregelen worden genomen, waarvan de kosten door de overheid worden gedragen.

A6. Rechtsbescherming en optreden tegen grondrechtenschendingen

Achtergrond:

- Op dit moment ontbreekt een volwassen rechtsbescherming tegen het optreden van witwasbestrijdingsplichtigen en de overheidspartijen in de AML/CFT. Witwasbestrijdingsplichtigen hoeven geen verantwoording af te leggen over hun optreden, zie de uitspraak inzake onterechte blokkering door bunq van een rekening: <https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2024:14477>.
- Financiële instellingen (FI's) blokkeren soms zonder vooraankondiging of met onvoldoende vooraankondiging de bankrekening. Soms zijn de FI's niet bereikbaar voor de klant en ontstaat schade (voorbeeld: een bedrijf kan niet aan de salarisbetalingsverplichtingen voldoen).
- Witwasbestrijdingsplichtigen worden niet vervolgd wegens grondrechtenschendingen. Zij komen weg met het aanbieden van excuses.
- De in het consultatievoorstel vermelde grondrechtenfunctionaris van FIU-Nederland heeft onvoldoende bevoegdheden.
- Ook bij andere instanties is het gewenst een grondrechtenfunctionaris aan te stellen.

Commentaar:

- Wij adviseren te komen tot de oprichting van een financiële ombudsman die ook optreedt in AML/CFT zaken in verband met alle soorten witwasbestrijdingsplichtigen. De bevoegdheid van de ombudsman kan worden beperkt tot natuurlijke personen, mkb en kleine en middelgrote non-profit organisaties. Eventueel kan dit ook worden bereikt door de bevoegdheden van de Nationale Ombudsman uit te breiden.
- Er wordt laagdrempelige toegang tot de onafhankelijke rechter gecreëerd voor natuurlijke personen, mkb en kleine en middelgrote non-profits, bijvoorbeeld bij de kantonrechter. Het Kifid wordt opgeheven.
- Er komt een onafhankelijk kennisinstituut dat tegenwicht biedt aan het groepsdenken van de financiële sector en de overheid.
- De positie van de grondrechtenfunctionaris van FIU NL dient beter geborgd te worden door middel van onder andere wettelijke minimumeisen voor onafhankelijkheid, benoemingstermijn, middelen, mandaat en ontslagbescherming, waarvoor de basis in de Iwt dient worden opgenomen. De grondrechtenfunctionaris krijgt de bevoegdheid niet-naleving te melden bij de financiële ombudsman, AP en het College voor de Rechten van de Mens.

- Ook bij andere grote organisaties wordt het instellen van een grondrechtenfunctionaris met bevoegdheden verplicht (onder andere Belastingdienst/FIOD, alle grootbanken, het landelijk Bibob bureau).
- Het wordt financiële instellingen verboden om rekeningen te blokkeren, tenzij [a] de blokkering tijdig is aangekondigd en de financiële instelling de ontvangst van de aankondiging kan aantonen, [b] de financiële instelling bereikbaar is via een noodnummer of andere noodvoorziening, zodat de klant de financiële instelling kan bereiken en schade voor de klant kan worden voorkomen; [c] de noodzaak voor blokkering door de financiële instelling wordt aangetoond (het nog niet afronden van het CDD is nooit een reden voor blokkering, behoudens nauwkeurig omschreven uitzonderingen).

A7. Gegevens delen door witwasbestrijdingsplichtigen (artikel 75 AMLR) en uitbesteding

Achtergrond:

- De nieuwe Europese regelgeving zal mogelijk maken dat grote witwasbestrijdingsplichtige ondernemingen (waarschijnlijk met name de banken) kunnen samenwerken op het gebied van klantenonderzoek en transactiemonitoring door middel van *artificial intelligence*. Dit zal naar verwachting zijn gebaseerd op het AMLR-artikel over uitbesteding en het AMLR-artikel over 'partnerschappen' (artikel 75 AMLR).¹⁸ De nieuwe regels van het Payment Package (PSD3 en PSR) bevatten gelijksoortige mogelijkheden voor banken en betaaldienstverleners. Deze samenwerking is toegestaan in een groot aantal situaties, onder andere bij 'hoog risico klanten' ¹⁹ en zal om zeer veel gegevens gaan.²⁰
- Nu in de Nederlandse NRA's witwassen en terrorismefinanciering het hele betalingsverkeer via banken en betaaldienstverleners als hoog risico is aangemerkt, is het mogelijk voor de banken om het hele betalingsverkeer door middel van artikel 75 AMLR te gaan monitoren.
- De AI-industrie is al druk bezig met het aanprijzen van de AML/CFT producten en uit Europese publicaties blijkt dat men daar een heilig geloof heeft in IT.

¹⁸ De consultatietoelichting spreekt ook over artikel 48 AMLR, gebruikmaken van het CDD door andere witwasbestrijdingsplichtigen. Dit is iets wat ons alleen voor de grote ondernemingen geschikt lijkt.

¹⁹ Zie het artikel van Alexandra Pagnier-Desbois en Célie Allagnat, *Information sharing partnerships under the new AML/CFT and upcoming Payment Services packages (AML 27/03/2025). Balancing the fight against financial crime with the fundamental right to personal data protection*, verschenen in Bank- en Financieel Recht / Droit bancaire et financier, 2025/6 – 10 april 2025, te raadplegen via https://www.stradalex.com/en/sl_rev_utu/toc/dbf_bfr_2025_6-en/doc/dbf_bfr2025_6p1. Zij constateren dat de reikwijdte van de groep klanten die kan worden onderzocht zeer ruim is, zie paragraaf 2.2.2.

²⁰ Zie paragraaf 4.1 van het artikel van Pagnier-Desbois en Allagnat.

- De banken zijn enige tijd geleden een samenwerkingsverband onder de naam Transactie Monitoring Nederland (TMNL) gestart, dat naar aanleiding van kritiek is gestopt en nu bezig is met het voorbereiden van een herstart onder de nieuwe regels, zie **bijlage 2** voor nadere informatie.

Commentaar:

- Er moet nu al in de Iwt een wetgevend kader worden gecreëerd inzake de toekomstige samenwerking op grond van artikel 75 AMLR en de bepalingen van PSR/PSD3, waarin aanvullende strenge eisen aan die samenwerking worden gesteld, zodat er geen bancaire sleepnet kan ontstaan.
- De 'gespecialiseerde entiteiten' aan wie kleinere witwasbestrijdingsplichtigen hun antiwitwasverplichtingen kunnen uitbesteden ²¹ wordt vergunningplichtig (systeem inclusief integriteitstoetsing beleidsbepalers c.s., toetsing digitale systemen en dergelijke).

NB: het bovenstaande houdt niet in dat Privacy First instemt met artikel 75 AMLR of andere bepalingen van Europees of Nederlands recht die kunnen leiden tot financiële surveillance zonder gerichte verdenkingen.

A8. Open finance verbod

Achtergrond:

- Op dit moment zijn er al private partijen die klanten verplichten om hun bankrekening open te stellen, zie de berichtgeving over verhuurders die toegang tot de bankrekening vragen via *open banking*. De staatssecretaris van Justitie en Veiligheid gaf recent aan ²² dat de Kansspelautoriteit kansspel aanbieders heeft geadviseerd dat zij hun

²¹ Zie de toelichting: "Door middel van uitbesteding krijgen de meldingsplichtige entiteiten, in het bijzonder de kleinere, de mogelijkheid om gebruik te maken van de expertise en doeltreffendheid van gespecialiseerde entiteiten, waardoor ze hun naleving doeltreffender kunnen uitvoeren en tegelijkertijd hun efficiëntie kunnen verbeteren. Hierbij kan bijvoorbeeld gedacht worden aan om transacties te laten monitoren of de risico's van een cliënt te laten analyseren door een gespecialiseerde partij."

²² Brief staatssecretaris van Justitie en Veiligheid d.d. 3 juli 2025, 24557-273, https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2025D32045&did=2025D32045.

draagkrachttoets mogen baseren op toegang tot de bankrekening van de speler.²³ Dit is een klassiek voorbeeld van *function creep*.

- De verleiding van witwasbestrijdingsplichtigen zal groot zijn om van hun klanten toegang tot de bankrekening te eisen. Die verleiding moet de weg worden afgesneden.

Commentaar:

- Neem in de lwt een verbod op tot het dwingen van de klant via *open finance* toegang te verlenen tot bankrekeningen en spaarrekeningen.
- Een zelfde verbod wordt opgelegd aan overheidsdiensten, bijvoorbeeld als toegang wordt gevraagd in het kader van subsidieverlening.

A9. Verwijzingsportaal banken

Achtergrond:

- De toelichting bij het wetsvoorstel vermeldt dat aangaande het Verwijzingsportaal banken ('het Portaal') al voldaan is aan artikel 16, eerste lid, van AMLD6. Dit onderdeel van AMLD6 vergt een voorziening om (louter) identificatie van bepaalde rekeninghouders (bijvoorbeeld bankrekeninghouders) mogelijk te maken in het kader van het tegengaan van witwassen en terrorismefinanciering in de zin van AMLD6. Dat laatste wil zeggen witwassen verbandhoudend met de limitatieve lijst (ernstige) basisdelicten uit AMLR. Het huidige Portaal gaat veel verder dan AMLD6 vergt en vormt (verregaande) *goldplating*. Een behoorlijk aantal instanties heeft toegang tot het Portaal, terwijl zij geen rol spelen bij het tegengaan van witwassen en terrorismefinanciering en de toegang dus voor hele andere doeleinden is gegeven. Zo heeft de Belastingdienst op grond van art. 62bis Invorderingswet 1990 bijv. toegang tot het Portaal om betalingen te kunnen koppelen aan te vorderen bedragen (reconciliatie). Het Portaal wordt hiermee ingezet om de bedrijfsvoering van de Belastingdienst te vergemakkelijken en is niet gerelateerd aan enig doel onder de AMLR of AMLD6. Ook instanties als de Arbeidsinspectie hebben geen rol bij witwasbestrijding.

²³ "Naar aanleiding daarvan heeft de Ksa nadere invulling gegeven aan de draagkrachttoets die aanbieders sinds 1 oktober 2024 moeten uitvoeren bij spelers die meer willen storten dan 700 euro (vanaf 24 jaar) of 300 euro (jongvolwassenen van 18 tot 24 jaar) (...) Daarbij dient gebruik te worden gemaakt van objectieve bewijsstukken, zoals salarisstroken, aangiften inkomstenbelasting of open banking toepassingen".

- Privacy First is bekend met voornemens om de inhoud van het Portaal uit te breiden, zodat aangesloten instanties voortaan ook volautomatisch toegang krijgen tot alle saldo- en betaalgegevens van rekeninghouders en het e-mailadres, het mobiele telefoonnummer en het International Mobile Equipment Identity number (IMEI-nummer) van het mobiele telefoontoestel dat de rekeninghouder gebruikt om zijn zaken mee te regelen. Ook zijn er voornemens om de toegang tot het Portaal te verruimen met onder andere het Centraal Justitieel Incassoburo (CJIB) en deurwaarders. De voorgenomen uitbreiding is op geen enkele manier gerelateerd aan AMLD6 of AMLR.
- AMLD6 bepaalt dat gecentraliseerde automatische mechanismen als bedoeld in artikel 16 van AMLD6 onderling worden verbonden via het koppelingssysteem voor registers van bankrekeningen (bank account registers interconnection system – BARIS) dat door de Commissie moet worden opgezet en beheerd. De lidstaten moeten ervoor zorgen dat alleen de in de Richtlijn bedoelde informatie beschikbaar komt via BARIS.
- Privacy First meent dat het duidelijk is dat de inrichting van het huidige Portaal aangepast zal moeten worden en dat het zeker niet voor de hand ligt om het Portaal uit te breiden. Het consultatievoorstel maakt niet duidelijk hoe het Portaal, inclusief de uitbreidingsplannen, zich verhouden tot AMLD6 en de wens tot harmonisatie in het algemeen.

Commentaar:

- Privacy First verzoekt om de wetgeving inzake het Portaal door middel van de Iwt aan te passen naar hetgeen vereist is onder AMLD6 en nationale mogelijkheden die verder gaan dan vereist is te schrappen.

A10. Schrappen bestaande nationale regels die afwijken van de EU-regels

Achtergrond:

- Het AML Package gaat zorgen voor zeer veel nieuwe regels. Dit dient reden te zijn voor het schrappen of beperken van bestaande regels, zoals de *Wet gegevensverwerking door samenwerkingsverbanden* (WGS).
- AMLR en AMLD6 beogen harmonisatie. Met het oog op harmonisatie zou implementatie óók moeten betekenen dat de Ministers een analyse maken van bestaande, afwijkende of overlappende regels die witwassen en terrorismefinanciering beogen tegen te gaan. Regels die afwijken van of verder gaan dan de EU-regels zouden hierbij geschrapt moeten worden. Als dit niet gebeurt, is geen sprake van harmonisatie maar van stapeling van nationale regels op Europese regels. Serieuze harmonisatie wordt dan nooit bereikt. Privacy First roept de Ministers op werk te maken van het schrappen van nationale regels. Ook is het noodzakelijk duidelijk te maken hoe deze wet 'past' op bestaande regels. Wij geven hieronder een paar voorbeelden waar aandacht aan besteed dient te worden, maar benadrukken dat de voorbeelden niet uitputtend zijn. Er

zijn veel gevallen van overlap en samenloop te bedenken. Het is aan de wetgever een complete analyse te maken.

- Onder de Politiewet kunnen gegevens afkomstig van de FIU niet zomaar gebruikt worden door de opsporingsdiensten voor 'andere doeleinden' dan waarvoor de gegevens door de FIU-Nederland zijn verstrekt. Hoe verhouden de regels onder de Politiewet zich tot het voorgestelde artikel 5.6 lwt dat de FIU en toezichthouders gegevens aan de politie kunnen verstrekken?
- Op dit moment is het wetsvoorstel tot implementatie van de Confiscatierichtlijn in consultatie, zie <https://www.internetconsultatie.nl/implementatieconfiscatierichtlijn/b1> (de 'afpakwet'). Op grond van dit voorstel mag vermogen worden afgepakt (geconfisqueerd) zonder dat de eigenaar is veroordeeld voor een strafbaar feit. Hoe verhouden deze richtlijn en de daarop gebaseerde afpakwet zich tot AMLR en AMLD6?
- Voor het Verwijzingsportaal banken verwijzen we naar A9.
- Voor zover er nationaal afwijkende regels zijn, dienen deze te verdwijnen.

Commentaar:

- Privacy First stelt voor om alle regels inzake gegevensverwerking door samenwerkingsverbanden voor zover het AML/CFT betreft in de lwt op te nemen. De samenwerkingsverbanden inzake AML/CFT gebaseerd op de WGS worden opgeheven.
- Wij adviseren na te gaan of de WGS nog reden van bestaan heeft als de WGS geen gegevensdeling voor AML/CFT-doeleinden meer omvat. Als het belang beperkt is, trek de wet dan in of beperk het tot het minimale.
- Privacy First adviseert te inventariseren welke nationale regels afwijken van AMLR/AMLD6 en deze te schrappen.
- Wij verzoeken u om toe te lichten hoe artikel 5.6 lwt zich verhoudt tot de doelbepaling in de Politiewet en om ook aandacht te besteden aan andere aanpalende wetgeving, zoals de afpakwet.

B. Detailonderwerpen uit het voorstel voor de lwt

Artikel 1.3 lid 2 lwt – nieuwe verordeningen inzake AML/CFT

Achtergrond:

- In artikel 1.3 lid 2 lwt wordt vooruitgelopen op antiwitwasverordeningen waarvan de inhoud nog niet bekend is.

Commentaar:

- Vanwege de grote maatschappelijke gevolgen van de AML/CFT-regels, acht Privacy First het ongewenst dat op nieuwe verordeningen op dat terrein wordt vooruitgelopen zonder dat de inhoud bekend is. Wij adviseren deze bepaling te laten vervallen.

Hoofdstuk 3 – de governance van FIU NL

Achtergrond:

- Vanwege de rol die FIU NL speelt in het AML/CFT systeem en de vele ingrijpende bevoegdheden, is een krachtige governance nodig. In het huidige hoofdstuk 3 lwt is dat onvoldoende geregeld. Zo dienen er waarborgen te zijn inzake de onafhankelijkheid van de FIU en dient de benoeming van het hoofd van de FIU niet politiek te zijn. De Egmont groep heeft die onafhankelijkheidseisen toegelicht in deze paper https://egmontgroup.org/wp-content/uploads/2021/09/2018_Understanding_FIU_Operational_Independence_and_Autonomy.pdf.
- In de meest recente audit van de FIU NL was veel kritiek op de inrichting van de FIU NL. Wij verwijzen naar de 'Uitkomsten quick scan verantwoordingsdocument Waarborgen taakscheiding FIU' dat te vinden is via: <https://zoek.officielebekendmakingen.nl/kst-29911-306.html>.
- In de lwt ontbreekt een regeling die het mogelijk maakt dat burgers en organisaties FIU NL aanspreken op de wijze waarop FIU NL haar taken uitoefent, voor zover dat invloed heeft op de rechtspositie en grondrechten van burgers en organisaties.
- Op grond van artikel 3.2 lwt krijgt FIU NL nagenoeg onbeperkte informatiebevoegdheden, zij heeft toegang tot omvangrijke overheidsinformatie, waaronder financiële, administratieve en rechtshandavingsinformatie en kan voorts informatie opvragen bij witwasbestrijdingsplichtigen. De afbakening in artikel 3.2 is zeer vaag, terwijl de inlichtingen in kwestie in de regel persoonsgegevens zullen omvatten. Privacy First merkt op dat de EDPS (EDPS Opinion 12/2021 via https://www.edps.europa.eu/system/files/2021-09/21-09-22_edps-opinion-aml_en.pdf) in een eerder stadium al heeft aangegeven dat het noodzakelijk is om duidelijk te definiëren tot welke informatie de FIU toegang zal

hebben. De noodzakelijke afbakening ontbreekt echter in dit wetsvoorstel. Dit geldt ook in relatie tot andere overheidsinstanties.

- De positie van de grondrechtenfunctionaris is onvolkomen, zie ons eerdere commentaar onder A6.

Commentaar:

Privacy First verzoekt de wetgever meer aandacht te besteden aan de inrichting van de FIU en onder meer in de lwt op te nemen:

- De benoeming van het hoofd van FIU NL zal geen politieke benoeming zijn en in de lwt worden nadere regels opgenomen inzake de onafhankelijkheid van het hoofd van FIU NL en van FIU NL zelf. Wellicht dient FIU NL een zelfstandig bestuursorgaan met een volwassen governance te worden.
- Er wordt een regeling getroffen inzake de wijze waarop FIU NL kan worden aangesproken op haar handelswijze, voor zover dat invloed heeft op de rechtspositie en grondrechten van burgers en organisaties.
- In de lwt wordt nader afgebakend tot welke informatie FIU NL en de andere overheidsinstanties toegang hebben. Dit gebeurt op hoofdlijnen in de lwt, eventueel nader uit te werken in een algemene maatregel van bestuur.
- FIU NL wordt vóórdat zij nieuwe bevoegdheden op grond van de lwt kan uitoefenen verplicht geaudit door de Auditdienst Rijk en de auditrapporten worden openbaar gemaakt. Vervolgens wordt FIU NL periodiek, bijvoorbeeld om de drie jaar, geaudit.

Artikel 3.6 lwt – Opschorting van transacties in opdracht van FIU-Nederland

Achtergrond:

- De FIU krijgt in artikel 3.6 lwt de bevoegdheid om witwasbestrijdingsplichtigen op te dragen dat transacties of de zakelijke relatie moet worden opgeschort. Dit is mogelijk *"indien een vermoeden bestaat dat de transactie of transacties, rekening of zakelijke relatie verband kan of kunnen houden met witwassen of financieren van terrorisme of indien een financiële-inlichtingeneenheid uit een andere staat hierom verzoekt"*. Toetsing van het verzoek van de buitenlandse FIU (kan ook van buiten de EU zijn!) vindt niet plaats.
- De klant wordt alleen op diens verzoek geïnformeerd (lid 8). De FIU en haar bestuurders en werknemers zijn niet aansprakelijk voor schade (lid 9).
- Een gelijksoortige bevoegdheid staat in het wetsvoorstel versterking strafrechtelijke aanpak ondermijnende criminaliteit II. Lid van de Tweede Kamer Six Dijkstra had in een amendement <https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2025D29004&did=2025D29004> kritiek op dat voorstel, kritiek die door Privacy First wordt gedeeld. Het Tweede Kamerlid schreef:

Indiener is kritisch op de toenemende push-button power of drukknopmacht van de staat. De digitale transformatie van de samenleving heeft ertoe geleid dat de overheid op veel vlakken veel machtiger tegenover haar burgers staat dan in het verleden überhaupt technisch mogelijk was, bijvoorbeeld als het gaat om het kunnen controleren en blokkeren van financiële geldstromen van burgers. Ook heeft de beschikbaarheid en inzet van digitale technologie geresulteerd in scheefgroei van de machtsverdeling binnen de trias politica, daar dit de macht van de regering ten opzichte van de rechtspraak en het parlement onevenredig vergroot heeft [*]. Indiener is derhalve van mening dat drukknopmacht enkel uitgebreid zou moeten mogen worden wanneer hier volwaardige rechtsstatelijke waarborgen tegenover staan.

Hoe dit in een westerse democratie mis kan gaan, is onder andere gebleken bij de zogeheten trucker protests in Canada in 2022, een reeks coronademonstraties naar aanleiding waarvan de Canadese premier de noodtoestand had uitgeroepen. Hierbij droeg hij banken op om eigenstandig de rekeningen te bevriezen van personen die deelnamen aan deze demonstraties, dan wel van personen die deelnemers financieel ondersteunden. Dit vond plaats zonder verdere controlemechanismen die konden voorkomen dat mensen onterecht niet bij hun financiële middelen konden komen. Achteraf heeft de Canadese rechtbank geoordeeld dat het handelen van de premier niet gerechtvaardigd was in relatie tot de relevante feitelijke en juridische beperkingen die in aanmerking hadden moeten worden genomen. Indiener is van mening dat dergelijk ingrijpend en disproportioneel regeringsoptreden zeer schadelijk is voor het vertrouwen van burgers in de overheid. Het is daarom zaak om vergelijkbare situaties in Nederland te voorkomen.

Onder voorliggend wetsvoorstel ligt de juridische drempel voor het kunnen blokkeren van een transactie met het hoeven aantonen van een aanwijzing voor een verband met witwassen of terrorismefinanciering door de FIU, relatief laag. Er is daarnaast geen externe toestemmings- of toetsingsprocedure ingeregeld voor de inzet van deze bevoegdheid door de FIU. Vanuit het perspectief van snel en wendbaar kunnen acteren op ondermijnende criminaliteit is deze keuze volstrekt begrijpelijk. Echter, wanneer een transactie vijf werkdagen lang onterecht bevroren blijft, kan dit voor veel burgers ingrijpende gevolgen hebben, bijvoorbeeld als deze vijf werkdagen de periode tussen het storten van het salaris en het betalen van de huur beslaat.

In het kader van rechtszekerheid stelt indiener voor om banken te verplichten om de rekeninghouder actief en binnen 24 uur te informeren over het feit dat gevolg is gegeven aan een eis van de FIU. Dit stelt de rekeninghouder in staat om tijdig stappen te ondernemen indien hij denkt dat een transactie onterecht is bevroren. Dit versterkt in de ogen van indiener de rechtspositie van de burger ten opzichte van de overheid.

[*] Zie bijvoorbeeld: R. Passchier, *Artificiële intelligentie en de rechtsstaat* (2021)

- In de praktijk komt nu al voor dat banken ingekomen betalingen vasthouden zonder de klant te informeren.
- Deze bevoegdheid dient met waarborgen te worden omgeven, om te voorkomen dat grondrechten geschonden worden en het vertrouwen in de rechtsstaat ondergraven.

Commentaar:

- In de lwt wordt opgenomen dat ook voor verzoeken van buitenlandse FIU's (van binnen en buiten de EU) dient te gelden dat er een aantoonbaar criminaliteitsvermoeden is en de gegevensbescherming aantoonbaar op orde is.
- Wij adviseren op te nemen dat de rekeninghouder / klant onmiddellijk over toepassing van artikel 3.6 lwt wordt geïnformeerd, tenzij er bijzondere omstandigheden zijn.
- Het is banken niet toegestaan om inkomende betalingen of uitgaande betalingen vast te houden, tenzij sprake is van toepassing van artikel 3.6 lwt. In alle gevallen wordt de klant onmiddellijk door de bank geïnformeerd.
- FIU NL richt een laagdrempelige, snelle en effectieve bezwaarprocedure in zodat geraakte burgers de schorsing kunnen aanvechten. Aanvullend wordt laagdrempelige rechtsbescherming gecreëerd via de kantonrechter en financiële ombudsman, zoals elders al opgemerkt. Het is onvoldoende dat de mogelijkheid van een civiele procedure achteraf bestaat (zie de consultatietoelichting ²⁴) aangezien dit alleen voor kapitaalkrachtige klanten een haalbare kaart is en de schorsing niet kan opheffen.
- Schade als gevolg van een onterechte toepassing van artikel 3.6 lwt dient te worden vergoed door de Nederlandse Staat: er dient tenminste een wettelijke regeling te worden getroffen ten behoeve van natuurlijke personen, mkb en kleine en middelgrote non-profit-organisaties.
- Artikel 3.6 lid 9 lwt dient te vervallen.

Artikel 2.3 lwt – Personentoetsing bij alle witwasbestrijdingsplichtigen

Achtergrond:

- In artikel 2.3 lid 1 lwt wordt voorgesteld dat een betrouwbaarheidstoetsing moet plaatsvinden bij alle witwasbestrijdingsplichtigen, dit omvat de leden van het hoger leidinggevend personeel en de uiteindelijk begunstigde. De voormelde personen mogen

²⁴ "Dit laat onverlet dat een cliënt wiens transactie, bank-, betaal- of cryptoactivarekening of zakelijke relatie is opgeschort een rechterlijke (civiele) procedure kan starten op grond van een onrechtmatige overheidsdaad, als deze van oordeel is dat de FIE niet rechtmatig heeft gehandeld bij de toepassing van de opschorting".

ook niet 'geassocieerd' zijn met personen die veroordeeld zijn voor witwassen, daarmee verbandhoudende basisdelicten of terrorismefinanciering. Het begrip 'geassocieerd' wordt niet toegelicht. De in artikel 2.3 lid 1 lwt beschreven toetsing wordt niet voorgeschreven door artikel 6 lid 2 AMLD6. Daar staat alleen dat voorkomen wordt dat iemand leidinggevend of uiteindelijk begunstigde is en veroordeeld is.

- De toetsing is achteraf, maar zal allerlei nieuwe regeldruk opleveren terwijl de gevolgen onduidelijk zijn. Aan welke standaard worden betrokkenen gehouden? Wat zijn de gevolgen als men afgetoetst wordt? Komt betrokkene dan op een zwarte lijst?
- Screening hoort alleen bij aangetoonde noodzaak plaats te vinden. Als zich in bepaalde bedrijfssectoren specifieke problemen voordoen, kan er voor die sectoren eigen regelgeving worden gecreëerd (zoals bij trustkantoren is gebeurd). Een generieke personentoetsing is naar de mening van Privacy First buitenproportioneel.

Commentaar:

- Privacy First adviseert artikel 2.3 te vervangen door een bepaling inhoudend dat een witwasbestrijdingsplichtige er voor zorgdraagt dat leidinggevend en uiteindelijk begunstigde niet veroordeeld zijn voor de aangegeven delicten en voorts te bepalen dat de witwasplichtige op eerste verzoek van de toezichthouder de VOG / VOG s moet overleggen van de relevante personen. Verder kan het aan de witwasbestrijdingsplichtige worden overgelaten om maatregelen te nemen.

Artikel 2.4 – Verscherpt cliëntenonderzoek voor aanbieders van trustdiensten of vennootschapsrechtelijke diensten

Achtergrond:

- Artikel 2.4 lwt schrijft niet alleen verscherpt cliëntenonderzoek voor aan trustkantoren. De verplichting van artikel 2.5 lwt omvat alle ondernemingen onder de definitie van "trustdiensten of vennootschapsrechtelijke diensten" van artikel 3, punt 3, onder c AMLR. Een verscherpt cliëntenonderzoek heeft tot gevolg dat er veel extra persoonsgegevens worden verzameld en wordt alleen gerechtvaardigd door een onderbouwde noodzaak.
- Deze groep omvat niet alleen trustkantoren in de zin van de Wtt 2018 maar ook – aldus artikel 2 lid 1 onder 11) sub c) AMLR – *"het verstrekken van een statutaire zetel, bedrijfsadres, correspondentieadres of administratief adres, alsmede andere daarmee samenhangende diensten"* aan klanten. Verhuurders van bedrijfsruimte vallen hier onder. Iedere zzp'er, mkb onderneming of nonprofit organisatie die bedrijfsruimte huurt kan hier mee te maken krijgen en wordt als 'hoog risico' klant behandeld. Privacy First ziet niet dat de noodzaak hiervan wordt onderbouwd.
- Er dient nader beoordeeld te worden welke andere ondernemingen, die geen trustkantoor als bedoeld in de Wtt 2018 zijn maar ook onder artikel 2 lid 1 onder 11) AMLR vallen, per definitie hoog risico klanten zouden hebben. In de toelichting op de bepaling is die onderbouwing niet te vinden.

- De AMLR en AMLD6 schrijven niet voor dat er van moet worden uitgegaan dat de diensten als bedoeld in artikel 2 lid 1 onder 11) AMLR per definitie aan hoog risico klanten worden verleend. In ieder geval acht Privacy First het onzinnig dat een zzp'er die een bedrijfsruimte huurt en daar zijn bedrijfsadres vestigt als hoog risico klant wordt aangemerkt.

Commentaar:

- Nu AMLR niet voorschrijft dat alle klanten van trustkantoren per definitie hoog risico zijn, is artikel 2.4 lwt een 'nationale kop' waarvan beoordeeld moet worden of deze kan worden gehandhaafd. Privacy First adviseert – ter voorkoming van onnodige verwerking van persoonsgegevens – deze bepaling volledig te schrappen en de risicobeoordeling aan de betrokken ondernemingen over te laten.
- Privacy First acht het ongewenst dat verhuurders van bedrijfsruimte onder de werking van artikel 2.4 lwt worden gebracht, alleen al vanwege het feit dat zij dat verscherpte cliëntenonderzoek niet kunnen uitvoeren. De toepasselijkheid van artikel 2.4 lwt op verhuurders en bedrijfsverzamelgebouwen zal zzp'ers en andere kleine klanten schaden en zal zorgen voor disproportionele verzameling van persoonsgegevens.
- Andere ondernemingen als bedoeld in artikel 2 lid 1 onder 11) AMLR (die geen trustkantoor of verhuurder van bedrijfsruimte zijn) dienen alleen onder een bepaling als artikel 2.4 lwt te worden gebracht als zij aantoonbaar uitsluitend hoog risico klanten hebben.

Artikel 3.13 – Verschillende definities basisdelicten

Achtergrond:

- In artikel 3.13 van het consultatievoorstel staat:
Verschillen in wettelijke definities van basisdelicten vormen geen belemmering voor de Financiële-inlichtingeneenheid om bijstand te verlenen aan andere financiële-inlichtingeneenheden en beperken de uitwisseling, de verspreiding en het gebruik van informatie op grond van de artikelen 3.9, 3.11 en 3.12 niet.
- Dit mag echter niet betekenen dat de Nederlandse overheid assistentie verleent aan landen die informatie vragen in verband met iets dat daar strafbaar is en in Nederland niet, terwijl de strafbaarstelling in Nederland niet-acceptabel wordt geacht, bijvoorbeeld bij de verkoop van softdrugs. Dit kan niet alleen aan de orde zijn bij landen buiten de EU, maar kan ook in de EU spelen (bijvoorbeeld als de AfD in Duitsland aan de macht komt).

Commentaar:

- Neem in artikel 3.13 lwt op dat deze bepaling niet van toepassing is als de buitenlandse strafbaarstelling in strijd is met de Nederlandse openbare orde of met andere fundamentele Nederlandse beginselen of met de Nederlandse handhavingspraktijk.



Tot slot

Voor nadere informatie of vragen met betrekking tot bovenstaande is Privacy First te allen tijde bereikbaar op telefoonnummer 020-8100279 of per email: info@privacyfirst.nl.

Hoogachtend,
namens Stichting Privacy First,

Vincent Böhre
directeur

Bijlage 1 – De schaduwkant van de privatisering van de misdaadbestrijding

Als achtergrond voor onze consultatiedeelname is het van belang u te wijzen op de grote maatschappelijke schade die nu al het gevolg is van de privatisering van de misdaadbestrijding onder de noemer 'witwasbestrijding', bestrijding van terrorismefinanciering en bestrijding van de niet-naleving van gerichte sancties. Die schade zal – als er geen adequate wetgevende en andere maatregelen worden genomen – door de implementatie van het Europese antiwitwaspakket, het 'AML Package' nog groter kunnen worden.

Naleving grondrechten is nodig om het vertrouwen van burgers te verdienen

Effectieve witwasbestrijding vraagt om meer dan alleen regels en systemen, het vraagt ook om vertrouwen van burgers. Dat vertrouwen komt onder druk te staan wanneer banken of andere witwasbestrijdingsplichtigen zich wel strak houden aan de antiwitwasregels, maar de grondrechten van hun klanten structureel negeren. Zonder duidelijke wettelijke grenzen en toezicht op de omgang met persoonsgegevens binnen cliëntenonderzoek, ontstaat het risico dat de antiwitwasregels worden gebruikt als vrijbrief om diep in iemands privéleven te graven, zonder noodzaak of transparantie.

De problemen spelen al langer en zijn bekend

Al lange tijd is bekend dat de uitbesteding van overheidstaken aan bedrijven door middel van de antiwitwaswetgeving grote schade veroorzaakt. Inmiddels is het ook door de minister van Financiën erkend in zijn brief van 14 mei jl. (https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2025D21156&did=2025D21156). De in die brief door de minister van Financiën gedane toezeggingen zijn echter onvoldoende. Ook is Privacy First er niet van overtuigd dat de beloften van de banken om hun leven te beteren voldoende effect kunnen sorteren. De problemen zijn namelijk een gevolg van het antiwitwas-systeem zelf, dat bedrijven onder meer dwingt tot risicoprofilering van ieder van hun klanten, gebaseerd op het verzamelen van zeer veel gegevens.

In het parlement en in de media wordt er al lange tijd aandacht besteed aan de ongewenste gevolgen van privatisering van de misdaadbestrijding, zonder dat dit tot een koerswijziging aanleiding heeft gegeven. Het blijkt uit de grote aantallen parlementaire vragen over diverse excessen in de witwasbestrijding.

Media

De problemen kunnen worden afgelezen uit diverse artikelen en uitzendingen in de media, onder andere:

- Simon van Teutem, die zelf ervaring opdeed met de amateur-rechercheurs van de bank (De Correspondent), [Banken pompen miljarden in fraudebestrijding. Maar dat levert amper wat op.](#)
- Jan-Hein Strop (Follow the Money), [Ontspoorde fraudejacht van Rabobank maakt slachtoffers.](#)
- Nick de Jager (Follow the Money), [Banken zetten hun klanten vliegensvlug op een zwarte lijst: Ik werd een verbitterde klootzak.](#)
- Saar Slegers (Argos), [Zo spoorde de Rabobank terroristen op | paintball, outdoor kleding en donaties aan de moskee](#), het artikel [Rabobank discrimineerde bij klantcontroles.](#)
- Saar Slegers (Argos), [Helpt stichtingen en verenigingen heeft problemen bank dankzij doorgeschoten anti-terrorisemaatregelen.](#)
- Olivia den Hollander en Mirjam van der Puijl schreven voor Follow the Money het artikel [Zo misbruiken landen regels tegen witwassen om critici de mond te snoeren.](#)²⁵
- Allart van der Woude, [De banken en hun risicoklanten: een zaak voor de rechter.](#)
- Bart Custers, opinie over de zwarte lijsten van de verzekeraars: [Nederlandse verzekeraars spelen voor aanklager en rechter tegelijk.](#)

De klanten die problemen ondervinden

Zowel consumenten als het mkb en de nonprofit ondervinden grote hinder en schade door de privatisering van overheidstaken naar witwasbestrijdingsplichtige bedrijven. Veel klachten van consumenten over financiële instellingen komen terecht bij de geschillencommissie van de financiële sector, Kifid, maar hebben niet geleid tot veranderingen. De problemen in het mkb hadden tot gevolg dat de Nederlandse regering heeft gepleit voor het aanpakken van de problemen die zakelijke klanten ondervinden.²⁶

Diverse nonprofit organisaties hebben klachten geuit bij het ministerie van Financiën:

- Grote problemen bij bankrekeningen voor VvE's; soepeler toezicht noodzakelijk, Vereniging Eigen Huis, <https://www.eigenhuis.nl/nieuws/grote-problemen-bij->

²⁵ Het artikel maakt duidelijk dat de gegevens die bedrijven zoals banken aan de nationale meldpunten moeten leveren over vermoedelijke criminaliteit, de Financial Intelligence Units (FIU's) – in Nederland aan FIU Nederland – op ongecontroleerde manier worden uitgewisseld met buitenlandse meldpunten: "De nationale meldpunten wisselen gegevens uit, ze bepalen zelf met welke aangesloten landen. Bankgegevens bijvoorbeeld, maar ook analyses – 'financial intelligence'. Ook van burgers, organisaties en bedrijven die niet als verdacht zijn aangemerkt."

²⁶ Zie de aankondiging Aanbiedingsbrief non-paper faciliteren toegang zakelijke betaalrekeningen, <https://www.rijksoverheid.nl/documenten/kamerstukken/2025/03/20/aanbiedingsbrief-non-paper-faciliteren-toegang-zakelijke-betaalrekeningen>.

[bankrekeningen-vves](#). Op de site van VvE 010 verscheen het artikel [Banken zien VvE's vaak als criminele organisatie](#).

- Vrijwilligerswerk Nederland is al lange tijd bezig met de problemen van maatschappelijke organisaties rondom de bankrekening, zie onder andere hun bericht over de brandbrief die een aantal organisaties aan de minister van Financiën schreven, <https://www.vrijwilligerswerk.nl/nieuws+en+blogs/2106433.aspx>, problemen die nog steeds niet zijn opgelost.²⁷

Financiële instellingen hoeven aan hun klanten geen verantwoording af te leggen van hun werkwijze, zoals over de redenen en het beleid dat ten grondslag ligt aan het plotseling blokkeren van de bankrekening, zie rechtbank Den Haag 9 september 2024, <https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2024:14477>. Jan-Hein Strop (Follow the Money) schreef over deze zaak het artikel [Banken hoeven je niet te vertellen waarom je een frauderisico bent, oordeelt de rechtbank](#).

Misstanden blijken uit rapporten

Inmiddels zijn er diverse rapporten en uitingen van instanties bekendgemaakt waaruit misstanden blijken:

- In opdracht van de rijksoverheid stelde KPMG een rapport op, aankondiging rijksoverheid <https://www.rijksoverheid.nl/documenten/publicaties/2024/04/19/rapport-kmpg-en-i-o-research-naar-ervaren-discriminatie>, het rapport <https://open.overheid.nl/documenten/3c2996be-9fa9-463f-9a39-7flaa3d40c99/file>.
- Het College voor de Rechten van de Mens heeft onderzoek gedaan en publiceerde onder andere Discriminatiemonitor 2024: discriminatie door banken in beeld, <https://www.mensenrechten.nl/actueel/nieuws/2025/01/29/discriminatiemonitor-2024-discriminatie-door-banken-in-beeld>.²⁸ Het College heeft ook aan onderhavige consultatie deelgenomen met een kritisch commentaar <https://www.internetconsultatie.nl/implementatiewetervoorcomingvanwitwassenenterro-risimefinanciering/reactie/aa6a92cf-0e02-4136-83df-386881dc506b>.

²⁷ Zie ook <https://www.vrijwilligerswerk.nl/nieuws+en+blogs/2313818.aspx> en <https://www.vrijwilligerswerk.nl/PageByID.aspx?sectionID=172153&contentPageID=2313804>

²⁸ Andere publicaties: ING discrimineert twee klanten door betalingen te blokkeren en controleren vanwege niet-Nederlands klinkende naam <https://www.mensenrechten.nl/actueel/nieuws/2024/07/25/ing-discrimineert-twee-klanten-door-betalingen-te-blokkeren-en-controleren-vanwege-niet-nederlands-klinkende-naam>, ASN discrimineert klant door geen geld over te maken naar Palestina, <https://www.mensenrechten.nl/actueel/nieuws/2024/09/02/asn-discrimineert-klant-door-geen-geld-over-te-maken-naar-palestina>, Discriminatie door financiële instellingen veelvoorkomend probleem zonder gerichte maatregelen: wat gaat er mis en wat moet er gebeuren? <https://www.mensenrechten.nl/actueel/weblogs/toegelicht/2024/discriminatie-door-financiele-instellingen-veelvoorkomend-probleem-zonder-gerichte-maatregelen>.

- De Nationaal Coördinator Discriminatie & Racisme (NCDR) heeft meerdere keren gewezen op misstanden, onder meer in de position paper <https://www.tweedekamer.nl/kamerstukken/detail?id=2025Z09362&did=2025D21507> voor een rondetafelgesprek in mei 2025.

Bits of Freedom kende de minister van Financiën de Big Brother Award 2024 publieksprijs toe vanwege het maken van het antiwitwasbeleid dat indirect leidt tot privacyschendingen en discriminatie door financiële instellingen. De organisatie pleitte er voor het maatschappelijke belang voorop te zetten en financiële instellingen niet langer een perverse prikkel te geven om het onschuldige klanten onnodig moeilijk te maken.²⁹

Niet alleen in Nederland

Discriminatie en uitsluiting doet zich in heel de EU voor. Dat valt onder meer af te leiden uit de 'Finance Watch feedback on Consumer Agenda 2025-2030 and action plan on consumers in the Single Market'³⁰ van 6 augustus jl. Daarin constateert Finance Watch dat in de EU nog steeds veel consumenten geen toegang hebben tot een basisbankrekening, onder meer vanwege excessieve de-risking. Het gebruik van AI draagt daaraan bij:

Evidence shows, however, that the use of AI is increasingly leading to people being denied a bank account due to discriminatory outcomes of AI systems used for the customer due diligence process (see: <https://algorithmwatch.org/en/false-positives/>). (...) Therefore, there is an urgent need to extend the scope of high-risk AI systems in the EU AI Act by broadening the scope of Annex III of the regulation.

Erkenning door de banken

De Nederlandse bancaire sector heeft inmiddels erkend dat bij hen het nodige is fout gegaan. Zo schreef de Nederlandse Vereniging van Banken op 22 april 2024: "Het maatschappelijk draagvlak voor de poortwachtersrol van banken staat onder druk. Te veel burgers, bedrijven en andere organisaties hebben last van het klantonderzoek en vragen die voortkomen uit het monitoren van transacties (...) Nog los van alle administratieve lasten geven deze controles veel klanten het ongemakkelijke gevoel dat ze in de gaten worden gehouden. Tegelijkertijd leveren al deze maatregelen te weinig zichtbare resultaten op in de vorm van opgepakte criminelen en afgepakt crimineel vermogen. Om er dus voor te zorgen dat er voldoende draagvlak blijft voor de witwasonderzoeken door banken moeten de zichtbare resultaten omhoog en de last die goedwillende klanten ervaren, omlaag."³¹

²⁹ <https://www.bitsoffreedom.nl/2025/02/13/big-brother-awards-2024-de-winnaars/>

³⁰ <https://www.finance-watch.org/policy-portal/retail-inclusion/the-consumer-agenda-2025-2030-must-address-barriers-to-accessing-essential-financial-services/>

³¹ <https://www.nvb.nl/nieuws/nvb-pleit-voor-nieuwe-aanpak-witwassen/>

Eind mei 2025 erkende grootbank ING ³² dat zij ten onrechte op grote schaal hebben gediscrimineerd: "ING Nederland deelt vandaag in een open brief aan haar klanten op wat voor manier ze verantwoordelijkheid neemt om ervaren discriminatie te voorkomen. ING reageert hiermee op rapporten uit 2024 van het Ministerie van Financiën en De Nederlandsche Bank. Hieruit bleek dat veel klanten van Nederlandse banken discriminatie ervaren bij processen die juist bedoeld zijn om het financiële stelsel veilig te houden, zoals de bestrijding van witwassen en terrorismefinanciering. Omdat de uitkomsten van deze onderzoeken ook ING-klanten raken, heeft de bank de afgelopen tijd extra maatregelen genomen om deze ervaren discriminatie aan te pakken."

Het systeem

Maar daarmee zullen de problemen niet kunnen worden opgelost, omdat de oorsprong van de discriminatie en uitsluiting ligt in de antiwitwasregels die risicoprofilering en het beoordelen van gedrag en transacties voorschrijven, in de veronderstelling dat banken en andere witwasbestrijdingsplichtigen op basis daarvan crimineel geld kunnen ontdekken.

Bij de overheid gaat het ook mis bij het plaatsen van mensen op zwarte lijsten en het opsporen van fraude, zie bijvoorbeeld het bericht van de Nationale Ombudsman: [Te weinig aandacht voor mensenrechten burgers op terrorisme- en extremismelijst](#). De Ombudsman schreef [een rapport](#) over de terroristenlijsten die de overheid bijhoudt en waar onschuldige burgers op terecht komen, met akelige consequenties. De problematiek die de Nationale Ombudsman beschrijft geldt ook aan de private kant van de witwasbestrijding.

De gemeente Amsterdam haalde *Technologyreview* met het artikel [Inside Amsterdam's high-stakes experiment to create fair welfare AI](#) over discriminerende algoritmen.

Diezelfde overheid is verantwoordelijk voor de risico analyses, typologieën en indicatoren die witwasbestrijdingsplichtigen moeten gebruiken voor de uitvoering van hun overheidstaken.

Gegevensbeschermingsrisico's

De privatisering van de criminaliteitsbestrijding levert steeds grotere gegevensbeschermingsrisico's op vanwege de toenemende omvang van de gegevens die worden verwerkt en uitgewisseld. Dat betreft zowel de private sector als de overheden.

Nederland

Bij de Nederlandse overheid zijn een toenemend aantal databases aanwezig waarin op grote schaal persoonsgegevens en andere vertrouwelijke gegevens zijn opgeslagen. Voorbeelden daarvan zijn de databases die door de politie worden beheerd en geanalyseerd, waartoe ook de databases van FIU Nederland behoren. Over het gebruik van

³² <https://nieuws.ing.nl/nl-NL/250333-ing-luistert-leert-en-handelt-om-ervaren-discriminatie-te-voorkomen/>

artificial intelligence (AI) door de politie bracht de Wetenschappelijke Adviesraad Politie (WARP) in juni 2025 een kritisch advies uit met als titel 'Navigeren in niemandsland' <https://www.wetenschappelijkeadviesraadpolitie.nl/uploads/publications/Navigeren-in-niemandsland.pdf>. In dat advies wordt onder meer opgemerkt dat het wettelijk kader te wensen overlaat en dringend moet worden herzien en voorts dat belangrijk is dat een evaluatiecommissie Wet politiegegevens wordt ingesteld vergelijkbaar met de evaluatiecommissie Wet op de inlichtingen- en veiligheidsdiensten. De rapporteurs merken onder meer op:

De Raad constateert dat herziening van de huidige wetgeving ten aanzien van de vergaring en de verwerking van gegevens noodzakelijk en urgent is. Het ontbreken van een adequaat wettelijk kader voor datagedreven werken leidt ertoe dat de grondrechten van burgers onvoldoende worden beschermd en dat de operationele strategie van de politie – als het gaat om datagedreven werken – hierdoor onder druk komt te staan.

en maakt in de voetnoot bij deze passage melding van het advies van de Autoriteit Persoonsgegevens:

De Autoriteit Persoonsgegevens (AP) heeft in maart 2025 een wetsvoorstel getoetst dat gaat over de vergaring en verwerking van gegevens door de politie en dat onderdeel is van de modernisering van het Wetboek van Strafvordering. De AP constateert dat dit voorstel burgers onvoldoende beschermt tegen mogelijke disproportionele schendingen van hun grondrechten. Zie: <https://www.autoriteitpersoonsgegevens.nl/actueel/ap-nieuw-wetboek-van-strafvordering-bescherm-t-mensen-onvoldoende>.

Op 5 maart 2025 werd het advies van de Afdeling advisering van de Raad van State over het bewaren door de politie van politiegegevens bekend <https://www.raadvanstate.nl/adviezen/@146778/w16-24-00313-ii/>, waarin de Afdeling zeer kritisch is over het voornemen de bewaartermijn voor politiegegevens te verlengen, terwijl die gegevens nu al te lang bewaard worden.

De afgelopen tijd is bekend geworden dat zowel politie, Openbaar Ministerie als andere overheidsinstanties geconfronteerd zijn met cybercrime en met het lekken van persoonsgegevens en andere vertrouwelijke gegevens. Uit een rapport van de Auditdienst Rijk dat in juni 2025 bekend werd gemaakt ³³, blijkt dat het Openbaar Ministerie nog niet aan de AVG voldoet.

Er zal veel moeten gebeuren, voordat de gegevensbescherming bij de Nederlandse overheid op orde is.

³³ <https://www.rijksoverheid.nl/documenten/rapporten/2025/06/10/tk-brief-auditrapport-2024-ministerie-van-justitie-en-veiligheid-vi-auditdienst-rijk>

EU

Steeds meer transactiegegevens worden uitgewisseld met de EU, daar opgeslagen en met AI geanalyseerd, voorbeelden zijn:

- CESOP, de Europese database waaraan banken en betaaldienstverleners betaalgegevens inzake alle grensoverschrijdende transacties verschaffen;
- de Europese database waarin cryptovaluta-aanbieders gegevens inzake alle cryptotransacties moeten leveren;
- de Europese database waarin met ingang van 1 juli 2030 alle facturen van grensoverschrijdende transacties in de EU zullen worden opgenomen, gebaseerd op de *VAT in the Digital Age* richtlijn.

Hoe veilig deze databases zijn en of de uitwisseling die er aan ten grondslag ligt wel veilig is, is onbekend.

Gegevensverwerking door de witwasbestrijdingsplichtigen

Van contactpersonen uit de financiële sector horen wij dat de huidige praktijk bij de banken regelmatig niet aan de AVG voldoet. Voorbeelden zijn:

- het klantenonderzoek (CDD) wordt niet uitgevoerd met behulp van veilige communicatiekanalen;
- klanten worden met het dreigement van beëindiging van de relatie onder druk gezet en regelmatig worden er vragen gesteld die verder gaan dan nodig of die klanten niet kunnen beantwoorden (zoals verzoeken om bewijsstukken waarvan de klant niet kon verwachten dat deze nodig zouden zijn, vragen aan consumenten over transacties van zeven jaar geleden);
- gevoelige persoonsgegevens (zoals bezoek aan sekswerkers, gokverslaving en informele geldstromen binnen familie- of kennissenkring) worden soms zonder afscherming opgeslagen in het klantdossier en onnodig gedeeld met andere medewerkers, soms worden gegevens toegevoegd aan het dossier van de partner zonder toetsing van noodzaak en toestemming;
- inzage in de klantdossiers wordt niet gelogd, toegangscontrole is onvoldoende;
- periodieke toetsing of gegevens verwijderd kunnen worden ontbreekt (herbeoordeling noodzaak bewaren), dataminimalisatie voorschriften worden niet nageleefd.

Kernprobleem: de verwerking van persoonsgegevens vindt plaats zonder passende beveiliging, zonder juridische toets op noodzakelijkheid (geen onderscheid tussen noodzakelijke en overbodige informatie), en zonder respect voor de vertrouwelijkheid van de communicatie. Identificatie- en verificatiedocumenten (zoals kopieën van legitimatiebewijzen, KvK-uittreksels en organogrammen) worden opgevraagd via e-mail en vervolgens in bulk opgeslagen in gedeelde mappen. Deze documenten worden automatisch aan klantdossiers toegevoegd – ongeacht het individuele risicoprofiel of de noodzaak in de context van het onderzoek.

Wij tekenen daarbij aan dat de praktijk per bank verschillend is.

Privacy First maakt zich zorgen over de naleving van de gegevensbeschermingsregels door de financiële sector en vreest dat het bij de andere witwasbestrijdingsplichtigen niet veel beter is gesteld.

Bescherming tegen fraude

Klanten van financiële instellingen verwachten dat zij worden beschermd tegen fraude, maar dat is regelmatig niet het geval. Zo zijn er financiële instellingen die criminaliteit faciliteren, lees onder andere:

- NRC artikel over Worldline: [Veel gebruikte betalingsdienst Worldline haalde kunstgrepen uit om fraude te verhullen.](#)
- NOS artikel over Worldline: <https://nos.nl/artikel/2572388-nrc-betaalverwerker-worldline-dekte-jarenlang-fraude-door-webwinkels-toe>.
- Betaaldienstverlener Payone bediende hoogrisicoklanten zonder voldoende maatregelen te nemen, <https://www.golem.de/news/sparkassen-dienstleister-payone-arbeitete-mit-pornodiensten-zusammen-2506-197448.html>.

In zeer veel Kifid zaken van klanten tegen financiële instellingen vanwege tegen hen gepleegde fraude, delft de klant bij het Kifid het onderspit omdat de klant zelf fouten heeft gemaakt. Die fouten worden vaak veroorzaakt door verwarring en onkunde van klanten. Privacy First is van mening dat meer voorlichting niet voldoende is. Basisdiensten moeten zodanig worden ingericht dat mensen makkelijk kunnen nagaan of er geen criminaliteit in het spel is.

Breng de gegevensbescherming op orde

De intrekking van de Wwft en de implementatie van het AML Package via de Iwt biedt een belangrijk moment om waarborgen wettelijk te verankeren. In het consultatievoorstel en de consultatietoelichting worden de grondrechten van burgers wél genoemd, maar niet concreet uitgewerkt. Wij zien dit als een gemiste kans, juist omdat witwasbestrijdingsplichtigen in de praktijk veel ruimte nemen, vaak ten koste van burgers. De hiervoor beschreven risico's spelen ook buiten de financiële sector.

Opvallend is dat tegen witwasbestrijdingsplichtigen hard wordt opgetreden als de overheid meent dat zij hun overheidstaken niet goed hebben uitgevoerd, maar dat de bedrijven niet worden gedagvaard als zij de grondrechten van burgers structureel schenden.

De risico's van artificial intelligence | de witwasbestrijding mag geen machine worden

De risico's voor klanten zullen door het gebruik van AI door witwasbestrijdingsplichtigen (in de praktijk met name banken en betaaldienstverleners) toenemen, nu de AI Act niet van toepassing is op dat gebruik ³⁴ en de AI wordt ontwikkeld in de black box van financiële instellingen, de overheid en grote IT-ondernemingen uit de VS ³⁵, zonder dat sprake is van volwassen tegenspraak.

Lees over de risico's verbonden aan digitale surveillance het boek *Mass data surveillance and predictive policing Contested Foundations and Human Rights Impact* ³⁶ door Plixavra Vogiatzoglou, verbonden aan de Universiteit van Amsterdam, waarin zij beschrijft dat op steeds grotere schaal surveillance systemen worden gecreëerd ten behoeve van de 'veiligheid'. Deze brengen zeer grote risico's voor burgers met zich mee en adequate waarborgen ontbreken. In het slothoofdstuk doet zij waardevolle voorstellen. Onder meer doet ze voorstellen inzake collectieve handhaving:

The collective enforcement of rights should be encouraged and enriched. To start with, the requirement of proving individual harm in cases of mass data surveillance and predictive policing could be loosened. Admissible in abstracto claims should not focus on individual harm but broader collective and societal harms imposed by inter alia power and informational asymmetries, the enhanced capacity for arbitrary interferences and abuse of power, and the inherent risks carried by data-driven systems.

Privacy First is van mening dat beter moet worden nagedacht over het AML/CFT systeem. Het systeem is door financiële beleidsmakers van FATF en de EU ontworpen, zonder onvoldoende aandacht voor de mens en voor grondrechten. Die aandacht moet er nu wel gaan komen.

Wij brengen tot slot de wijze woorden van de Nationale Ombudsman uit 2019 in herinnering die hij sprak in het interview dat in Trouw verscheen onder de titel *De overheid is een machine geworden* (<https://www.trouw.nl/politiek/de-overheid-is-een-machine-geworden-b0d70c4b/>):

³⁴ Zie [Das Dunkelfeld aufhellen. Über Schutzlücken der EU-KI-Verordnung bei der Regulierung der automatisierten Detektion von Geldwäsche](#) door Lena Leffer. Lees over de risico's van algoritmische misdaadopsporing en voorkoming het boek van Plixavra Vogiatzoglou: *Mass data surveillance and predictive policing. Contested Foundations and Human Rights Impact*, <https://www.routledge.com/Mass-data-surveillance-and-predictive-policing-Contested-Foundations-and-Human-Rights-Impact/Vogiatzoglou/p/book/9781032825915>.

³⁵ Finance Watch besteedde aandacht aan AI in de financiële sector in bredere zin, zie *Report – Artificial intelligence in finance: how to trust a black box?*, <https://www.finance-watch.org/policy-portal/digital-finance/report-artificial-intelligence-in-finance/>, maart 2025.

³⁶ <https://www.routledge.com/Mass-data-surveillance-and-predictive-policing-Contested-Foundations-and-Human-Rights-Impact/Vogiatzoglou/p/book/9781032825915>

Regels van de overheid worden voor steeds meer mensen te ingewikkeld. En ik heb al eerder gezegd: de overheid geeft geen vertrouwen meer en vraagt telkens aan burgers om zich te verantwoorden. Of het nou om Groningers gaat die kampen met aardbevingsschade of mensen die ten onrechte kinderopvangtoeslag moeten terugbetalen. De overheid vraagt veel van de burger en geeft zelf zo weinig. Dat komt ook doordat de overheid systemen heeft ontwikkeld om de burger te beoordelen. Het is een machine geworden."

Dat klinkt zorgelijk.

Dat is het ook. Wat meespeelt is dat de overheid steeds verder uit zicht verdwijnt. Je ziet het bij schuldhulpverlening en bij het aan de slag helpen van mensen met een beperking. Een aantal gemeenten zet samen een organisatie op die het werk uitvoert of de dienstverlening wordt overgeheveld naar particuliere instanties. Door de decentralisaties, van het Rijk naar de gemeenten, zou de afstand tussen burger en overheid verkleind moeten worden, maar we zien ook het omgekeerde gebeuren. De burger krijgt een overheid die hij niet meer kent." (...)

Waar gaat het mis?

Overheden doen heel veel via automatische systemen, waar geen mens meer aan te pas komt. Iedereen snapt de frustratie van die mevrouw met haar huurtoeslag. De tragiek is dat de ambtenaar formeel het juiste heeft gedaan. Zo is het systeem bedacht. We zien hier te veel voorbeelden van. Wat er zou moeten gebeuren is dat een ambtenaar de professionele ruimte heeft om een andere beslissing te nemen dan het systeem aangeeft." (...)

Van Zutphen worstelt met die voortschrijdende digitalisering. Het lot van de burger ligt in toenemende mate in handen van geautomatiseerde processen, met een overheid die zich sluipenderwijs terugtrekt.

Wat de Nationale Ombudsman in het interview beschrijft doet zich in de privatisering van de misdaadbestrijding voor.

Bijlage 2 – Samenwerking tussen de banken

Er worden voorbereidingen getroffen voor gegevensdeling door banken:

- De aankondiging van Transactie Monitoring Nederland (TMNL), de samenwerkings-bv van vijf Nederlandse banken, *Transactiemonitoring Nederland past werkwijze aan nieuwe Europese wetgeving aan*, 1 juli 2024, <https://tmnl.nl/article/transactiemonitoring-nederland-past-werkwijze-aan-nieuwe-europese-wetgeving-aan/>, met onder andere: "AMLR biedt nieuwe mogelijkheden. De AMLR zal grotendeels het Nederlandse wettelijke initiatief vervangen. Deze zorgt onder meer voor duidelijkheid over de manier waarop informatie over klanten geassocieerd met een hoger risico op witwassen of terrorismefinanciering kunnen vormen, kan worden gedeeld. Dat kan zijn tussen banken maar ook met andere poortwachters en de autoriteiten; zowel in Nederland als in heel Europa."
- DNB spreekt erover in het artikel d.d. 28 mei 2024, *Wat de klok doet tikken: op weg naar meer samenwerking in de witwasbestrijding*, <https://www.dnb.nl/algemeen-nieuws/speech-2024/wat-de-klok-doet-tikken-op-weg-naar-meer-samenwerking-in-de-witwasbestrijding/>. Daarin wordt niet alleen gesproken over toepassing van technologie, "Bijvoorbeeld om slimmer klantonderzoek en transactiemonitoring te doen, kunstmatige intelligentie in te zetten bij de risicoanalyse van klanten en gebruik te maken van digitale identificatie methodieken" en wordt gemeld dat de internationale samenwerking door private partijen zal gaan plaatsvinden: "Ook zien we grote toegevoegde waarde in het versterken van de samenwerking, zowel binnen Nederland als in Europa. Dan heb ik het niet alleen over de komst van de Europese toezichthouder AMLA. Ook internationale samenwerking tussen private partijen kan de effectiviteit van de transactiemonitoring verder vergroten."
- Wellicht dat de uitwisseling op Europees niveau zal gaan plaatsvinden. In een fiche van 9 mei 2025 schreef het kabinet: "Ook kondigt de Commissie aan een nieuw EU-systeem te onderzoeken om criminele geldstromen en terrorismefinanciering te kunnen volgen (tracken)", zie https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2025D20495&id=2025D20495. Details ontbreken, maar mogelijk houdt het verband met het initiatief van de Europese Commissie om te komen tot een nieuwe fraudebestrijdingsarchitectuur, zie het persbericht https://ec.europa.eu/commission/presscorner/detail/nl/ip_25_1849. Uit de bijbehorende white paper <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025DC0546> blijkt dat het initiatief breder zal kunnen zijn dan alleen de belangen van de portemonnee van de EU.

- In de brief van de minister van Financiën van 14 mei 2025, <https://open.overheid.nl/documenten/4f5365de-a995-45e7-bb4d-982dfec67f5b/file> staat vermeld dat er een nieuw transactiemonitoringsinitiatief komt: *"We gaan een pilot initiëren om te onderzoeken hoe gegevensdeling op Europees niveau kan worden vormgegeven. Hierbij werken we samen met onze nationale publieke en private partners, zoals de FIU-Nederland, NVB en DNB. Het doel is om in 2026 met de pilot te starten."* Hoewel TMNL niet wordt vermeld, zal deze bv hier waarschijnlijk een rol bij krijgen.
- In de consultatietoelichting wordt gesproken over verbeterde mogelijkheden tot gegevensdeling en uitbesteding, zie onder andere paragraaf 2.3. De bedoeling is bij het klantenonderzoek en de transactiemonitoring gebruik te maken van "nieuwe technologieën" zoals *artificial intelligence*. De witwasbestrijdingsplichtigen kunnen gegevens met elkaar delen en daarmee gericht en secuurder cliëntenonderzoek mogelijk maken, aldus de toelichting.

Privacy First ziet een ontwikkeling naar financiële surveillance waarbij het financiële doen en laten van iedere burger en organisatie op grote schaal wordt geanalyseerd en in de gaten gehouden, zonder dat sprake is van een verdenking. Dat is een kant die wij niet uit moeten.