aan	De Nederlandsche Bank Per e-mail: consultatie@dnb.nl
uw kenmerk	
ons kenmerk	SPF20231130
datum	30 november 2023
onderwerp	Consultatie DNB Q&A Good Practices Wwft

Geachte heer/mevrouw,

Stichting Privacy First maakt hierbij graag gebruik van de mogelijkheid om haar visie te geven op het consultatievoorstel voor een nieuwe aanpak voor de bestrijding van witwassen, zoals blijkend uit het document '*Consultatieversie DNB 'Q&As' en 'Good Practices' Wwft*' ('ontwerp Q&A'). Deze consultatie is bekendgemaakt via https://www.dnb.nl/nieuws-voor-de-sector/toezicht-2023/dnb-legt-nieuwe-aanpak-witwassen-voor-aan-financiele-sector/.

Privacy First meent dat uw nieuwe aanpak niet alleen relevant is voor financiële instellingen en de compliance industrie, maar dat ook de klanten van financiële instellingen worden geraakt door de wijze waarop financiële instellingen hun taken uitvoeren in opdracht van De Nederlandsche Bank (DNB) en de Autoriteit Financiële Markten (AFM).

Witwasbestrijding en bestrijding van terrorismefinanciering op grond van de *Wet ter voorkoming van witwassen en financieren van terrorisme* (Wwft) en de naleving van de sanctieregelgeving zijn onderwerpen die onze interesse hebben omdat bij die onderwerpen de financiële privacy van burgers in het geding is. Financiële privacy is één van de speerpunten van Privacy First. Het is van belang dat de financiële grondrechten van burgers worden gerespecteerd in een tijd dat de vertrouwelijkheid van financiële gegevens steeds meer wordt bedreigd, met grote risico's op het gebied van gegevensbescherming en verlies aan zelfbeschikkingsrecht.

Al langere tijd is duidelijk dat die financiële grondrechten niet goed gewaarborgd zijn bij de bestrijding van witwassen en terrorismefinanciering en de naleving van de sanctieregelgeving. Het optreden van de private ondernemingen aan wie die overheidstaken werden opgelegd heeft inmiddels geleid tot veel rechtspraak en een groot aantal Kamervragen.

Privacy First ziet aanleiding om commentaar te leveren op het consultatievoorstel, nu het van belang is dat de financiële privacy van Nederlandse burgers wordt gerespecteerd door de financiële instellingen die met de uitvoering van de Wwft zijn belast. Voorts dringt Privacy First er op aan dat DNB en AFM het privacybelang van de klant meenemen in hun toezicht op de naleving van de Wwft.

Privacy First verzoekt u deze consultatie integraal op uw website te publiceren.

PRIVACY FIRST

Inhoudsopgave

Achtergrond

Privacy First onderschrijft het belang van bestrijding van witwassen en terrorismefinanciering en van de naleving van de sanctieregels ('witwasbestrijding c.a.'), maar ziet met bezorgdheid dat deze overheidstaken worden uitbesteed aan private ondernemingen, die daar niet geschikt voor zijn en die soms klem zitten tussen de dreiging van forse sancties door u als toezichthouder of de opsporingsinstanties enerzijds, en het respecteren van de privacy van de klant anderzijds.

Om die reden volgen we de ontwikkelingen op dit terrein nauwlettend. Zo hebben we in december 2022 naar aanleiding van het wetsvoorstel *Plan van aanpak witwassen* een brief aan de vaste commissie Financiën van de Tweede Kamer gestuurd met als bijlage een memorandum.[1] In bijlage 1 bij het memorandum hebben wij onze zorgen geuit over de gegevensverwerking in het kader van de witwasbestrijding.

Op dit moment ontbreekt inzicht in de kwaliteit van de verwerking van persoonsgegevens en de naleving van de AVG door financiële instellingen in het kader van de witwasbestrijding.[2] Daar komt nog bij dat financiële ondernemingen datalekken niet hoeven te melden aan de benadeelde burgers.[3]

Zo zien wij risico's waar Wwft-plichtigen in verband met de naleving gebruik maken van externe leveranciers, zoals compliance dienstverleners, datahandelaren (World Check, Relian e.d.) en IT-leveranciers. Via die externe leveranciers kunnen persoonsgegevens en andere vertrouwelijke gegevens weglekken. Voor deze externe partijen geldt geen vergunningplicht, er worden geen integriteitseisen gesteld en er is onvoldoende of geen toezicht op de wijze waarop zij de persoonsgegevens en andere vertrouwelijke gegevens van de klanten van Wwft-plichtigen verwerken.

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

Het is ons niet gebleken dat DNB en AFM tot nu toe aandacht besteden aan de spanning die bestaat tussen de eisen die volgen uit witwasbestrijding en de eisen die samenhangen met het waarborgen van de privacy van burgers. Wij weten dat de Autoriteit Persoonsgegevens (AP) signalen over overtredingen van de AVG in het kader van de witwasbestrijding heeft ontvangen, maar de AP heeft geen capaciteit om te kunnen onderzoeken en handhavend op te treden. Ook is bekend dat instellingen spanning ervaren

[1] Te vinden via https://privacyfirst.nl/artikelen/misdaadbestrijding-is-niet-gediend-met-bancair-sleepnet-en-navraagplicht/ (zie aan het slot).

[2] Onder meer naleving van de verplichtingen tot dataminimalisatie, toegang op need-to-know basis, tijdig verwijderen persoonsgegevens en het informeren van betrokkenen over de gegevensverwerking.

[3] Artikel 42 Uitvoeringswet Algemene verordening gegevensbescherming (UAVG).

tussen de eisen van de toezichthouders en het waarborgen van de privacy van hun klanten.[4]

Om die reden roepen wij u op in uw Q&As en Good Practices meer aandacht te besteden aan de gegevensbeschermingsaspecten van de verwerking van persoonsgegevens voor de witwasbestrijding. Wij brengen in herinnering dat DNB toezicht houdt op naleving van wet- en regelgeving door financiële instellingen[5], hetgeen ook de naleving door die instellingen van de AVG omvat.

Het consultatiedocument

In ons commentaar gaan we alleen in op de privacy-aspecten van het ontwerp, niet op de overige onderwerpen.

Inleidende opmerkingen

Allereerst maken wij een aantal inleidende opmerkingen:

1. Financiële instellingen hebben geen opsporingstaken. Dat is voorbehouden aan opsporingsinstanties. De verplichtingen die instellingen hebben onder de Wwft kunnen als het voorstadium van de opsporing worden beschouwd, al gaat de monitoringverplichting van de Wwft in de praktijk heel ver. De met de naleving van de Wwft en sanctieregelgeving samenhangende inbreuk die instellingen maken op de privacy van burgers zou daarmee veel minder verregaand mogen zijn, dan als sprake zou zijn van verwerking van persoonsgegevens met het oog op de opsporing van strafbare feiten. Dit uitgangspunt lijkt verlaten in hoe DNB kijkt naar Wwft-naleving. Het voortdurend monitoren van klanten zonder dat duidelijke criteria zijn geformuleerd waaronder dat monitoren mag plaatsvinden, verhoudt zich bijv. niet goed tot de AVG. Als dergelijke monitoring van burgers door opsporingsdiensten plaatsvindt, lijkt zij met meer waarborgen omgeven dan wanneer zij onder de Wwft plaatsvindt. Wij roepen DNB op duidelijker te maken hoe instellingen kunnen voldoen aan de Wwft mét inachtneming van de AVG. De door de Wwft vereiste 'vastlegging' (het leveren van bewijs dat aan de Wwft is voldaan) dient op grond van de dataminimalisatie-verplichtingen van de AVG niet verder te gaan dan nodig is met het oog op de bestrijding van witwassen. Verduidelijking daarvan door middel van

[4] Kaderwetevaluatie DNB 2016-2020, te vinden via: https://www.rijksoverheid.nl/documenten/rapporten/2021/11/08/evaluatie-de-nederlandsche-bank-dnb-2016-2020.

[5] Zoals ook door u aangegeven in het op 28 november jl. bekendgemaakte *Toezicht in beeld 2023-2024*, pagina 4: "*Als toezichthouder ziet DNB erop toe dat instellingen voldoen aan wet- en regelgeving, dat risico's in kaart worden gebracht en dat deze adequaat en tijdig worden beheerst*".

deze ontwerp Q&A is van groot belang voor de instellingen en voor de betrokkenen (de klanten).

2. Wwft-instellingen worden geacht een grote hoeveelheid persoonsgegevens te verwerken om te kunnen voldoen aan hun wettelijke verplichtingen onder de Wwft.[6] Noch de Wwft, noch de ontwerp Q&A bieden inzicht in wat die verplichtingen exact zijn. De Wwft is een zeer generiek geformuleerde wet, zodat vele keuzes gemaakt kunnen worden in hoe daarop toezicht gehouden wordt of in hoe deze wet wordt nageleefd. In de praktijk leidt dit ertoe dat onduidelijk is hoe financiële instellingen hun dataminimalisatie-plicht moeten naleven. Wwft-naleving is risico-gebaseerd, maar AVG-naleving is dat niet. Van de wetgever en toezichthouders kan meer verwacht worden aan duiding over hoe Wwft-naleving en gelijktijdige AVG-naleving concreet vormgegeven dient te worden. Het maken van generieke opmerkingen over de AVG volstaat hiertoe niet: DNB en AFM zouden – bij voorkeur samen met de AP - hierover meer duiding moeten geven.

3. Burgers kunnen in het dagelijks leven niet om financiële instellingen heen. Deelname aan het maatschappelijk verkeer is bijvoorbeeld onmogelijk zonder over een bankrekening te beschikken. Als het gebruik van een bankrekening er per definitie toe leidt, dat burgers feitelijk een groot deel van hun privacy moeten opgeven, gaat er fundamenteel iets mis: de AVG wordt hiermee een dode letter. Privacy First roept DNB op meer oog te hebben voor dit aspect van Wwft toepassing. Privacy First is zich ervan bewust dat veel Wwft-regels uit Europa komen. Desalniettemin is er ruimte deze regels op meer privacy-bewuste wijze toe te passen dan DNB lijkt te doen. Privacy First neemt hierbij in aanmerking, dat uit vele onderzoeken blijkt dat anti-witwasregelgeving niet effectief is. Ook tegen deze achtergrond roepen wij DNB/AFM en de AP op om meer oog te hebben voor de AVG.

4. Deze ontwerp Q&A geven geen inzicht in wat DNB/AFM verstaan onder een risico-gebaseerde benadering in de witwasbestrijding. In combinatie met het feit dat de toezichthouders de laatste jaren fors handhaven bij instellingen of zelfs aangifte tegen instellingen en bestuurders doen, leidt dit ertoe dat instellingen het zekere voor het onzekere nemen en – bij gebrek aan duidelijkheid over wanneer de toezichthouder vindt dat de instelling exact 'voldoende' inspanningen heeft gedaan om aan de Wwft te voldoen – aan klanten liever teveel informatie vragen dan te weinig. Het spanningsveld tussen Wwft-naleving en voldoen aan de AVG wordt hiermee ten onrechte bij de instellingen gelegd. Begrijpelijkerwijs kan niet vooraf exact bepaald worden wanneer Wwft compliance 100% volstaat, maar het ligt op de weg van de toezichthouder om in de ontwerp Q&A meer duidelijkheid te creëren dan nu is gedaan.

Privacy First roept DNB en AFM op om niet alleen een Q&A op te stellen die overwegend een samenvatting is van wet- en regelgeving. Het is aan te bevelen om juist te zorgen voor

[6] De grondslag van artikel 6, eerste lid, onder c van de AVG.

verduidelijkingen op het gebied van gegevensbescherming, die bewerkstelligen dat de AVG correct kan worden nageleefd door de financiële instellingen.

Deelonderwerpen

Wij dringen er bij DNB en AFM op aan om meer duidelijkheid te creëren rondom een aantal voor burgers belangrijke onderwerpen op het gebied van de AVG in relatie tot witwasbestrijding c.a.

Verificatie van de identiteit

De wijze waarop financiële instellingen de identiteit van hun cliënten, vertegenwoordigers en de uiteindelijk belanghebbenden verifiëren roept veel problemen op, wat ook samenhangt met het verdwijnen van fysieke kantoren van financiële instellingen.

Verificatie van de cliënt vindt op grond van de Wwft plaats vóór de aanvang van de relatie. De Wwft bevat *geen* verplichting dat er periodiek moet worden geheridentificeerd of dat er een niet-verlopen identiteitsbewijs in het dossier moet zitten. De identiteit verandert immers niet. De actualiseringsplicht van de Wwft heeft betrekking op andere gegevens inzake de cliënt en de opdracht, die relevant zijn voor het risicoprofiel. Er is alleen reden voor heridentificatie als de financiële instelling hiertoe redenen ziet, bijv. als de instelling denkt dat de cliënt is overleden of er iemand anders achter de relatie zit. Wij adviseren u dit duidelijk te maken aan de financiële instellingen.

De Wwft verplicht verder niet tot het opslaan van kopieën van identiteitsbewijzen (maar het mag wel); er kan worden volstaan met het inzien van het originele identiteitsbewijs en het noteren van de in de Wwft voorgeschreven gegevens. In het kader van de dataminimalisatie-plicht is het daarom essentieel dat - als dergelijke kopieën zijn opgevraagd - deze zo spoedig mogelijk worden verwijderd.

Hierbij speelt ook een rol dat in de financiële sector langdurige relaties voorkomen en de bewaarplicht van artikel 33 Wwft pas verwijdering toestaat vijf jaar na het eindigen van de zakelijke relatie. Dat betekent dat financiële instellingen die een relatie van twintig jaar hebben met een klant, in voorkomende gevallen alle kopieën van identiteitsbewijzen 25 jaar lang bewaren. Dit is een gegevensbeschermingsrisico voor de klant en de bij de klant betrokken personen en is in strijd met de dataminimalisatieplicht. Wij adviseren u duidelijk te maken aan de financiële instellingen dat actualisering van de identiteit en bewaren van het identiteitsbewijs niet noodzakelijk is, maar dat kan worden volstaan met vastlegging van de relevante gegevens.

Er zijn financiële instellingen die van hun klanten eisen dat zij selfies van zichzelf maken en aan de instelling versturen. Dit is iets wat niet is gebaseerd op de Wwft, wat dus ook

betekent dat de bewaartermijnen van de Wwft niet gelden. Wij adviseren u aan de financiële instellingen duidelijk te maken dat het maken van selfies niet is gebaseerd op de Wwft en dat de instellingen zullen moeten aangeven welke andere geldige AVG-grondslag daarvoor is en dat zij de AVG-verplichtingen correct zullen moeten naleven (o.a. tijdige verwijdering).

Informeren van betrokkenen

Een van de basisverplichtingen van de AVG is dat betrokkenen worden geïnformeerd als hun gegevens door derden worden verschaft (artikel 14 AVG). Het is Privacy First bekend dat dat financiële instellingen deze verplichting niet naleven als zij van hun cliënten die geen natuurlijke persoon zijn, persoonsgegevens verkrijgen van personen die niet zijn betrokken bij het contact met de instelling, bijvoorbeeld persoonsgegevens inzake uiteindelijk belanghebbenden (UBO's) en persoonsgegevens van personen werkzaam bij de cliënt. Deze betrokkenen in de zin van de AVG worden niet geïnformeerd door de instellingen en zijn dus ook niet in staat te verifiëren of de gegevens terecht zijn verstrekt en of de gegevens juist zijn.

Als DNB zou menen dat voormelde verplichting uit de AVG niet zou gelden, ontvangen wij graag een juridisch onderbouwde motivering, waarbij eventueel ook aandacht kan worden besteed aan de renseignering die hierna wordt genoemd.

In dat verband is het eveneens relevant dat cliënten worden geïnformeerd over het aan hen toegekende risicoprofiel (zie paragraaf 3.8 ontwerp Q&A) en de grondslagen daarvoor. Dit is van belang omdat de cliënt (natuurlijke persoon) dan kan beoordelen of de financiële instelling is uitgegaan van onjuiste feiten respectievelijk een onjuiste conclusie (hoog risico) heeft getrokken. Er geldt op grond van de Wwft geen verplichting tot geheimhouding van het risicoprofiel. Privacy First adviseert de toezichthouders in de Q&A te verduidelijken dat de cliënten geïnformeerd dienen te worden.

Ook hier nodigen wij DNB, als zij zou menen dat Wwft-plichtigen hun cliënten niet over het risicoprofiel en de feiten waarop dat is gebaseerd zou hoeven informeren, een juridisch onderbouwde toelichting te geven waarom dit niet van toepassing zou zijn.

Verder leven financiële instellingen hun verplichting om betrokkenen te informeren over verstrekking van gegevens aan derden, bijvoorbeeld aan de Belastingdienst buiten de gebruikelijke renseignering[7] niet na. Zie over de verplichting om betrokkenen te informeren over verstrekking van persoonsgegevens aan derden de uitspraak van het Europees Hof d.d. 12 januari 2023 inzake Österreichische Post, zaak C-154/21.

[7] De gegevens die de fiscus krijgt voor de Nederlandse belastingheffing.

Voorbeeld: banken zijn op grond van CRS en FATCA verplicht om bepaalde financiële gegevens aan de Belastingdienst te verschaffen, die de Belastingdienst weer aan buitenlandse belastingdiensten verstrekt. De banken informeren betrokkenen hierover niet.

Privacy First adviseert DNB en AFM om de financiële instellingen op deze verplichting te wijzen en hen er op te wijzen dat deze verplichting nageleefd dient te worden.

NB: de tekst in het ontwerp Q&A, QA.2.32, verwijst alleen naar de bepaling in de Wwft dat de cliënt wordt geïnformeerd. Als de cliënt geen natuurlijke persoon is, zal de financiële instelling de AVG moeten naleven en de betrokkenen moeten informeren.

Privacy First realiseert zich dat financiële instellingen niet blij zullen zijn met het feit dat zij tot naleving van artikel 14 AVG zijn verplicht. Dat artikel is er echter niet voor niets en stelt de betrokkenen (zoals UBO's en vertegenwoordigers) in staat na te gaan of hun persoonsgegevens terecht en op juiste wijze worden verwerkt.

Veilige communicatie met klanten over het klantenonderzoek in het kader van witwasbestrijding c.a.

Het is Privacy First bekend dat veel financiële instellingen het cliëntenonderzoek op grond van de Wwft op een onveilige manier uitvoeren. Zo worden allerlei persoonsgegevens per e-mail opgevraagd. Een voorbeeld daarvan zijn banken die van klanten die geen natuurlijke persoon zijn, verwachten dat een kopie van het identiteitsbewijs van de uiteindelijk belanghebbende (UBO) per e-mail (zeer onveilig) wordt verstuurd. Dat is zeer problematisch en datzelfde geldt voor allerlei andere vertrouwelijke gegevens die banken bij hun klanten opvragen, zoals belastingaangiften, eigendomsbewijzen en andere notariële akten.

Deze werkwijze doet merkwaardig aan, nu het betalingsverkeer wel goed wordt beveiligd. Het is in strijd met de basisverplichting van de AVG om te zorgen voor passende informatiebeveiliging.

Wij adviseren u de financiële instellingen erop te wijzen dat voor het uitwisselen van vertrouwelijke gegevens in het kader van het cliëntenonderzoek vereist is, dat een beveiligd kanaal wordt aangeboden. Datzelfde geldt als de cliënt in het kader van het cliëntenonderzoek wordt bijgestaan door een adviseur (zoals een accountant, belastingadviseur of een advocaat).

Onderzoek naar 'bron van de middelen'

Instellingen moeten 'zo nodig' onderzoek doen naar de bron van de middelen van klanten. Het is aan de instelling te bepalen of onderzoek nodig is op grond van de inschatting die de instelling maakt van 'het risico'.

In de praktijk worden door instellingen onderzoeken uitgevoerd, die verder gaan dan nodig om naleving van deze regel te waarborgen. Op deze wijze wordt gehandeld in strijd met de dataminimalisatie-plicht van de AVG.

Privacy First adviseert een nadere duiding in de Q&A op te nemen over de grenzen die in acht genomen moeten worden bij het onderzoek naar de bron van de middelen. De tekst zoals geformuleerd in de wet en de ontwerp Q&A is te weinig specifiek om diepgaande inbreuken op de privacy van burgers te rechtvaardigen.

Bad press

De toezichthouders verwachten dat instellingen voortdurend oog houden voor externe signalen over klanten ('bad press'). Dit kunnen zij doen door middel van een extern systeem of zelf doen bijv. door checks op de naam van de klant uit te voeren in combinatie met andere zoektermen zoals fraude, terrorisme en witwassen.

Online monitoring van personen of zelfs stelselmatig onderzoek naar personen is niet zomaar mogelijk onder de AVG. Het kan onder omstandigheden noodzakelijk zijn online monitoring uit te voeren, maar hiervoor moet dan wel een stevige wettelijke basis zijn gelet op de ingrijpende inbreuk op de privacy die hiermee gemoeid is.

Privacy First adviseert DNB – eventueel in samenspraak met de AP – aan te geven in de Q&A wanneer online monitoring door instellingen legitiem en proportioneel is.[8]

Vermeend hoog risico wegens nationaliteit

Het is Privacy First bekend dat mensen met de Iraanse of Russische nationaliteit, ook al wonen ze lang in Nederland, grote problemen met financiële instellingen ondervinden. Het hebben van een bepaalde nationaliteit kan echter nooit betekenen dat iemand per definitie een hoog risico vormt op het overtreden van antiwitwasregelgeving.

Privacy First adviseert in de ontwerp Q&A op te nemen dat een bepaalde nationaliteit of herkomst nooit een reden hoort te zijn om iemand als hoog risico aan te merken.

Vermeend hoog risico van iedere PEP

In paragraaf 3.5 van de ontwerp Q&A staat dat PEPs niet per definitie hoog risico zijn, ook al gaat de Wwft daar vanuit. Privacy First begrijpt in dat licht niet waarom de in QA3.33 genoemde aanvullende maatregelen nodig zijn en ook niet waarom bij laag-risico PEPs die extra maatregelen nog twaalf maanden moeten worden gecontinueerd als de cliënt/UBO niet langer PEP is.

[8] Ter inspiratie: er wordt momenteel gewerkt aan nadere guidance op dit gebied voor gemeenten (Kamerbrief 29 april 2022, TK 32 761, nr. 224).

Realiseren de toezichthouders zich dat de QA3.33 genoemde maatregelen (en mogelijk de PEP-kwalificatie zelf) op gespannen voet staan met de financiële grondrechten van de betrokken personen? En zo ja, waarom dringen de toezichthouders dan niet aan op wijziging van zowel de Nederlandse als Europese regelgeving, zodat de grondrechten alsnog worden gerespecteerd?

Vermeend hoog risico diversen

In de voorbeelden die in de ontwerp Q&A voorkomen staan teksten die vragen oproepen, zoals in GP3.33, waarin onder andere als rode vlag staat vermeld: "*De cliënt/UBO verschaft documenten over de bron van middelen en vermogen die inconsistent zijn met dat wat vergelijkbare cliënten aanleveren*". Kunnen de toezichthouders toelichten wat 'vergelijkbare cliënten' zijn met dezelfde soorten bronnen van middelen en vermogen? Heeft deze opmerking een wetenschappelijke basis? Hoe moeten instellingen uitvoering geven aan deze Q&A?

Een andere rode vlag in dezelfde alinea veronderstelt dat iedere cliënt of UBO perfect begrijpt wat de financiële instelling van hem/haar verlangt, "*De cliënt/UBO verschaft documenten over de bron van middelen en vermogen die gebrekkig zijn of waar de rationale van ontbreekt.*" Het komt regelmatig voor dat cliënten en UBO's de gestelde vragen niet begrijpen en het komt ook regelmatig voor dat financiële instellingen hun vragen op een onduidelijke manier stellen.

Privacy First adviseert de toezichthouders zeer kritisch naar dit soort teksten te kijken, aangezien deze financiële discriminatie in de hand werken.

In onder meer GP3.48 en QA3.62 geeft het ontwerp Q&A aan, wanneer klanten opgezegd of geweigerd mogen worden. Dat kan ertoe leiden dat mensen die fouten hebben gemaakt geen bankrekening kunnen krijgen en niet meer in staat zijn om hun leven te beteren. Privacy First mist in dit onderdeel een toelichting op de omgang van financiële instellingen met dergelijke situaties en de exacte verhouding tot de (on)mogelijkheid tot het aanbieden van een basisbankrekening (de basisbankrekening komt helemaal niet voor). Privacy First adviseert het ontwerp op dit punt aan te vullen.

In de passages over geautomatiseerde transactiemonitoring[9] mist Privacy First aandacht voor de discriminatierisico's en risico's van schending van grondrechten verbonden aan het gebruik van geautomatiseerde transactiemonitoring (inclusief AI/*machine learning*) en voor de schade die onterechte bevragingen van cliënten over transacties kunnen veroorzaken. Privacy First adviseert toe te voegen dat de instelling zorg draagt voor grondrechtentoetsing van de geautomatiseerde transactiemonitoring en voorts dat

[9] Zoals GP4.1-GP4.7, GP4.18, QA4.32-QA4.34 en GP4.30-GP4.32.

onderzoek wordt gedaan naar de schade die klanten ondervinden door onterechte bevraging.

Privacy First ziet dat DNB van mening is dat pintransacties in Oost-Turkije een indicatie opleveren voor het bestaan van een verdachte transactie (GP4.24). Turkije staat niet op de lijst van landen met een hoog Wwft risico.[10] Waarom is pinnen in Oost-Turkije een risico-indicator? Betekent dit voorbeeld dat DNB pin-opnamen in vele landen van de wereld verdacht acht, ook al staan deze landen niet op de lijst van de Europese Commissie en gaat het om kleine bedragen? Privacy First beveelt aan bij dit soort voorbeelden toe te lichten welke landen DNB in aanvulling op de lijst van de Europese Commissie risicovol vindt en waarom DNB deze mening toegedaan is, om te voorkomen dat financiële instellingen zonder objectieve redenen hiertoe discriminerend optreden.

Contant geld

Het bestaan van contant geld is vanuit privacy perspectief een groot goed. DNB wijst er in deze Q&A terecht op dat contant geld een wettig betaalmiddel is, waarvan het legitieme gebruik niet gehinderd mag worden. Tegelijk suggereert DNB in veel beleidsuitingen, dat contant geld een verhoogd risico met zich meebrengt.

Het gebruik van contant geld door particulieren zou naar mening van Privacy First geen (mede) risico-indicator mogen zijn voor een potentieel hoog risico op witwassen.[11] Het kwalificeren van klanten als (hoog) risicovol mede omdat zij regelmatig cash gebruiken en/of vaker cash gebruiken dan de gemiddelde klant, komt met mogelijk impactvolle gevolgen voor de desbetreffende klant. Hiermee worden klanten die hechten aan het gebruik van contant geld vanwege bijvoorbeeld hun privacy ten onrechte bij voorbaat in het verkeerde hoekje geplaatst. Privacy First ziet voorshands geen legitieme reden waarom deze potentiële negatieve impact opweegt tegen het principe dat contant geld een wettig betaalmiddel is dat voor eenieder beschikbaar moet zijn.

Privacy First dringt aan op aanpassing van het beleid en de ontwerp Q&A.

Niet meer persoonsgegevens dan nodig

Het is Privacy First bekend dat financiële instellingen van klanten meer persoonsgegevens vragen dan de Wwft en de sanctieregelgeving voorschrijven. Zo vragen instellingen 'voor de veiligheid' soms om persoonsgegevens van alle financieel belanghebbenden van een entiteit, ook als zij geen uiteindelijk belanghebbende (UBO) zijn in de zin van de Wwft en de Handelsregisterwet.

---

[10] Gedelegeerde Verordening (EU) 2013/1219 van de Commissie.

[11] Zie bijvoorbeeld GP4.11 waarin betalingen aan de Filipijnen van EUR 13.000 zonder duidelijke toelichting als ongebruikelijk worden aangemerkt. Ook het voorbeeld van GP4.16 is onbegrijpelijk nu niet wordt toegelicht waarom op de kleine transacties de subjectieve indicator is toegepast.

In het kader van de sanctieregelgeving wordt door financiële instellingen soms dezelfde UBO-definitie gehanteerd als in de Wwft (meer dan 25% eigendomsbelang dan wel bijzondere zeggenschap), terwijl de Europese verordeningen een eigen UBO-definitie kennen: '*toebehoren aan, eigendom zijn, in het bezit zijn of onder zeggenschap staan*', zoals nader toegelicht in de EU Best Practices.

Het verwerken van persoonsgegevens mag alleen plaatsvinden als er een wettelijke grondslag is. Dat betekent dat persoonsgegevens van mensen die geen UBO zijn in de zin van de Wwft dan wel de sanctieregelgeving niet mogen worden verwerkt en dat financiële instellingen als zij dat wel doen de AVG overtreden.

Privacy First adviseert in de ontwerp Q&A toe te lichten dat instellingen wel algemene informatie over de structuur en het aantal belanghebbenden mogen vragen, maar dat de verwerking van persoonsgegevens alleen is toegestaan als er een wettelijke grondslag is (dus bijvoorbeeld als betrokkene UBO is, vertegenwoordiger is of cliënt is).

Vastleggen gegevens

Waar het de vastlegging van gegevens betreft, verwijst u naar artikel 33 Wwft, dat specificeert welke gegevens instellingen minimaal moeten vastleggen. Voorts verwijst u naar de website van de AP waar vermeld is dat instellingen een kopie van het identiteitsbewijs mogen vastleggen en het BSN enkel mogen vastleggen als dat in de wet staat.

De Q&A zijn hiermee niet erg behulpzaam voor de praktijk en geven geen inzicht in wat burgers van instellingen kunnen verwachten in dit kader. Zie ook onze eerdere opmerkingen over verificatie van de identiteit.

Objectieve en subjectieve indicatoren

Vanwege het uitgangspunt dat financiële instellingen geen opsporingsdiensten zijn, is oorspronkelijk bedacht dat zij ongebruikelijke transacties dienden te melden op basis van objectieve indicatoren. Na melding op basis van objectieve criteria zou het vervolgens aan de opsporingsdiensten zijn om al dan niet tot verder onderzoek over te gaan. Echter, inmiddels bestaat de plicht om ook verdachte transacties te melden op basis van zgn. subjectieve indicatoren. Dit veronderstelt dat een financiële instelling kan beoordelen of er een vermoeden van witwassen is, iets wat zeer moeilijk uitvoerbaar is.

Nederland is het enige land in de EU waar 'ongebruikelijke' transacties moeten worden gemeld, in plaats van (enkel) verdachte transacties. Daardoor is het aantal FIU-meldingen

in Nederland het hoogst in de EU en moeten Nederlandse burgers meer inbreuken op hun privacy dulden dan andere EU-burgers.[12]

Privacy First pleit ervoor dat alleen melding van verdachte transacties zal plaatsvinden en verzoekt DNB en AFM bij de wetgever daarop aan te dringen.

Bewaartermijnen en terugkijkperiode

Particulieren hoeven hun administratieve gegevens (zoals bankafschriften en loonstrookjes) niet verplicht te bewaren, al moeten ze wel met de terugvorderingstermijn van de fiscus rekening houden. De Belastingdienst mag tot vijf jaar terug belasting vorderen. Ondernemers (zoals in het midden- en kleinbedrijf) hebben een bewaarplicht op grond van de fiscale regelgeving.

Privacy First is er mee bekend dat financiële instellingen in de praktijk soms vragen aan particulieren en aan midden- en kleinbedrijf stellen over financiële transacties van vele jaren terug. De instellingen gaan dan uit van de veronderstelling dat de klant nog over allerlei gegevens beschikt om aan te kunnen tonen dat de transactie legitiem was; daardoor worden klanten verrast die regelmatig bepaalde gegevens niet meer hebben (en ook niet wisten dat de financiële instelling er om kon vragen).

Privacy First adviseert om in de ontwerp Q&A duidelijk te maken dat financiële instellingen zich redelijk opstellen bij het vragen van informatie over transacties uit het verleden, waarbij naar onze mening instellingen voor particulieren (maximaal) terug kunnen gaan naar vijf jaar voor een bepaalde transactie en voor midden-en kleinbedrijf ook moeten aansluiten bij de fiscale bewaarplichttermijn. Privacy First herhaalt dat instellingen geen opsporingstaken vervullen, maar onder de Wwft enkel monitoringsverplichtingen naleven. Waar de Belastingdienst bij particulieren niet meer kan terugvorderen na vijf jaar, valt niet in te zien dat instellingen van klanten vergen dat zij informatie aanleveren over een transactie die meer dan vijf jaar in het verleden ligt, terwijl op grond van de belastingwetgeving maar vijf jaar kan worden teruggegaan en in het civiele recht voor veel vorderingen een verjaringstermijn van vijf jaar geldt.

Ook de bewaarplicht van instellingen onder de Wwft vergt aandacht. Artikel 33 Wwft bepaalt dat instellingen gegevens met betrekking tot het cliëntenonderzoek minimaal vijf jaar na het beëindigen van de relatie of na het uitvoeren van de transactie moeten bewaren. Het betreft alle gegevens die zijn verkregen tijdens het klantacceptatieproces, zoals kopieën identiteitsbewijzen, correspondentie, gespreksnotities met cliënt, etcetera.

[12] Volgens het Europol-rapport 'From suspicion to action' (2017) is 65% van alle meldingen in de EU afkomstig van twee lidstaten, nl. het Verenigd Koninkrijk en Nederland. Nu het VK de EU heeft verlaten, zal Nederland de grootste melder zijn. Het rapport kwalificeert het aantal meldingen in Nederland als een 'anomalie'. Dit rapport is te vinden via: https://www.europol.europa.eu/cms/sites/default/files/documents/ql-01-17-932-en-c_pf_final.pdf.

Privacy First is bezorgd dat bij de langdurige relaties die bij financiële instellingen veel voorkomen, veel te veel gegevens langdurig worden bewaard. Dit is hiervoor al aangekaart bij het onderwerp verificatie van de identiteit, maar geldt ook voor andere gegevens van het klantenonderzoek.

In het kader van de dataminimalisatie-plicht en de gegevensbescherming (inclusief cybersecurity) adviseert Privacy First dat persoonsgegevens uit het klantenonderzoek die ouder zijn dan vijf jaar worden beperkt tot het hoogst noodzakelijke, rekening houdend met het risicoprofiel van de klant en de betrokken natuurlijke persoon. Verder adviseert Privacy First dat DNB – in overleg met de AP – nadere duiding geeft over de naleving van deze verplichting.

Tot slot

Hoogachtend,

namens Stichting Privacy First,

Vincent Böhre
juridisch adviseur