

aan Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Ministerie van Financiën
Via www.internetconsultatie.nl

ons kenmerk SPF20260323

datum 23 maart 2026

onderwerp Internetconsultatie *Besluit tot wijziging Besluit BRP i.v.m. derdenaanwijzing banken*, aangekondigd op
<https://www.internetconsultatie.nl/derdenaanwijzingbankenbesluit/bl>

Geachte heer/mevrouw,

Met grote zorgen volgt Stichting Privacy First de ontwikkelingen rondom de privatisering van de criminaliteitsbestrijding (bestrijding van witwassen, terrorismefinanciering en overtreding van de sanctieregelgeving) naar private ondernemingen. In dat kader wordt een grote hoeveelheid overheidstaken aan banken uitbesteed, zonder dat sprake is van passende waarborgen.

Ter voorkoming van misverstanden:

Privacy First onderschrijft dat het belangrijk is misdaad te bestrijden en vindt het belangrijk dat dit gebeurt door actoren die geschikt zijn voor de aan hen toebedeelde taken en verplichtingen, op basis van proportionele regelgeving. De afgelopen twintig jaar is echter duidelijk geworden dat de privatisering van misdaadbestrijdingstaken naar bedrijven ertoe heeft geleid dat onschuldige burgers worden gediscrimineerd en benadeeld. In onze consultatiereactie op de internetconsultatie over het wetsvoorstel tot implementatie van de nieuwe Europese antiwitwasregels hebben wij dat in *Bijlage 1 - De schaduwkant van de privatisering van de misdaadbestrijding* uitvoerig toegelicht.¹

¹ Zie inleidend artikel *Permanente surveillance dreigt onder nieuwe anti-witwasregels* <https://privacyfirst.nl/artikelen/permanente-surveillance-dreigt-onder-nieuwe-anti-witwasregels/> en onze consultatiereactie https://privacyfirst.nl/wp-content/uploads/consultatie_lwt_PrivacyFirst_29aug2025.pdf.

In deze consultatiereactie zullen wij aan u duidelijk maken dat toegang tot de basisregistratie personen (BRP) disproportioneel en onnodig is, alsmede in strijd met de AVG, aangezien het geen bijdrage levert aan de bestrijding van witwassen, terrorismefinanciering en naleving van de sanctieregels, tezamen aan te duiden als 'AML/CFT'.

Onderwerp van deze consultatie

Deze consultatie vindt plaats op grond van het nieuwe verzoek van de Nederlandse Vereniging van Banken (NVB) om toegang tot de BRP.²

Voorgesteld wordt om dit te regelen via het ontwerpbesluit dat een wijziging van bijlage 4 van het Besluit basisregistratie personen bevat ('het ontwerpbesluit'). In het ontwerpbesluit is een nota van toelichting opgenomen ('de ontwerptoelichting').

De NVB heeft een consultatiereactie³ gegeven waarin een gelijksoortige toelichting wordt gegeven en waarin wordt gezegd dat deze toegang in Zweden, België en Oostenrijk al voor banken is geregeld. Voorts wordt verzocht nog meer persoonsgegevens te mogen raadplegen, namelijk van uiteindelijk begunstigen (UBO's) en vertegenwoordigers van organisaties. Het valt op dat ook in de NVB-reactie niet wordt onderbouwd waarom toegang tot de BRP noodzakelijk zou zijn voor het cliëntenonderzoek. Wij zullen in dit commentaar ook deels ingaan op de NVB-reactie.

Te raadplegen persoonsgegevens

Persoonsgegevens zonder wettelijke grondslag (partner, niet-vaststelling nationaliteit)

Opvallend is dat de gegevensverstrekking persoonsgegevens uit de BRP omvat die niet worden vereist in artikel 22 van de Europese antiwitwasverordening (AMLR), want in het ontwerpbesluit worden de persoonsgegevens van de partner vermeld terwijl die niet in artikel 22 AMLR zijn opgenomen:⁴

² Vreemdgenoeg wordt dit niet aan het begin van de ontwerptoelichting vermeld maar pas in paragraaf 3.4, waar wordt vermeld dat de NVB zich "met een nadrukkelijk en onderbouwd verzoek tot aansluiting op de BRP tot de minister van Financiën [heeft] gewend".

³ <https://www.internetconsultatie.nl/derdenaanwijzingbankenbesluit/reactie/c07f5024-79ef-47bb-86ea-482ce9d16898>.

⁴ Het ontwerpbesluit vermeldt: "Uit de basisregistratie personen kunnen geen andere gegevens worden verstrekt dan: de algemene gegevens over de naam, de geslachtsnaam van de echtgenoot,

de geslachtsnaam van de echtgenoot, de eerdere echtgenoot, de geregistreerde partner of de eerdere geregistreerde partner en het gebruik door de ingeschrevene van die naam

Ook het volgende is niet in artikel 22 AMLR opgenomen:

een aanduiding dat de nationaliteit van de betrokkene niet kan worden vastgesteld

In de ontwerptoelichting is nergens te vinden waarop de verwerking van voormelde persoonsgegevens in het kader van privatisering van de misdaadbestrijding naar banken gebaseerd zou zijn. Ook wordt niet toegelicht waarom het cliëntenonderzoek van een witwasbestrijdingsplichtige (zoals een bank) deze persoonsgegevens zou moeten omvatten en waarom er een dringend belang zou zijn om deze persoonsgegevens te verifiëren via de BRP.

Commentaar Privacy First

- Er is geen wettelijke grondslag voor het verwerken door banken van persoonsgegevens van de partner (echtgenoot/geregistreerd partner, voormalige echtgenoot/geregistreerd partner), zodat deze verstrekking uit de BRP niet is toegestaan.
- Ook de verstrekking van de "aanduiding dat de nationaliteit van de betrokkene niet kan worden vastgesteld" is niet toegestaan.

De 'missende' gegevens bij inwerkingtreding van AMLR

Uit de ontwerptoelichting blijkt dat de ministeries de banken na het inwerkingtreden van AMLR (medio 2027) in staat willen stellen om de 'missende' persoonsgegevens op een goedkope manier op te halen uit de BRP, waarbij de banken de ergernis bij klanten over het onnodig opvragen van persoonsgegevens willen verminderen. Ook in de NVB-reactie is deze argumentatie aan te treffen en wordt gezegd dat dit aan de 'lastenluwheid' van de implementatie van AMLR zou bijdragen. In de ontwerptoelichting staat als een van de raadplegingsmomenten:

*- Eenmalig na inwerkingtreding van de antiwitwasverordening voor de uitvoering van de identificatie- en verificatieverplichting.*⁵

de eerdere echtgenoot, de geregistreerde partner of de eerdere geregistreerde partner en het gebruik door de ingeschrevene van die naam, de geboorteplaats, de geboortedatum, nationaliteit of nationaliteiten, dan wel een aanduiding dat de betrokkene geen nationaliteit bezit, of een aanduiding dat de nationaliteit van de betrokkene niet kan worden vastgesteld, het burgerservicenummer en het adres."

⁵ Paragraaf 3.3 ontwerptoelichting.

In de ontwerptoelichting wordt niet duidelijk uitgelegd welke persoonsgegevens zouden missen en waarom die persoonsgegevens van belang zouden zijn voor identificatie en verificatie. Ook de relevantie van de ontbrekende gegevens voor de misdaadbestrijding wordt niet toegelicht. Deze toelichting is evenmin in de NVB-reactie te vinden.

De persoonsgegevens die de bank moet registreren

Op grond van de huidige antiwitwasregels moeten witwasbestrijdingsplichtigen zoals banken de volgende persoonsgegevens registreren en verifiëren: ⁶

1. geslachtsnaam
2. voornamen
3. geboortedatum
4. adres en woonplaats
5. aard, nummer, datum en plaats van uitgifte van het identiteitsbewijs.

Privacy First wijst erop dat deze gegevens, die een burger kan aantonen door een paspoort of identiteitskaart te tonen, voldoende zijn om de identiteit van de persoon vast te stellen.

In artikel 22 AMLR worden daar de navolgende persoonsgegevens aan toegevoegd:

6. geboorteplaats
7. nationaliteiten / staatloosheid, vluchtelingenstatus of subsidiaire beschermingsstatus
8. nationaal identificatienummer
9. fiscaal identificatienummer.

Nationaliteit

Privacy First attendeert erop dat als iemand de Nederlandse nationaliteit heeft, een eventuele andere nationaliteit niet in de BRP geregistreerd mag worden. Recent is daarover

⁶ Artikel 33 lid 2 Wet ter voorkoming van witwassen en financieren van terrorisme.

door de rechtbank Rotterdam een uitspraak gewezen.⁷

Voorts wijst Privacy First erop dat de geboorteplaats geen aanwijzing geeft over de nationaliteit. Dit is ook niet het geval bij mensen die in de Verenigde Staten zijn geboren, aangezien zij die nationaliteit via een andere weg dan het certificaat van afstand (CLN) verloren kunnen hebben.

Geen dringende noodzaak op grond van AMLR

Privacy First wijst erop dat de inwerkingtreding van AMLR niet betekent dat de banken op die datum (10 juli 2027) alle in artikel 22 AMLR vermelde gegevens al in hun bezit moeten hebben. Hoewel de Europese wetgever vergeten is om in AMLR overgangsrecht op te nemen, blijkt uit uitspraken van Europese instanties dat de ontbrekende persoonsgegevens kunnen worden verzameld binnen de termijn van artikel 26 lid 2 AMLR, te weten vijf jaar, tenzij sprake is van een hoog-risico-cliënt.⁸

Dit betekent dat alleen al op grond van AMLR en de uitspraken van de Europese instanties er geen dringende noodzaak voor de banken is om op of kort na 10 juli 2027 de

⁷ Zie ECLI:NL:RBROT:2025:1810 (<https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2025:1810>). In paragraaf 3.3, wordt een passage uit de parlementaire geschiedenis geciteerd: "De aanleiding voor deze wijziging is het oplossen van een gevoelig maatschappelijk probleem, dat wordt veroorzaakt door de registratie van gegevens over de vreemde nationaliteit naast de Nederlandse nationaliteit in de huidige gemeentelijke basisadministratie persoonsgegevens. Het kabinet acht het ongewenst dat burgers die Nederlander zijn en tevens een of meer vreemde nationaliteiten bezitten, maar zich uitsluitend Nederlander voelen, ongewild en voortdurend, over meerdere generaties, vanuit de basisregistratie personen worden geconfronteerd met hun vreemde nationaliteit(en). Een quickscan onder gemeenten in 2009 heeft uitgewezen dat bijna 10% van de gemeenten in het jaar voorafgaand aan de quickscan klachten heeft ontvangen over de registratie van de vreemde nationaliteit(en) naast het Nederlanderschap. Tevens is in deze quickscan naar voren gekomen dat er personen zijn die zich uitsluitend Nederlander voelen en niet met een vreemde nationaliteit in de bevolkingsadministratie geregistreerd willen worden. Het kabinet meent dat de registratie van gegevens over de vreemde nationaliteit van deze personen in de Brp in lijn moet worden gebracht met de omstandigheid dat deze personen zich uitsluitend Nederlander voelen."

⁸ Zie paragraaf 2.3 *Draft RTS on Customer Due Diligence under Article 28(1) of Regulation (EU) 2024/1624* uit de EBA response to het European Commission's call for advice on six AMLA mandates, EBA/REP/2025/35, oktober 2025, <https://www.eba.europa.eu/sites/default/files/2025-10/b5a9a9aa-ce4f-4130-89a7-a19f2e791750/EBA%20response%20to%20EC%20CfA%20on%20six%20AMLA%20mandates%202025%2010%2030.pdf> en het consultatiedocument van AMLA over het cliëntenonderzoek, aangekondigd op https://www.aml.europa.eu/policy/public-consultations/consultation-draft-rti-customer-due-diligence_en, waarin wordt gezegd dat de actualisering van cliënteninformatie binnen vijf jaar moet plaatsvinden voor cliënten die geen hoog risico zijn.

ontbrekende gegevens bij klanten of de BRP op te halen.

Geen verificatie

Daar kan nog aan worden toegevoegd dat – anders dan in de ontwerptoelichting wordt opgemerkt – verificatie van de identiteit van een persoon niet kan plaatsvinden door raadpleging van de BRP. Die verificatie kan alleen plaatsvinden doordat de natuurlijke persoon het kantoor van de bank bezoekt, aldaar de overeenkomst tekent en het fysieke identiteitsbewijs toont. Alleen via die weg is een bank er *zeker* van dat er een overeenkomst is gesloten met de juiste persoon. Alle voor de bank relevante persoonsgegevens zijn zichtbaar op het identiteitsbewijs.

In de ontwerptoelichting wordt op geen enkele wijze onderbouwd dat de bank de op grond van artikel 22 AMLR missende gegevens nodig zou hebben.

Daar kan bij worden aangetekend dat paspoort en rijbewijs (als het origineel wordt ingezien) nog steeds een goede manier zijn om de identiteit te verifiëren. In de meest recente *Monitor Identiteit* (2025) wordt opgemerkt: "*Fraude met wettige identiteitsmiddelen zoals DigiD, paspoort of rijbewijs komen relatief weinig voor*" (pagina 41). Banken doen er goed aan de verificatie met een paspoort of identiteitsbewijs uit te voeren. Dat bevordert ook de inclusie, aangezien een zeer groot deel van de Nederlandse bevolking (4 à 5 miljoen personen) onvoldoende digitaal vaardig is.

In diezelfde Monitor wordt gezegd dat identiteitsfraude bij uitstek wordt gepleegd in het online domein, waarbij het gebruik van kopieën van paspoort en identiteitskaart een hoog risico oplevert.

Overigens blijkt uit de Monitor dat het aantal meldingen van identiteitsfraude bij het Centraal Meldpunt Identiteitsfraude (CMI) sterk is toegenomen (pagina 58). In 2017 waren dat er 2915. Het aantal is daarna flink opgelopen, 7115x in 2023, 6774x in 2024 en 8841x in 2025. In de helft van het aantal meldingen betreft het kopieën van identiteitsdocumenten. Dit maakt duidelijk dat het belangrijk is dat banken de verificatie van de identiteit en het aangaan van de overeenkomst zeer zorgvuldig dienen uit te voeren.

Geen relevantie voor AML/CFT en verhoging van de risico's voor burgers

Daar komt nog bij dat de nieuwe gegevens die door artikel 22 AMLR worden vereist geen relevantie hebben voor de misdadbestrijding. Uit de geboorteplaats van een persoon kan niet worden afgeleid dat hij of zij crimineel is. Datzelfde geldt voor de nationaliteit, staatloosheid, vluchtelingenstatus of subsidiaire beschermingsstatus.

Ook uit de identificatienummers die alle witwasbestrijdingsplichtigen moeten registreren, kan niet worden afgeleid dat betrokkene crimineel is.

De nieuwe gegevens die op grond van artikel 22 AMLR worden gevraagd betekenen naar de mening van Privacy First een verhoging van de risico's voor burgers. Die risico's betreffen:

- (geboorteplaats en nationaliteit c.a.) toename van de kans op nationaliteitsdiscriminatie, andere vormen van discriminatie en de-risking door banken en andere witwasbestrijdingsplichtigen;
- (nationaal identificatienummer en fiscaal identificatienummer) toename van de gegevensbeschermingsrisico's door de verwerking door witwasbestrijdingsplichtigen van voormelde identificatienummers.

Het is uw ministeries bekend dat in Nederland op grote schaal wordt gediscrimineerd, wat wij in onze consultatiereactie van vorig jaar (zie noot 1 hierboven) al hebben aangegeven, wat mede door de overheid zelf wordt veroorzaakt. Uit diverse recente rapporten kan dit worden afgeleid, zoals uit het recent bekendgemaakte rapport van de Algemene Rekenkamer, *'Gevolgen groot, opbrengsten onbekend - Onderzoek naar de anti-witwasaanpak in de bankensector'* ⁹, het ECRI-rapport over Nederland ¹⁰ en het rapport *'Denkrichtingen ten behoeve van een nationaal programma tegen Discriminatie en Racisme 2025-2029'*. ¹¹

Het is op het gebied van gegevensbescherming zeer risicovol dat alle witwasbestrijdingsplichtigen gevoelige identificatienummers moeten verwerken, terwijl van die witwasbestrijdingsplichtigen maar enkelen fiscale kennis hebben (te weten belastingadviseurs, administratiekantoren en dergelijke, die deze nummers toch al verwerken omdat deze nodig zijn voor hun werkzaamheden). Een onderbouwing van de AML/CFT-noodzaak hebben wij echter nergens aangetroffen. Ook bij banken kunnen datalekken plaatsvinden, zodat het belangrijk is dat ook banken niet over niet-noodzakelijke persoonsgegevens beschikken (dataminimalisatie).

Privacy First is van mening dat de aanvulling in artikel 22 AMLR met betrekking tot extra persoonsgegevens disproportioneel is en zich zou moeten beperken tot een zeer beperkte groep ondernemingen voor wie die verwerking van specifieke persoonsgegevens

⁹ Algemene Rekenkamer, aankondiging van het rapport *Gevolgen groot, opbrengsten onbekend - Onderzoek naar de anti-witwasaanpak in de bankensector*, <https://www.rekenkamer.nl/documenten/2026/03/11/gevolgen-groot-opbrengsten-onbekend---onderzoek-naar-de-anti-witwasaanpak-in-de-bankensector>.

¹⁰ ECRI-rapport over Nederland (zesde monitoringcyclus), <https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2026D11795&did=2026D11795>.

¹¹ Denkrichtingen ten behoeve van een Nationaal Programma tegen Discriminatie en Racisme 2025-2029, <https://www.tweedekamer.nl/downloads/document?id=2025D51923>, bijlage bij de brief van 12 december 2025 https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2025D51922&did=2025D51922.

daadwerkelijk relevant is in het kader van specifieke doeleinden. Daartoe behoren banken in het kader van het uitwisselen van gegevens met de Nederlandse overheid ten behoeve van de belastingheffing (zoals nu al is toegestaan). Wij zien niet in welke toegevoegde waarde deze identificatienummers voor banken hebben in het kader van AML/CFT.

Commentaar Privacy First

- Zoals hiervoor is toegelicht, is er geen noodzaak voor de banken om eenmalig toegang te krijgen tot de BRP om op een goedkope manier de extra persoonsgegevens van artikel 22 AMLR te oogsten, nu de Europese instanties al hebben aangegeven dat banken daarvoor vijf jaar de tijd krijgen.
- Bovendien is er geen dringend belang bij de banken om zo spoedig mogelijk over die extra gegevens te beschikken, aangezien die persoonsgegevens niet relevant zijn voor AML/CFT en evenmin nodig om de identiteit van een persoon te verifiëren.

Toegang banken ten behoeve van *onboarding* en risicogebaseerde extra verificatie

De NVB heeft niet alleen om toegang verzocht om de 'achterstand' bij te werken, vanwege de extra persoonsgegevens waar artikel 22 AMLR om vraagt. Uit de ontwerptoelichting blijkt dat de banken ook toegang wensen:

- *Bij het aangaan van een nieuwe klantrelatie met een nieuwe klant (ook wel onboarding genoemd)*
- *Periodiek op basis van het risicoprofiel van een klant.*

Redenen voor toegang

Onboarding

In de ontwerptoelichting wordt niet aangegeven waarom bij *onboarding* toegang tot de BRP nodig zou zijn voor de op grond van artikel 22 AMLR te vergaren informatie, nu de noodzakelijke persoonsgegevens:

- al blijken uit het paspoort of identiteitskaart;
- diverse gegevens niet in de BRP aanwezig zijn (zoals andere nationaliteiten dan de Nederlandse, of woonplaats buiten Nederland).

De ontwerptoelichting beperkt zich tot algemene teksten over het cliëntenonderzoek in het algemeen, maar geeft geen onderbouwing van de noodzaak voor toegang tot de BRP. Wij troffen die onderbouwing ook niet aan in de NVB-reactie.

Risicogebaseerde extra toegang

Al helemaal onbegrijpelijk is dat banken op basis van het risicoprofiel van natuurlijke personen de BRP opnieuw willen raadplegen. Immers, een deel van de op grond van AMLR vereiste persoonsgegevens is onveranderlijk en het deel dat wel veranderlijk is, is niet relevant voor de misdaadbestrijding. Voor zover er strafvervolgning wordt ingesteld, hebben de autoriteiten voldoende eigen bronnen, zodat een schaduw-BRP bij de banken niet nodig is. Ook in de NVB-reactie is nergens onderbouwd wat de 'risicogebaseerde' toegang precies inhoudt en waarom de BRP geraadpleegd zou moeten worden.

In de ontwerptoelichting is geen enkele onderbouwing van deze toegang aan te treffen. Privacy First wijst erop dat de risicogebaseerde actualisering van het cliëntenonderzoek op grond van de huidige en toekomstige antiwitwaswetgeving inhoudt dat de banken nagaan of er feiten of omstandigheden zijn die er op wijzen dat hun klant bij crimineel handelen betrokken is of crimineel geld onder zich heeft. De gegevens in de BRP zijn voor die risicogebaseerde actualisering irrelevant.

Doos van Pandora: alle witwasbestrijdingsplichtigen willen toegang

Voorspelbaar is dat als de banken toegang krijgen tot de BRP, alle andere witwasbestrijdingsplichtigen dit ook willen. Wij zagen dat het Verbond van Verzekeraars in hun consultatiereactie reeds meldt dat ook zij toegang tot de BRP wensen. Inmiddels is ook bepleit dat buitenlandse banken en overige betaaldienstverleners toegang krijgen tot de BRP.

Een onderbouwing van de noodzaak om banken toegang te geven ontbreekt, zoals al hiervoor is toegelicht. Dat banken op grote schaal persoonsgegevens van Nederlandse burgers verwerken is geen goede reden. Dit is ook geen reden voor verzekeraars en andere financiële instellingen.

NB: het Verbond van Verzekeraars meent ten onrechte dat actualisering van het cliëntenonderzoek betekent dat periodieke *heridentificatie* moet plaatsvinden. Dat is een bekend *compliance*-spreekje dat onjuist is. Actualisering van het cliëntenonderzoek betekent dat de elementen die relevant zijn voor bepaling van het risicoprofiel van iedere klant periodiek moeten worden gecontroleerd. Daarvoor zijn de gegevens van artikel 22 AMLR niet relevant.

Eigen regie van de burger en ergernis over het cliëntenonderzoek door banken

Het is zorgelijk dat uw ministeries aan de burger de eigen regie over de gegevensverstrekking willen ontnemen, terwijl het de kern van de AVG is dat een betrokkene weet welke persoonsgegevens over hem/haar worden verstrekt aan een verwerkingsverantwoordelijke zoals de bank. Die eigen regie voorkomt ook dat criminelen rekeningen op andermans naam openen bij banken. Wij begrijpen dat het de bank financiële voordelen biedt als zij geautomatiseerd overheidsgegevens kunnen raadplegen. Het is echter ongewenst dat banken die gegevens achter iemands rug om kunnen raadplegen, zonder dat er een noodzaak is (zoals hiervoor is toegelicht) en zonder dat de betreffende burger voorafgaand aan die raadpleging wordt geïnformeerd.

Privacy First is verontrust over de passages in de toelichting waarin door uw ministeries wordt gezegd dat de toegang voor de banken de inclusie zou bevorderen, *de-risking* zou voorkomen en de ergernis van burgers over het optreden van banken zou verminderen. Gelijksortige teksten zijn ook in de NVB-reactie te vinden. Uw ministeries en de NVB behoren te weten dat de problemen die banken met hun klanten ondervinden niet te maken hebben met basisgegevens als naam en adres, maar met alle overige informatie die banken van klanten willen hebben, zoals deze vreemde vraag van een Nederlandse grootbank aan een gepensioneerde burger:

Welke geldstromen verwacht u dat komend jaar via uw rekeningen lopen? Geef een specifieke indicatie van deze bedragen en leg per rekeningnummer uit waarvoor ze bedoeld zijn.

Dit is slechts één voorbeeld van de vele vreemde vragen die banken aan burgers hebben gesteld.

Het achter de rug van burgers opvragen van persoonsgegevens uit de BRP gaat dit probleem niet oplossen. Uw ministeries en de NVB dienen zich te realiseren dat het onbegrip bij burgers over het cliëntenonderzoek op grond van de AML/CFT-regels toeneemt, aangezien niet kan worden onderbouwd dat deze grootschalige en zeer riskante gegevensverwerking resultaat oplevert (zoals uit het eerder genoemde rapport van de Algemene Rekenkamer blijkt). De gegevensbeschermingsrisico's als gevolg van de AML/CFT-regelgeving groeien exponentieel. Dat betekent dat iedere vorm van nieuwe gegevensuitwisseling op grond van die regels een gedetailleerde en overtuigende onderbouwing vereist. Die onderbouwing wordt in de onderhavige consultatie niet gegeven.

Wij herhalen nogmaals: verificatie van de identiteit verloopt niet via de BRP. Die verificatie vindt plaats doordat de bank een origineel identiteitsbewijs inziet en daarvan de gegevens noteert. Bovendien zal de bank moeten verifiëren of zij met de juiste persoon de overeenkomst is aangegaan.

Op het gebied van verificatie kan het Europese inlogmiddel, ook bekend als Europese digitale identiteit, eID, EUDI-wallet of EDI-wallet, een rol gaan spelen als dat inlogmiddel daadwerkelijk vrijwillig is ¹² en op de juiste manier is ingericht (onder andere *privacy by design*) ¹³. De EUDI-wallet is niet alleen inlogmiddel, maar kan ook functioneren als een digitale kaartenbak, waarin geverifieerde persoonsgegevens (afkomstig uit overheidsbronnen) kunnen worden opgenomen, die via de wallet aan de bank kunnen worden verstrekt.¹⁴ Digitaal vaardige burgers die de risico's van de EUDI-wallet overzien, kunnen via de wallet gegevens aan de bank verstrekken. Dat is een veel betere weg dan toegang tot de BRP, zoals terecht in deze consultatie door Bart Jacobs en Mattis van 't Schip wordt opgemerkt.¹⁵

Commentaar Privacy First

- Bij *onboarding* ontbreekt de noodzaak voor toegang tot de BRP. De bank zal zich er van moeten overtuigen dat zij een overeenkomst aangaat met de juiste persoon. Voor die overtuiging is de BRP irrelevant.
- De 'risicogebaseerde' toegang van de banken is op geen enkele wijze onderbouwd.
- De Doos van Pandora wordt opengetrokken door banken toegang tot de BRP te verschaffen. Het is ongewenst dat alle witwasbestrijdingsplichtigen met omvangrijke groepen natuurlijke personen als klant aan de deur van de BRP gaan kloppen.
- Banken behoren niet achter de rug van de klant om de BRP te kunnen raadplegen, nu er geen noodzaak is en digitaal vaardige burgers indien zij dat wensen van de EUDI-wallet gebruik kunnen maken (als die wallet goed zou zijn ingericht).

Voorts - geheel ten overvloede als aan banken toegang tot de BRP zou worden toegestaan (waar Privacy First mordicus op tegen is):

¹² Zie het artikel *Brandbrief Privacy First over verplichtstelling Europese digitale identiteit bij banken* d.d. 9 maart 2026, <https://privacyfirst.nl/artikelen/brandbrief-privacy-first-over-verplichtstelling-europese-digitale-identiteit-bij-banken/> en onze open brief https://privacyfirst.nl/wp-content/uploads/open_brief_SPF_EUDI-wallet_AMLA_9maart2026.pdf.

¹³ Op dit moment is Privacy First er nog niet zeker van of het Europese inlogmiddel wel goed is ingericht, zie onder andere de kritiek van EDRI, *The eID Wallet still doesn't deserve your full trust*, <https://edri.org/our-work/the-eid-wallet-still-doesnt-deserve-your-full-trust/>.

¹⁴ Die persoonsgegevens kunnen ook worden beperkt, zoals bijvoorbeeld bij de geboortedatum: de wallet moet het bijvoorbeeld mogelijk maken dat een ontvangende partij alleen een bevestiging ontvangt dat de betrokkene ouder dan 18 jaar is.

¹⁵ Reactie Radboud Universiteit (B.P.F. Jacobs & M. van 't Schip), <https://www.internetconsultatie.nl/derdenaanwijzingbankenbesluit/reactie/1d5822f0-e6e3-4dd2-af4c-d801608307fa>.

- behoort dat uitsluitend voor een zeer beperkte set aan gegevens plaats te vinden met een ja/nee systeem (de BRP bevestigt alleen dat het door de bank aangedragen persoonsgegevens wel of niet juist is);
- wordt alleen aan de AVG voldaan als de BRP voorafgaand aan iedere gegevensafgifte toestemming aan de betrokkene vraagt, zodat deze kan verifiëren of de bank op juiste gronden iets aan de BRP vraagt;
- worden er een groot aantal extra maatregelen genomen die er voor zorgen dat kan worden gemonitord of banken daadwerkelijk alleen gegevens van hun eigen klanten opvragen, er geen bankmedewerkers met *fishing expeditions* bezig zijn en de AVG ook in andere opzichten wordt nageleefd;
- vindt er intensief toezicht plaats door de Autoriteit Persoonsgegevens (AP) op de naleving door banken van de AVG, met onmiddellijke handhavingsmaatregelen als er gebreken zijn;
- vanwege het grote maatschappelijke belang van correcte naleving door financiële instellingen van de AVG, komen de kosten van de AP voor het toezicht bij financiële instellingen voor rekening van die instellingen.

Maar – zoals gezegd – de afgifte van deze gegevens aan banken is volgens Privacy First niet nodig en disproportioneel.

Extra wensen van de NVB

In de consultatiereactie laat de NVB weten dat zij extra wensen heeft inzake de toegang tot de BRP. Zo wenst de NVB dat banken BRP-gegevens over de gezagsrelatie met gemachtigden (zoals ouder-kind, wettelijke vertegenwoordiging) kan raadplegen. Anders dan door de NVB opgemerkt, is in AMLR niet opgenomen dat dergelijke gegevens verplicht geregistreerd moeten worden. Dat betekent dat er geen grondslag in de witwasbestrijdingsregels is die vereist dat banken deze persoonsgegevens mogen verwerken. Als er speciale maatregelen nodig zouden zijn, horen die niet thuis in het BRP-besluit. Voorts wordt door de NVB opgemerkt dat banken UBO-gegevens uit de BRP willen kunnen halen omdat het UBO-register onvoldoende zou zijn en wenst de NVB persoonsgegevens van vertegenwoordigers van entiteiten die klant zijn te kunnen raadplegen (terwijl die gegevens bij Nederlandse entiteiten in het Handelsregister staan). Overigens gaat de NVB niet in op de vraag of alle gewenste gegevens wel in de BRP zijn opgenomen en waarom het UBO-register en het Handelsregister geen goede informatiebron zouden zijn.

De wensen van de NVB laten zien dat de persoonsgegevensbehoefte van banken ongelimiteerd is, zonder dat wordt onderbouwd dat er enige noodzaak is.

Overige opmerkingen

Tot slot nog enkele detailopmerkingen (onverlet dat wij tegen de voorgestelde toegang zijn):

- **'Beperking':** ten onrechte wordt de suggestie gewekt dat slechts 'bepaalde' banken toegang zouden krijgen tot de BRP. Het gaat om alle in Nederland gevestigde banken, inclusief de grootbanken die het grootste deel van de burgers in Nederland bedienen. Het gaat hier om grootschalige gegevensuitwisseling, waarvoor de wet op dit moment geen juridische grondslag biedt.
- **'Beperking':** ten onrechte wordt de suggestie gewekt dat het om beperkte persoonsgegevens zou gaan. Zoals hiervoor is opgemerkt, gaat het om een grootschalige data-uitwisseling die alle Nederlanders betreft.
- **'Veiligheid':** ten onrechte wordt de suggestie gewekt dat er een veiligheidsbelang zou zijn. De gegevens uit de BRP zijn echter niet relevant voor de primaire activiteit van banken, namelijk het verifiëren dat zij met de juiste persoon een overeenkomst aangaan. Dat is een uitwisseling met de klant, niet met de BRP. Het rechtstreeks raadplegen door banken is juist een veiligheidsrisico voor de klant, want het betekent dat een crimineel op naam van een ander een overeenkomst kan aangaan en dat de bank zonder de betrokkene te informeren de persoonsgegevens raadpleegt.
- **'Transparantie':** dit betekent voor uw ministeries kennelijk dat de uitwisseling van persoonsgegevens ergens is verstoppt op de websites van de banken en/of de overheid (paragraaf 3.5 ontwerptoelichting). Dat is niet de transparantie die de AVG beoogt. Transparantie is dat de betrokkene vooraf om toestemming wordt gevraagd.
- **Autorisatiebesluit:** in de ontwerptoelichting staat dat de minister van BZK per bank een autorisatiebesluit neemt, kennelijk gericht op alle 'geautoriseerde banken'. Dat besluit bevat kennelijk nieuwe persoonsgegevens, want de toelichting spreekt over "*welke gegevens, van welke personen, op welk moment, en op welke wijze*". Dit is onbegrijpelijk, in strijd met de AVG en biedt ruimte voor ongewenste praktijken. Als banken al toegang zouden krijgen (waar Privacy First op tegen is) hoort de uitwerking daarvan in regelgeving plaats te vinden. Via deze autorisatiebesluiten zouden de banken toegang kunnen krijgen tot andere persoonsgegevens dan nu in het ontwerpbesluit genoemd zijn. Dat is in strijd met de AVG, onnodig en zeer ongewenst.

Tot slot

Privacy First is van mening dat het verschaffen van toegang tot het BRP aan banken en andere witwasbestrijdingsplichtigen ongewenst is, nu het disproportioneel is, geen bijdrage levert aan de misdaadbestrijding en niet voldoet aan de AVG en het Europese Handvest.



Wij adviseren u van het voornemen af te zien.

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