

Geachte heer/mevrouw,

Naar aanleiding van uw eerdere reacties en het uitblijven van een reactie op mijn verzoek om verder uitstel, schrijf ik u nogmaals.

Op 12 mei en opnieuw op 26 mei heb ik ASN verzocht om uitstel van de door ASN gestelde termijn van 31 mei 2026. Daarbij heb ik toegelicht dat beantwoording van mijn vragen en beoordeling door rechtsbijstand meer tijd vragen. Tot op heden heb ik op dit verzoek geen reactie ontvangen.

Dat vind ik bijzonder, juist omdat ASN in dit traject spreekt over mogelijke blokkade of beperking van toegang tot een bestaande betaalrekening. Wanneer een bank een dergelijke maatregel in het vooruitzicht stelt, mag van die bank worden verwacht dat zij zorgvuldig en tijdig reageert op een gemotiveerd verzoek om uitstel.

Voor de duidelijkheid herhaal ik mijn uitgangspunt.

Wij weigeren identificatie of verificatie niet. Ons bezwaar richt zich op de specifieke digitale en externe verificatieroute die ASN wil afdwingen, met digitale vastlegging, verwerking via AMP, NFC/OCR, betrokkenheid van meerdere partijen en langdurige opslag van gevoelige identificatiegegevens.

De kernvraag blijft:

Welke identificatie- en verificatiehandeling is wettelijk noodzakelijk, en welk deel is een beleidsmatige verzwaaring door ASN? Als de Wwft verplicht tot identificatie en verificatie, waarom zou persoonlijke verschijning met een geldig paspoort of identiteitsbewijs in een ASN-kantoor dan niet volstaan, en waarom zijn aanvullende digitale verwerkingen zoals NFC/OCR, chipuitlezing en verwerking via AMP volgens ASN noodzakelijk?

Daarbij maak ik onderscheid tussen identificatie, verificatie en de wijze waarop ASN bewijs daarvan wil vastleggen en bewaren.

## 1. Identificatie is niet hetzelfde als de gekozen verwerkingsroute

ASN verwijst meerdere keren naar de Wwft en stelt dat zij moet weten wie haar klanten zijn, dat zij de identiteit van klanten moet vaststellen en verifiëren en dat klantgegevens actueel moeten zijn.

Dat doel betwisten we niet.

Wat we betwisten, is de stap die ASN daarna maakt. Uit het algemene doel van cliëntenonderzoek volgt niet automatisch dat juist deze digitale of externe route, met digitale kopie, NFC/OCR, AMP-apparatuur en ketenverwerking, noodzakelijk is.

Het uitlezen van een chip zegt op zichzelf niets over de integriteit van een klant. Het kan hooguit iets zeggen over de authenticiteit van een document of de juistheid van bepaalde gegevens. ASN lijkt deze onderdelen door elkaar te laten lopen.

Het gebruik van de term “ID-check” mag niet verhullen dat verschillende handelingen samenkomen: identificatie van de persoon, verificatie van het document, technische uitlezing, gegevensverwerking en bewijsopslag. Ons bezwaar gaat niet over de identificatie, maar over de zware digitale verwerking die ASN daaraan koppelt.

Wanneer het doel is om vast te stellen wie de klant is, blijft onduidelijk waarom persoonlijke verschijning op een ASN-kantoor met een geldig identiteitsdocument niet zou volstaan. Zeker nu ASN identificatie “in persoon” via een AMP-medewerker wel accepteert.

Daarom verzoek ik ASN concreet toe te lichten waarom fysieke controle door een AMP-medewerker wel voldoende wordt geacht, terwijl fysieke controle door een ASN-medewerker op een ASN-kantoor niet als gelijkwaardig of minder ingrijpend alternatief wordt beoordeeld.

## 2. “Digital first” is beleid, geen wettelijke verplichting

In uw eerdere reactie heeft ASN aangegeven dat zij werkt vanuit een “digital first” werkwijze. Ook heeft ASN verwezen naar factoren als “iets wat je hebt”, “iets wat je weet” en “iets wat je bent”.

In mijn vervolgvragen heb ik daarom expliciet gevraagd of de door ASN gekozen route in dit traject primair een beleidskeuze is, of dat wet- en regelgeving deze specifieke methode voorschrijft.

ASN heeft daarop geantwoord dat banken zelf mogen bepalen welke methode zij inzetten, zolang deze betrouwbaar is, aan de wet voldoet en identiteitsfraude voorkomt. Daarbij schrijft ASN ook dat dit een beleidsmatige keuze is die binnen haar bevoegdheid valt.

Vervolgens heeft ASN aangegeven niet in te gaan op mijn vragen over de vergelijking met een kantoorroute of over de onderbouwing van het beleid.

Juist dat is voor mij de kern van het probleem.

Als ASN erkent dat de gekozen methode een beleidsmatige keuze is, dan moet ASN ook kunnen uitleggen hoe die keuze zich verhoudt tot noodzakelijkheid, proportionaliteit, subsidiariteit en dataminimalisatie.

Beleidsruimte is immers geen vrijbrief. Een wettelijke verplichting om cliëntenonderzoek te doen betekent niet automatisch dat iedere zelfgekozen uitvoeringswijze zonder nadere onderbouwing en toetsbare belangenafweging aan de klant kan worden opgelegd. Ook binnen beleidsruimte moet de gekozen methode voldoen aan de Wwft, de AVG, proportionaliteit, subsidiariteit, dataminimalisatie, zorgplicht en klantbelang.

Ik verzoek ASN daarom alsnog concreet te onderbouwen waarom haar “digital first” beleid in dit dossier zwaarder zou mogen wegen dan een minder ingrijpende fysieke verificatieroute.

ASN beroept zich herhaaldelijk op wettelijke verplichtingen, protocollen en beleidsruimte. Daarmee blijft echter de wezenlijke vraag onbeantwoord.

Het gaat mij niet om de vraag of ASN de klant mag identificeren. Dat moet, en dat begrijp ik. Het gaat om de vraag of ASN haar eigen beleidsmatige invulling van dat cliëntenonderzoek mag behandelen alsof deze specifieke uitvoeringsroute zelf wettelijk verplicht is.

Daar wringt het.

ASN lijkt algemene wettelijke doelen, zoals weten wie de klant is, klantgegevens actueel houden en het financiële stelsel beschermen, te gebruiken als onderbouwing voor een digitale en externe technische werkwijze. Maar uit die doelen volgt nog niet automatisch dat NFC/OCR, chipuitlezing, verwerking via AMP, digitale ketenverwerking en langdurige opslag noodzakelijk zijn.

Juist omdat toegang tot een bestaande betaalrekening op het spel staat, kan ASN niet volstaan met algemene verwijzingen naar “de wet” of “ons beleid”. De door ASN gekozen route wordt feitelijk afgedwongen doordat weigering van deze specifieke methode kan leiden tot beperking van toegang tot betalingsverkeer. Daarmee wordt de beleidskeuze van ASN voor de klant praktisch dwingend, terwijl de noodzaak van die keuze niet inhoudelijk is onderbouwd.

Ik verzoek ASN daarom niet opnieuw algemeen te verwijzen naar de Wwft, maar concreet aan te geven welk wettelijk voorschrift volgens ASN welk onderdeel van deze route noodzakelijk maakt.

### 3. Fysieke identificatie op kantoor wordt door ASN zelf genoemd

Op de website van ASN wordt in andere situaties wel verwezen naar identificatie in een ASN-kantoor, bijvoorbeeld bij het wijzigen of controleren van persoonsgegevens of accountgegevens. Daarbij wordt fysieke verschijning op kantoor kennelijk wél als passende route genoemd.

Daar komt bij dat uit mijn eigen ervaring op kantoor blijkt dat identificatie zelfs aan de hand van een rijbewijs werd geaccepteerd om gegevens in te zien of te controleren.

Dat maakt het onderscheid in dit dossier nog moeilijker te volgen.

Als ASN op kantoor kan vaststellen wie een klant is bij het wijzigen of controleren van persoonsgegevens of accountgegevens, waarom zou fysieke verschijning op kantoor met een geldig paspoort of identiteitsbewijs dan niet kunnen volstaan bij heridentificatie?

### 4. Een afschrift bewaren is niet hetzelfde als chipuitlezing of NFC/OCR verplichten

ASN stelt dat zij op grond van artikel 33 Wwft in samenhang met artikel 40 van de vierde anti-witwasrichtlijn een volledig afschrift van het identiteitsbewijs moet bewaren.

Zelfs als ASN meent dat zij een volledig afschrift moet bewaren, volgt daar nog niet automatisch uit dat dit afschrift uitsluitend via NFC/OCR, chipuitlezing, AMP-apparatuur of externe digitale verwerking tot stand moet komen.

De gegevens die ASN in haar reactie noemt als gegevens die via AMP worden verwerkt, zijn grotendeels gegevens die zichtbaar zijn op het identiteitsdocument of die bij fysieke verschijning op kantoor kunnen worden gecontroleerd en, voor zover wettelijk noodzakelijk, vastgelegd. Het gaat onder meer om voornamen, geboortedatum, documentnummer, datum van uitgifte, geldigheidsdatum, nationaliteit, BSN, geboorteplaats, adresgegevens en handtekening.

Voor die gegevens is niet zonder meer duidelijk waarom NFC/OCR, chipuitlezing, AMP-apparatuur en externe digitale verwerking noodzakelijk zijn.

Ook als ASN stelt dat de eerdere afgeleide identificatie niet langer volstaat en dat een afschrift ontbreekt, volgt daar nog niet uit dat heridentificatie uitsluitend via NFC/OCR, chipuitlezing, AMP of een externe digitale route moet plaatsvinden.

Als ASN stelt dat zij bepaalde gegevens of een afschrift van het identiteitsbewijs moet bewaren, zijn we bereid te bespreken hoe dit op een minder ingrijpende manier kan worden uitgevoerd.

Bijvoorbeeld door fysieke controle op kantoor en, voor zover wettelijk noodzakelijk, een statisch afschrift of foto van het zichtbare identiteitsdocument.

Ik verzoek ASN daarom concreet toe te lichten:

1. uit welke wettelijke bepaling volgt dat een afschrift van het identiteitsbewijs via NFC/OCR of chipuitlezing moet worden verkregen;
2. waarom een statisch afschrift of foto van het zichtbare identiteitsdocument niet zou volstaan;
3. waarom fysieke controle op kantoor niet kan worden gecombineerd met vastlegging van uitsluitend de minimaal noodzakelijke gegevens;
4. waarom het uitlezen van een chip noodzakelijk is wanneer een origineel identiteitsdocument fysiek wordt getoond aan een medewerker.

Daarbij wijs ik erop dat Privacy First in haar [brief van 1 juni 2026 aan de Tweede Kamer](#) schrijft dat zij geen juridische basis heeft kunnen vinden voor toegang door banken en derden tot de beveiligde omgeving van het identiteitsbewijs. Ook stelt Privacy First dat de huidige witwaswetgeving volgens haar niet voorschrijft dat kopieën van identiteitsbewijzen en biometrische persoonsgegevens door banken of andere Wwft-plichtigen bewaard moeten worden.

Dat onderstreept dat mijn vragen niet individueel of theoretisch zijn, maar raken aan een bredere juridische en maatschappelijke discussie.

## 5. Paspoort, identiteitsbewijs en toegang tot chipgegevens

In dit dossier speelt ook de vraag hoe de door ASN gekozen werkwijze zich verhoudt tot de functie van het paspoort en de daarin opgenomen gegevens.

Een belangrijke functie van een paspoort of identiteitsbewijs is dat iemand daarmee zijn identiteit kan aantonen. Fysiek tonen van een geldig document is daarom geen vrijblijvende of zwakke vorm van identificatie, maar juist de normale functie van het document. Als ASN stelt dat fysieke controle van een geldig identiteitsdocument op kantoor onvoldoende is en dat daarnaast chipuitlezing, NFC/OCR of verwerking via een externe partij noodzakelijk is, verzoek ik ASN concreet aan te geven op welke wettelijke bepaling die aanvullende verplichting berust.

Daarbij verzoek ik ASN ook toe te lichten waarom het tonen van een geldig paspoort of identiteitsbewijs op een ASN-kantoor onvoldoende zou zijn om de identiteit vast te stellen en te verifiëren.

## 6. De AMP-route is geen eenvoudige fysieke identificatie

ASN presenteert AMP als alternatief omdat daarbij volgens ASN geen gezichtsscan en geen biometrische verwerking plaatsvinden.

Dat neemt onze bezwaren echter niet weg.

De AMP-route neemt hooguit één onderdeel weg, namelijk de technische gezichtsscan via de app. Het bredere bezwaar blijft bestaan. Ook bij AMP is sprake van digitale vastlegging, een digitale foto of kopie van het identiteitsbewijs, verwerking via een externe partij, NFC/OCR, betrokkenheid van meerdere partijen en langdurige opslag van gegevens bij ASN.

ASN heeft zelf aangegeven dat AMP altijd werkt met NFC of OCR. ASN heeft ook aangegeven dat NFC bijdraagt aan betrouwbaarheid.

Maar “draagt bij aan betrouwbaarheid” is niet hetzelfde als “wettelijk verplicht”.

Als iemand persoonlijk met een origineel paspoort of identiteitsbewijs op een ASN-kantoor verschijnt, is dat ook een betrouwbare manier om identiteit te controleren. Bovendien kan die route juist minder ingrijpend zijn, omdat er minder externe partijen, minder technische schakels en minder gegevensstromen nodig zijn.

Dan ligt het op de weg van ASN om concreet te onderbouwen waarom de AMP-route noodzakelijk is en waarom een fysieke kantoorroute niet zou volstaan.

## 7. Externe keten, datarisico en zorgplicht

In uw beantwoording noemt ASN bij de AMP-route meerdere betrokken partijen en subverwerkers. Daarbij worden onder meer AMP, Microsoft, Tableau, hostingpartijen en overige subverwerkers genoemd. Bij Microsoft en Tableau vermeldt ASN dat gegevensverwerking binnen de EER plaatsvindt, maar dat deze partijen in de Verenigde Staten gevestigd zijn.

Dat maakt de keten complexer dan een eenvoudige fysieke controle op een ASN-kantoor.

Juist daarom blijft de vraag waarom ASN deze zwaardere route noodzakelijk acht. Elke extra partij en elke extra technische schakel vergroot de complexiteit, het afhankelijkheidsrisico en de vraag wie uiteindelijk verantwoordelijkheid draagt als er iets misgaat.

Daarbij blijft ook onduidelijk hoe ASN de betrouwbaarheid en integriteit van deze externe uitvoeringsketen toetst. Wordt AMP periodiek onafhankelijk gecontroleerd of geaudit? Hoe worden AMP-medewerkers gescreend? Hoe kan de klant bij een afspraak controleren dat de medewerker en de gebruikte apparatuur betrouwbaar zijn? En hoe kan de klant verifiëren welke gegevens daadwerkelijk met ASN worden gedeeld?

ASN vraagt om langdurige vastlegging van een omvangrijk identiteitsdossier. Tegelijk geeft ASN geen concrete duidelijkheid over mijn positie wanneer die gegevens betrokken raken bij een beveiligingsincident. ASN schrijft dat zij per geval beoordeelt of zij gebruikmaakt van de uitzondering uit artikel 42 UAVG en dat zij geen toelichting kan geven op dit interne beoordelingsproces. Ook op de vraag naar aansprakelijkheid of compensatie bij een beveiligingsincident gaat ASN niet inhoudelijk in.

Daarmee ontstaat een onevenwichtige risicoverdeling.

In de praktijk vraagt ASN om gevoelige identificatiegegevens langdurig af te staan als voorwaarde om toegang tot bestaande bankdiensten te behouden. Tegelijk blijft onduidelijk welke concrete bescherming, informatieplicht, herstellmogelijkheid of compensatie daar tegenover staat wanneer deze gegevens verloren raken, worden misbruikt of onbedoeld worden verspreid.

ASN kiest voor een zwaardere gegevensverwerking om haar eigen aantoonplicht in te vullen, terwijl de klant langdurig het risico draagt van verlies, misbruik of verspreiding van die gegevens.

Als klant moeten wij in belangrijke mate vertrouwen op de uitleg van ASN over de oorzaak, impact en afhandeling van digitale incidenten. Juist daarom is transparantie over risico's, verantwoordelijkheden en informatieplicht essentieel wanneer ASN van klanten verlangt dat zij gevoelige identificatiegegevens via digitale routes laten verwerken.

Ik verzoek ASN daarom alsnog concreet toe te lichten:

1. wanneer wij persoonlijk worden geïnformeerd bij een datalek of beveiligingsincident met onze identificatiegegevens;
2. welke herstelmogelijkheden er dan zijn;
3. welke aansprakelijkheid ASN erkent wanneer schade ontstaat door verlies, misbruik of verspreiding van deze gegevens;
4. hoe ASN het langdurige risico voor de klant meeweegt bij de keuze voor deze methode.

Ik ben mij ervan bewust dat ik vragen over datalekken, aansprakelijkheid en risicoverdeling eerder aan ASN heb voorgelegd. Juist omdat het hier gaat om langdurige vastlegging van gevoelige identificatiegegevens, neem ik echter geen genoegen met de mededeling dat ASN geen toelichting geeft op interne beoordelingsprocessen of niet ingaat op aansprakelijkheid en compensatie. Wanneer ASN deze gegevensverwerking noodzakelijk acht, moet ASN ook concreet kunnen uitleggen welke bescherming, informatie en verantwoordelijkheid daar voor de klant tegenover staan. Dat raakt rechtstreeks aan de zorgplicht van de bank en aan de vraag hoe ASN het belang van haar eigen aantoonplicht afweegt tegen het langdurige risico dat de klant draagt.

## 8. Gezamenlijke rekening en druk op de mede-rekeninghouder

ASN heeft aangegeven dat bij een en/of-rekening beide rekeninghouders compliant moeten zijn en dat de andere rekeninghouder ook de gevolgen ervaart wanneer één rekeninghouder zich niet tijdig identificeert.

Dat betekent dat zelfs wanneer mijn eigen identificatie op orde is, mijn toegang tot onze gezamenlijke rekening kan worden beperkt wanneer mijn man niet verantwoord kan instemmen met de door ASN gekozen methode zolang de noodzaak, proportionaliteit en risico's daarvan onvoldoende zijn onderbouwd.

Dit vergroot de druk aanzienlijk.

Daarmee wordt niet alleen mijn mans keuzevrijheid beperkt, maar wordt ook mijn toegang tot gezamenlijk geld afhankelijk gemaakt van zijn bereidheid of mogelijkheid om een specifieke, door ons betwiste gegevensverwerkingsroute te doorlopen.

Ik verzoek ASN daarom concreet toe te lichten waarom het proportioneel is om ook de mede-rekeninghouder te raken, terwijl het bezwaar niet gaat over identificatie als zodanig maar over de gekozen methode.

Welke minder ingrijpende maatregelen heeft ASN overwogen om te voorkomen dat een mede-rekeninghouder, van wie de eigen identificatie op orde is, wordt geraakt door blokkade of beperking van toegang?

## 9. De aangehaalde jurisprudentie vraagt om concrete duiding

ASN verwijst in haar reactie naar verschillende uitspraken van rechtbank, hof, de Advocaat-Generaal, de Hoge Raad en Kifid.

Ik verzoek ASN concreet toe te lichten in hoeverre deze uitspraken zien op dezelfde feitelijke situatie als mijn dossier.

Mijn situatie betreft een bestaande gezamenlijke betaalrekening, een betwiste heridentificatie, een door ASN geweigerde kantoortroute, verwerking via AMP, NFC/OCR, langdurige opslag van gegevens en mogelijke gevolgen voor een mede-rekeninghouder.

Niet iedere uitspraak over identificatie, een creditcard, een online-only situatie, een bewerkte kopie of een andere bank beantwoordt automatisch de vraag waarom ASN in ons geval geen minder ingrijpende fysieke route zou hoeven bieden.

Het enkel verwijzen naar eerdere uitspraken is daarom onvoldoende wanneer niet concreet wordt uitgelegd waarom die uitspraken ook deze specifieke situatie dragen.

Bovendien bevestigt de recente uitspraak van de Hoge Raad juist dat er juridische vragen openstaan over de verhouding tussen Wwft, AVG en het bewaren van kopieën of pasfoto's. Dat pleit voor zorgvuldigheid en terughoudendheid bij het afdwingen van vergaande gegevensverwerking zolang minder ingrijpende alternatieven niet inhoudelijk zijn beoordeeld. ([Hoge Raad 13 maart 2026, ECLI:NL:HR:2026:392](#))

## 10. Inconsistentie, maatwerk en doel van heridentificatie

Ik heb inmiddels signalen ontvangen van andere ASN-klienten waarbij de ID-check of heridentificatie in de praktijk anders lijkt te zijn afgehandeld dan ASN in ons dossier formeel stelt. Dat roept vragen op over consistentie, transparantie en de criteria die ASN hanteert bij maatwerk, uitstel of handmatige afronding.

Het gaat onder meer om signalen waarbij identificatie in een ASN-vestiging door een medewerker is afgerond, of waarbij een situatie telefonisch "op akkoord" zou zijn gezet nadat een klant bezwaar of moeite met de procedure had aangegeven.

Ik benoem dit niet om individuele klantdossiers te bespreken, maar omdat het raakt aan de vraag of ASN werkelijk één strikt noodzakelijke wettelijke route uitvoert, of dat er in de praktijk ruimte bestaat voor maatwerk, handmatige afronding of afwijking van de standaardroute.

Daarom verzoek ik ASN concreet toe te lichten:

1. welke objectieve criteria ASN hanteert voor maatwerk;
2. wanneer een identificatie handmatig kan worden afgerond;
3. wanneer een blokkade kan worden uitgesteld of opgeheven;
4. welke bevoegdheid ASN-medewerkers in vestigingen hebben bij identiteitscontrole of verificatie;
5. waarom in ons dossier geen minder ingrijpende of handmatige route wordt onderzocht.

Ik verzoek ASN bovendien om in haar reactie niet opnieuw te volstaan met algemene verwijzingen naar de Wwft, beleidsruimte of interne procedures, maar per onderdeel concreet aan te geven welke wettelijke bepaling, welke noodzaak en welke belangenafweging volgens ASN de gekozen methode rechtvaardigen.

**Met deze vragen wil ik helder krijgen of het doel van de heridentificatie daadwerkelijk is om vast te stellen wie de klant is, of dat de nadruk in de praktijk verschuift naar het digitaal vastleggen en bewaren van een uitgebreid identiteitsdossier.**

ASN spreekt in algemene zin over “identificeren”, maar de door ASN gekozen ID-check omvat meer dan het vaststellen wie de klant is. Het gaat immers ook om documentcontrole, digitale gegevensuitlezing, vastlegging, bewijsopbouw en langdurige opslag.

Als het doel is om vast te stellen wie de klant is, blijft fysieke verschijning op kantoor met een geldig paspoort of identiteitsbewijs een logisch, betrouwbaar en minder ingrijpend alternatief. Als ASN dat alternatief afwijst, verwacht ik een concrete onderbouwing waarom dat niet volstaat.

Als het doel daarnaast is om bewijs vast te leggen of gegevens langdurig te bewaren, dan moet ASN per onderdeel concreet onderbouwen welke wettelijke bepaling die verwerking noodzakelijk maakt, waarom die verwerking proportioneel is en waarom minder ingrijpende vastlegging niet zou volstaan.

## 11. Verzoek om inhoudelijk antwoord en opschorting

Ons bezwaar is vanaf het begin niet gericht tegen identificatie of verificatie. Ons bezwaar is gericht tegen de specifieke digitale en externe methode die ASN wil afdwingen zonder concrete onderbouwing waarom minder ingrijpende alternatieven niet volstaan.

Daarom verzoek ik ASN om ons bezwaar tegen deze specifieke digitale/externe verificatieroute niet te kwalificeren als weigering om mee te werken aan identificatie of verificatie.

Samenvattend verzoek ik ASN om schriftelijk en concreet:

1. te bevestigen dat ons bezwaar niet wordt behandeld als weigering van identificatie of verificatie;
2. te bevestigen dat geen blokkade of beperking van toegang wordt toegepast zolang deze inhoudelijke vragen niet zijn beantwoord;
3. de actuele status van de termijn na 31 mei 2026 toe te lichten;
4. per genoemd onderwerp de gestelde vragen te beantwoorden en concreet aan te geven welke wettelijke bepaling, welke noodzaak en welke belangenafweging volgens ASN de gekozen methode rechtvaardigen, zodat het beleid toetsbaar wordt aan wet, proportionaliteit, subsidiariteit, dataminimalisatie en klantbelang.

Omdat de beantwoording door ASN tot nu toe de kernvragen over wettelijke verplichting, beleidsruimte, proportionaliteit en minder ingrijpende alternatieven onvoldoende beantwoordt, heb ik inmiddels juridisch advies ingewonnen. We willen dit traject zorgvuldig voeren, maar daarvoor is het noodzakelijk dat ASN niet blijft volstaan met algemene verwijzingen naar de Wwft of beleidsruimte zonder toetsbare onderbouwing en zonder inzichtelijke belangenafweging richting de klant.

Ik zie uw inhoudelijke en concrete reactie graag tegemoet, inclusief bevestiging dat er geen blokkade of beperking van toegang wordt toegepast zolang deze vragen niet inhoudelijk zijn beantwoord.

Met vriendelijke groet,

[naam]  
mede namens [naam]