

Aan de Minister en Staatssecretaris van Economische Zaken en KlimaatBetreft: Consultatiereactie op Wetsvoorstel nummerbeleid ¹

Human Rights in Finance

Amsterdam

legal@hrif.eu

23 september 2026

De stichting Human Rights in Finance (EU) heeft met veel interesse kennisgenomen van de consultatie rond het wetsvoorstel nummerbeleid. In deze reactie leggen we de hoofdpunten van onze reactie vast en stellen we ons voor (zie ook bijlage 1). Daarna lichten we onze ervaringen en de inhoudelijke achtergrond van onze reactie toe.

We wijzen erop dat we hierbij werken vanuit een systemische analyse en kijkwijze naar maatschappij en effectieve maatschappelijke verandering. Onze reactie richt zich op de onderdelen die de identificatie van eindgebruikers en de verwerking en verstrekking van hun gegevens raken; de onderdelen suballocatie, buitenlands gebruik van nummers en nummerherkenning laten wij verder buiten beschouwing.

1. Inleiding en kern: vergaande identificatie, onbepaalde delegatie zonder dataminimalisatie-toets

HRIF.EU herkent, vanuit de financiële sector, het concept van vergaande identificatie en datadelingsmechanismen als een concept dat als panacee voor fraudebestrijding, voorkomen van witwassen en terrorismefinanciering wordt ingezet. De beleidslogica in dit voorstel bouwt op die theoretische visie voort, zonder vooraf te onderzoeken of het middel wellicht erger is dan de kwaal.

Het beleidskompas en de toelichting bij de wet zijn uitermate vaag gehouden, maar in de kern creëert het voorstel de grondslag om bij ministeriële regeling de anonieme prepaidkaart feitelijk af te schaffen en op nummerniveau te koppelen welke natuurlijke persoon welk nummer heeft gekocht/gebruikt en hoe mensen worden geïdentificeerd.² Die gegevens kunnen vervolgens worden gedeeld met partijen die de wet zelf niet noemt, zonder dat duidelijk is op welke gronden.³ Dat alles staat in nader te bepalen regelingen. De wet is daarmee een blanco cheque die de mogelijkheid tot anoniem bellen ontnemt⁴ (vergelijk: het met een muntstuk bellen vanuit een telefooncel).

Voor het functioneren van een rechtsstaat is het vrijelijk kunnen communiceren zonder id-verplichting een belangrijk vereiste. Voorkomen moet worden dat de staat, als actor die ook zélf gecompromiteerd kan worden, hierin een te grote en controlerende rol kan nemen. De vraag is daarbij of die identificatieplicht dienstbaar is aan het vermelde doel en of de nadelen niet groter zijn dan de voordelen. Verplichte identificatie en registratie vormen een inmenging in het recht op eerbiediging van de persoonlijke levenssfeer, die voorzienbaar, noodzakelijk en evenredig moet zijn.⁵

Ook ervaringen uit Frankrijk met datalekken in de cryptosector laten zien dat persoonsgegevens na een lek juist als grondstof voor nieuwe fraude worden gebruikt. De Franse overheidsdienst

¹ Voorstel van wet 'Wijziging van de Telecommunicatiewet in verband met marktontwikkelingen, de bescherming van de consument en het toezicht op het terrein van het nummerbeleid', consultatieversie 30 juni 2026, met memorie van toelichting (MvT), begeleidend document, beantwoording vragen beleidskompas en effectentoeets: <https://www.internetconsultatie.nl/nummers/b1>.

² Voorgesteld art. 4.8b, tweede lid, onder b, en derde lid, Tw. De MvT (par. 6.2) noemt het aanbod van 06-nummers met anonieme prepaidkaarten 'katalyserend' voor fraude en wijst erop dat de identiteit van deze gebruikers bij incidenten moeilijk in beeld te krijgen is.

³ Voorgesteld art. 4.8a, onder b, Tw; zie verder paragraaf 2.

⁴ Het gaat hier om anonimiteit tegenover aanbieder en overheid. De mogelijkheid om de weergave van het eigen nummer tegenover de gebelde of berichtontvanger te blokkeren, blijft in het voorgestelde art. 11.9 Tw behouden.

⁵ Art. 10 Grondwet (<https://wetten.overheid.nl/BWBR0001840>), art. 8 EVRM en art. 7, 8 en 52, eerste lid, Handvest van de grondrechten van de Europese Unie (<https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:12016P/TXT>).

Cybermalveillance.gouv.fr meldt naar aanleiding van datalekken bij crypto-operators (januari 2026) dat slachtoffers vervolgens worden benaderd door personen die zich voordoen als medewerkers van cryptobedrijven, antifraudediensten van banken of zelfs politie en justitie. In ernstige gevallen zijn bedreiging, fysieke afpersing, ontvoering en gijzeling gemeld.⁶

De relevante beleidsvraag kan daarom niet worden gereduceerd tot de vraag of identificatie de traceerbaarheid van een gebruiker kan verbeteren. **De noodzakelijke vraag is of de aantoonbare veiligheidswinst van verplichte identificatie opweegt tegen het additionele fraude-, privacy- en cyberrisico van de daarvoor gecreëerde gegevensinfrastructuur.**

Wij menen dat het wetsvoorstel die afweging op dit moment onvoldoende mogelijk maakt.

2. De wezenlijke omvang van de gegevensverwerking wordt niet in de formele wet bepaald

Het voorstel bevat meerdere delegatiegrondslagen waarmee later vergaande verplichtingen kunnen worden ingevoerd.

Artikel 4.8b, tweede en derde lid, maakt het mogelijk bij ministeriële regeling gevallen aan te wijzen waarin een aanbieder gegevens over de **beoogde nummergebruiker** of over het gebruik van het nummer moet registreren. Welke gevallen dat zijn en welke gegevens daarbij moeten worden vastgelegd, wordt niet in de wet zelf bepaald. De registratie moet bovendien plaatsvinden voordat het nummer in gebruik wordt gegeven.⁷

Artikel 11.10a, tweede lid, maakt het daarnaast mogelijk bij of krachtens algemene maatregel van bestuur regels te stellen over onder meer de **authenticatie van de nummergebruiker of nummercegebruiker**, validatie van gegevens en blokkering van oproepen of berichten.

Artikel 4.8a voorziet bovendien in gegevensverstrekking aan de ACM en maakt het mogelijk te bepalen dat gegevens op verzoek worden verstrekt aan **bij lagere regelgeving aan te wijzen partijen**, waarbij ook de voorwaarden waaronder dat gebeurt later worden vastgesteld. De wettekst spreekt van gegevens over de identiteit van de aanbieder en over het gebruik van het nummer; volgens de memorie van toelichting kan het daarbij ook gaan om gegevens over het gebruik van het nummer door de nummergebruiker.⁸

Daarmee worden geen louter technische details gedelegeerd. Het gaat potentieel om de doelgroep van registratie, de gegevenscategorieën, wijze van authenticatie, ontvangers en verstrektingsvoorwaarden.

Dat staat op gespannen voet met het primaat van de wetgever zoals neergelegd in Aanwijzing 2.19 van de Aanwijzingen voor de regelgeving. De formele wet behoort ten minste de hoofdelementen te bevatten, waaronder de reikwijdte en structurele elementen van de regeling. Aanwijzing 2.23 verlangt bovendien dat een delegatiebevoegdheid zo concreet en nauwkeurig mogelijk wordt begrensd naar omstandigheden, onderwerpen en doeleinden.⁹

Het Adviescollege toetsing regeldruk heeft bij de consultatieversie van 2022 al geconstateerd dat een deel van de verplichtingen pas in lagere regelgeving wordt geconcretiseerd en dat de gevolgen, onder meer voor gebruikers van anonieme prepaidkaarten, daardoor nog niet volledig in beeld waren. Het eindoordeel luidde 'niet indienen, tenzij'.¹⁰

⁶ Zie deze rapportage uit januari 2026: <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/violation-de-donnees-secteur-crypto-actifs-202601>.

⁷ Terzijde: art. 4.8b, derde lid, verwijst naar 'het eerste lid, onderdeel b', terwijl het eerste lid geen onderdelen kent; kennelijk is het tweede lid, onderdeel b, bedoeld. Ook de regeldrukparagraaf van de MvT (par. 9) verwijst voor art. 4.8b naar leden die niet overeenkomen met de wettekst. Dat onderstreept dat juist deze bepaling nog onvoldoende is uitgewerkt.

⁸ MvT, par. 7 ('Algemene transparantie-aspecten'). De toelichting noemt als voorwaarden voor toegang door derden onder meer een kostengeoriënteerd tarief en het voorkomen van misbruik of gebruik voor commerciële doeleinden; die voorwaarden zijn niet in art. 4.8a zelf opgenomen.

⁹ Aanwijzingen voor de regelgeving, aanwijzing 2.19 (primaat van de wetgever) en aanwijzing 2.23 (begrenzing delegatie): <https://www.kcbr.nl/trefwoorden/delegatie>.

¹⁰ ATR, advies 'Wijziging van de Telecommunicatiewet i.v.m. nummerbeleid', 7 september 2022, kenmerk ATR2329/2022-U099, par. 4 en dictum: <https://www.adviescollegeregeldruk.nl/site/binaries/site-content/collections/documents/2022/09/07/atr->

Dat de gevolgen voor burgers onvoldoende zijn doordacht, blijkt ook uit de consultatiestukken zelf. De effectentoets stelt dat voor burgers geen of te verwaarlozen regeldrukeffecten optreden, beperkt tot een kleine specifieke groep. Een registratieplicht voor prepaidgebruikers zou echter een grote groep burgers raken. Het beleidskompas noemt prepaidregistratie niet in de probleemanalyse en bevat geen afweging van de gevolgen voor privacy en grondrechten.¹¹

Dit soort wezenlijke keuzes moeten vooraf gemaakt worden, op grond van een gedegen impactanalyse. Het huidig voorliggend materiaal is daarin ontoereikend en de volledige delegatie is ongewenst. We zagen die overmatige delegatie ook al bij het voorstel voor de Wet chartaal betalingsverkeer¹² en zien dat als een zeer zorgelijke ontwikkeling. Het veronderstelt namelijk een overheid die nooit die bevoegdheden zal gaan misbruiken.

3. De open reikwijdte verhindert een volwaardige toets op doelbinding, noodzakelijkheid en dataminimalisatie

Het delegatieprobleem heeft onmiddellijk een tweede gevolg. Zolang niet voldoende duidelijk is **wie** moet worden geïdentificeerd, **welke persoonsgegevens** worden verzameld, **welk concreet doel** iedere gegevenscategorie dient, **hoe lang** de gegevens worden bewaard, **wie** toegang krijgt en **aan welke derden** ze kunnen worden verstrekt, kan vooraf niet behoorlijk worden beoordeeld of de verwerking noodzakelijk en evenredig is.

De AVG verlangt dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en dat de gegevensverwerking tot het noodzakelijke wordt beperkt.¹³ Een wettelijke grondslag in lidstatelijk recht moet ook zelf het doel van de verwerking vastleggen.¹⁴ Gegevensbescherming door ontwerp vereist bovendien dat dataminimalisatie reeds bij het bepalen van de verwerking en de middelen wordt ingebouwd.¹⁵ Wij vragen ons in dit verband af of de Autoriteit Persoonsgegevens over het voorstel is geraadpleegd en of een gegevensbeschermingseffectbeoordeling is uitgevoerd.¹⁶

Het begeleidende consultatiedocument erkent zelf de gevoeligheid van deze afweging. Daarin wordt gesproken over een grondslag voor analyse van verkeersgegevens en het delen daarvan met bijvoorbeeld banken¹⁷ (bij de consultatie van 2022 ging het nog om monitoring van metadata én van de inhoud van berichtenverkeer)¹⁸ en over een mogelijke verplichte registratie van prepaid-simgebruikers. Ten aanzien van die prepaidregistratie wordt tegelijkertijd aangegeven dat de effectiviteit en proportionaliteit nog nader worden onderzocht.

Daarmee ontstaat een onwenselijke volgorde: eerst wordt een ruime wettelijke infrastructuur gecreëerd waarmee toekomstige gegevensverwerking mogelijk wordt gemaakt, terwijl essentiële onderdelen van de noodzakelijkheids- en proportionaliteitstoets pas bij de latere invulling daarvan kunnen worden uitgevoerd.

Naar onze mening moet die volgorde worden omgekeerd. **Eerst behoort concreet te worden vastgesteld welk probleem met welke gegevensverwerking wordt opgelost en waarom die verwerking nodig is. Pas daarna kan de wetgever een voldoende nauwkeurig begrensde wettelijke bevoegdheid creëren.**

[advies-wijziging-van-de-telecommunicatiewet-i.v.m.-nummerbeleid/U099-Ministerie-EZK-Telecommunicatiewet-nummerbeleid-w.g.pdf](#). De huidige MvT vermeldt onder 'Advies en consultatie' (par. 11) nog 'PM'.

¹¹ Effectentoets (doelgroepen) en Beantwoording vragen beleidskompas, vragen 3 en 7, beide gepubliceerd bij de consultatie.

¹² Internetconsultatie 'Wet chartaal betalingsverkeer' (Ministerie van Financiën, 2024): <https://internetconsultatie.nl/chartaal/document/12193>.

¹³ Art. 5, eerste lid, onder b en c, AVG (Verordening (EU) 2016/679): <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

¹⁴ Art. 6, derde lid, AVG.

¹⁵ Art. 25 AVG (gegevensbescherming door ontwerp en door standaardinstellingen).

¹⁶ Art. 36, vierde lid, AVG (raadpleging van de toezichthoudende autoriteit bij de voorbereiding van wetgeving) en art. 35 AVG (gegevensbeschermingseffectbeoordeling).

¹⁷ Begeleidend document bij de huidige consultatie, onderdelen 'Overige onderdelen' en 'Context'.

¹⁸ Aldus het begeleidende document bij de consultatie van 2022, zoals weergegeven door Security.NL, 12 juli 2022: <https://www.security.nl/posting/760520/Kabinet+kijkt+naar+monitoren+inhoud+sms%27jes+en+verbod+op+anonieme+simkaarten>; consultatiepagina 2022: <https://www.internetconsultatie.nl/nummerbeleid/b1>.

4. Identificatie mag niet als panacee voor fraudebestrijding worden behandeld

Het begeleidende document stelt dat anonieme simkaarten online fraude kunnen vergemakkelijken en kondigt nader onderzoek aan naar verplichte registratie; in 2022 werd nog betoogd dat zo'n registratie aan de bestrijding daarvan kan bijdragen.¹⁹ Dat is op zichzelf een begrijpelijke hypothese. De Nederlandse overheid heeft dezelfde vraag echter eerder onderzocht en kwam toen tot een wezenlijk genuanceerdere conclusie, zoals het begeleidende document zelf ook erkent.

De minister van Justitie en Veiligheid berichtte de Tweede Kamer in 2019²⁰ dat uit een eerdere verkenning (2017)²¹ geen significant profijt voor opsporingsdiensten bij de opsporing van criminelen en terroristen werd verwacht van verplichte registratie van prepaid-simkaarten. Volgens de minister werd die conclusie onderschreven door het Openbaar Ministerie, de politie, de inlichtingen- en veiligheidsdiensten en het Ministerie van Economische Zaken. Daarbij werd expliciet gewezen op omzeiling door valse identiteiten en katvangers en op het bestaan van alternatieve communicatiemiddelen.

Het Adviescollege toetsing regeldruk heeft bij een eerdere versie van het wetsvoorstel eveneens gewezen op deze eerdere bevindingen en opgemerkt dat onduidelijk is op welke gronden nu een andere afweging wordt gemaakt.²²

Daar komt inmiddels een tweede effect bij dat in de eerdere discussie minder prominent was: grootschalige identiteitsregistratie heeft zelf een veiligheidsprijs.

De Revolut-casus van september 2026 is daarvan een treffend voorbeeld. Daar hoefde volgens de beschikbare informatie geen centrale database te worden gekraakt. De aanwezigheid van geverifieerde persoonsgegevens en een procedure waarmee die gegevens legitiem aan bevoegde instanties konden worden verstrekt, bood zelf een aanvalsvector toen aanvallers zich via een legitiem e-maildomein van een overheidsinstantie als die instantie voordeden en die procedure succesvol nabootsten.²³

Dit is rechtstreeks relevant voor een systeem waarin telecomaanbieders betrouwbare identiteit-nummerkoppelingen moeten opslaan en waarin vervolgens wettelijke routes voor gegevensverstrekking aan ACM en andere partijen worden gecreëerd.

De relevante vraag

De onbeantwoorde vraag, die wél beantwoord moet worden, luidt:

welke aantoonbare fraude wordt door verplichte identificatie voorkomen, welke kwaadwillenden kunnen deze verplichting eenvoudig omzeilen, welke aanvullende persoonsgegevens moeten daarvoor van de gehele bonafide populatie worden verzameld en welk nieuw cyber- en frauderisico ontstaat daardoor?

Zonder die analyse kan identificatie gemakkelijk een disproportioneel instrument worden: de gebruiker die zich aan de regels houdt wordt duurzaam identificeerbaar, terwijl de professionele fraudeur gebruik kan maken van gestolen identiteiten, katvangers, buitenlandse middelen of andere communicatietechnieken.

¹⁹ Begeleidend document, onderdeel 'Overige onderdelen': de maatregel werd in het verleden niet opportuun geacht omdat de effectiviteit te laag werd geacht. Dat het begeleidende document bij de consultatie van 2022 nog betoogde dat verplichte registratie aan fraudebestrijding kan bijdragen, blijkt uit het ATR-advies van 7 september 2022, p. 4.

²⁰ Kamerstukken II 2018/19, 29 279, nr. 534 (brief van de minister van Justitie en Veiligheid van 19 augustus 2019): https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2019Z15814&did=2019D32750.

²¹ Kamerstukken II 2016/17, 29 754, nr. 419, met bijlage (verkenning naar een verplichte registratie van prepaid-simkaarthouders, april 2017).

²² ATR, advies van 7 september 2022 (zie hiervoor), p. 4–5, met adviespunt 3.1.

²³ Revolut bevestigde op 12 september 2026 dat een onbevoegde derde, via e-mail vanaf een legitiem domein van een overheidsinstantie, klantgegevens had opgevraagd en verkregen, waaronder kopieën van identiteitsbewijzen en mogelijk verificatieselfies. Zie TechCrunch, 12 september 2026: <https://techcrunch.com/2026/09/12/revolut-confirms-customer-data-breach-through-fake-government-requests/>; Malwarebytes: <https://www.malwarebytes.com/blog/news/2026/09/revolut-gave-customer-ids-and-financial-data-to-a-government-impostor>.

Daarbij is om reden van toegankelijkheid van universele diensten en toegang tot communicatiemiddelen om het recht op vrije meningsuiting uit te oefenen grondrechtelijk gewenst dat er een mogelijkheid tot anoniem prepaid gebruik en communicatie behouden blijft. Een de-minimisdrempel van €250 zonder identificatieplicht verdient serieuze overweging als minder ingrijpend alternatief.²⁴ Hierbij kan gedacht worden aan een anonieme laag-risicocategorie, bijvoorbeeld met een maximaal tegoed en/of cumulatieve opwaardering van €250 per prepaidnummer binnen een nader vast te stellen periode.

Boven een dergelijke objectieve grens kan, alleen indien de noodzaak daarvan voldoende is aangetoond, een identificatieplicht gelden. Maar wanneer de regering identificatie ook beneden een dergelijke de-minimisdrempel noodzakelijk acht, behoort zij concreet aan te tonen welke aanvullende fraude daarmee wordt voorkomen, waarom minder ingrijpende maatregelen onvoldoende zijn en waarom die veiligheidswinst opweegt tegen de extra gegevens- en cyberrisico's.

5. Wettelijke waarborgen moeten integraal onderdeel zijn van het stelsel

Wanneer ondanks deze bezwaren een uitgebreider identificatie- en registratiestelsel wordt ingevoerd, behoren de beschermende waarborgen tegelijkertijd en op hetzelfde wettelijke niveau te worden vastgelegd.

Het voorgestelde artikel 4.9, vijfde lid, bevat al een beperkte waarborg voor het openbare nummerregister. Indien de nummerhouder een natuurlijke persoon is en het nummer niet uitsluitend bedrijfsmatig gebruikt, kunnen naam, adres en woonplaats op verzoek buiten het openbare gedeelte van het register worden gehouden.

Afscherming van uitsluitend het openbare register is echter niet voldoende wanneer dezelfde of vergelijkbare persoonsgegevens via andere registratie- en verstrekkingroutes alsnog beschikbaar kunnen zijn. Bovendien zijn gebruikers van prepaidkaarten doorgaans geen nummerhouder: hun gegevens komen niet in het nummerregister terecht maar in de registraties van aanbieders, zodat deze waarborg hen niet bereikt.

Iedere betrokkene moet daarom eenvoudig en kosteloos kunnen nagaan welke persoonsgegevens in het stelsel over hem of haar worden verwerkt, uit welke bron deze afkomstig zijn, voor welk doel ze worden gebruikt en aan welke partijen ze zijn verstrekt. Onjuiste gegevens moeten effectief en onverwijld kunnen worden gerectificeerd. De AVG kent reeds rechten op inzage en rectificatie en verlangt in beginsel dat eerdere ontvangers van een rectificatie, wissing of beperking op de hoogte worden gesteld.²⁵

Voor het onderhavige stelsel dienen deze rechten praktisch uitvoerbaar te worden gemaakt over de gehele keten van nummerhouder, aanbieder, eventuele nummergemachtigde, ACM en andere ontvangers.

Ook afscherming moet ketenbreed worden geregeld. Wanneer een natuurlijke persoon om afscherming verzoekt, behoort dat verzoek niet alleen het openbare register te raken, maar iedere openbaarmaking en iedere niet strikt noodzakelijke derdenverstrekking. Verstrekking zonder toestemming moet beperkt blijven tot een in de wet zelf omschreven kring van bevoegde partijen, voor concreet omschreven wettelijke doeleinden en alleen als die verstrekking noodzakelijk is.

Daarnaast dient de wet ieder commercieel of daarmee vergelijkbaar secundair gebruik (marketing, profilering, gegevensverrijking, kredietbeoordeling etc.) uitdrukkelijk uit te sluiten. De memorie van toelichting noemt het voorkomen van commercieel gebruik wel als voorwaarde voor toegang tot gegevens op grond van artikel 4.8a, maar de wettekst zelf bevat die waarborg niet.²⁶ Bulktoegang en bulkverstrekking behoren evenmin mogelijk te zijn zonder een gemotiveerde wettelijke grondslag.

²⁴ Vergelijk ATR, advies van 7 september 2022, adviespunt 2.1: als minder belastend alternatief adviseerde het college om kortdurend buitenlands gebruik van anonieme prepaidkaarten toe te staan.

²⁵ Art. 15 (inzage), 16 (rectificatie) en 19 (kennisgeving aan ontvangers) AVG.

²⁶ MvT, par. 7.

De raadplegingen en verstrekkingen behoren te worden gelogd, zodat controleerbaar is wie gegevens heeft ingezien, wanneer dat gebeurde, op welke grondslag en aan wie ze vervolgens zijn verstrekt. Ook moeten bewaartermijnen vooraf worden begrensd en moeten gegevens worden verwijderd zodra zij niet langer noodzakelijk zijn.

Deze waarborgen zijn geen uitvoeringsdetails. Zij bepalen de werkelijke omvang van de inmenging in de persoonlijke levenssfeer en behoren daarom onderdeel te zijn van de wettelijke architectuur zelf. Het is zorgelijk dat hieraan in essentie wordt voorbijgegaan.

6. Conclusie

De doelstelling van het voorstel — betere bescherming tegen spoofing, phishing en online fraude — is loffelijk. Maar die doelstelling vraagt wel om terughoudendheid met het creëren van nieuwe, omvangrijke en langdurige verzamelingen van identiteitsgegevens.

De recente Revolut-inbreuk laat zien waarom. Een maatregel die bedoeld is om fraude beter herleidbaar te maken kan tegelijkertijd een dataset creëren die fraudeurs juist in staat stelt hun slachtoffers nauwkeuriger te identificeren en nog overtuigender en indringender te benaderen.

Het voorstel toont naar onze mening nog niet aan dat de veiligheidswinst van een generieke identificatie- en registratieplicht groter is dan dit nieuw gecreëerde risico. Dat is des te problematischer omdat eerdere Nederlandse onderzoeken juist twijfels hebben opgeleverd over de effectiviteit van verplichte prepaidregistratie en omdat professionele kwaadwillenden identificatievereisten kunnen omzeilen.

Wij adviseren daarom de wetgever:

- de identificatieplicht niet als plicht op te nemen gezien de grondrechtelijke bescherming van de vrijheid van meningsuiting, de persoonlijke levenssfeer en het telecommunicatiegeheim (art. 7, 10 en 13 Grondwet; art. 8 en 10 EVRM),
- tenminste, een anonieme drempel van €250 vast te leggen waaronder dit niet geschiedt,
- voor zover er boven dat bedrag wél geïdentificeerd zou worden, de essentiële elementen van iedere identificatie-, registratie- en verstrekkingplicht in de formele wet zelf vast te leggen,
- vooraf per verwerking de noodzaak, doelbinding, proportionaliteit en dataminimalisatie aantoonbaar te maken,
- wettelijke garanties op te nemen voor inzage en rectificatie door burgers,
- wettelijke waarborgen te formuleren voor ketenbrede afscherming, gesloten en doelgebonden derdenverstrekking, logging, begrensde bewaartermijnen en een absoluut verbod op commercieel hergebruik van verplicht verzamelde identiteitsgegevens,
- het voorstel voor advies voor te leggen aan de Autoriteit Persoonsgegevens en de gegevensbeschermingseffectbeoordeling openbaar te maken.

Dezelfde wet die de mogelijkheid creëert om identiteit, telefoonnummer en gebruik aan elkaar te koppelen, behoort immers duidelijk, gemotiveerd en gewogen vooraf vast te leggen waar de grens van die gegevensmacht ligt.

Met vriendelijke groet,

Ir. S. Lelieveldt CCP

Voorzitter HRIF.EU – digitaal ingezonden

Bijlage 1: Achtergrond en oprichting HRIF.EU

De oprichters van HRIF.EU waren in de jaren 2020-2023 nauw betrokken bij diverse zaken in het financieel toezicht. Het gaat om ECLI:NL:RBROT:2021:2968²⁷ (leidend tot ingetrokken toezichtseis DNB) en om diverse zaken over toezichtkosten: ECLI:NL:RBROT:2023:9153, ECLI:NL:RBROT:2023:9157²⁸ (onder andere leidend tot vernietiging van NL-regels op grond van hoger recht).

HRIF.EU is in 2023 opgericht omdat de vanuit overmatige intrusieve regels voorgeschreven controles en regels in de financiële sector tot onnodige schending van de onschuldpresumptie leiden, discriminatie, schending van de privacy en beperking in de mogelijkheid om contant geld te gebruiken of rekeningen te krijgen in het betalingsverkeer. Drie jaar na onze oprichting blijkt die analyse ook gedeeld te worden door de Algemene Rekenkamer. De Rekenkamer concludeert in het rapport [Gevolgen groot, opbrengsten onbekend](#) (maart 2026)²⁹ dat van een effectieve en risicogebaseerde anti-witwasaanpak in de bankensector onvoldoende sprake is en dat onbekend is wat de aanpak oplevert. Naar ons oordeel ontbreekt daarmee een deugdelijke rechtvaardigingsgrond.

Het is spijtig dat de Nederlandse overheid, banken en betrokken stakeholders niét uit zichzelf de logische conclusie willen trekken dat sommige werkzaamheden moeten stoppen. Voor HRIF.EU is dat een treurige realiteit. Wel hebben wij, onder meer via een interventie richting de feitelijke hoster van het bancaire sleepnet (Amazon Cloud Hosting), [in 2024 bijgedragen aan het stilzetten van de naar ons oordeel zonder wettelijke grondslag uitgevoerde gezamenlijke monitoring van miljarden transacties door banken](#).³⁰

[HRIF.EU heeft als doel](#) om (lieftst vooraf: ex-ante) burgers in het financieel-economische domein tegen mensenrechtenschendingen (onder andere: inbreuk eigendom, privacy, onschuldpresumptie, discriminatie) te beschermen door achtereenvolgens met pen, publiciteit en eventueel procedure tot een verandering te komen. Wij pakken alleen zaken op die systemisch van aard zijn en vertegenwoordigen in procedures alleen personen van wie de casus representatief is voor het algemeen belang dat we vertegenwoordigen.

Typische dossiers waar we voor en achter de schermen actief in zijn, zijn de volgende:

- het onder Europees recht [onrechtmatig ingerichte stelsel van toezichtkosten DNB/AFM](#),
- het [recht op contant geld gebruik en het recht op bankrekening ondernemers](#),
- het onrechtmatige bancaire sleepnet en de overmatige monitoring rond ongebruikelijke in plaats van verdachte transacties, gevolgd door [onrechtmatige verwerking en datadeling door de Financial Intelligence Unit](#) (zonder passend recht op verwijdering onder internationaalrechtelijke verdragen),
- de [discriminatie die in financiële regelgeving besloten ligt](#), de onnodige exclusie die geschiedt van klanten/sectoren (sekswerkers, coffeeshops, intensieve cash-gebruikers),
- de [onvoldoende bescherming en invulling door AFM van haar rol als toezichthouder](#) op de Wet oneerlijke handelspraktijken, prospectusrichtlijn en financiële markten, tot bescherming van het recht op eigendom van klanten,
- de nationale Woo-uitzonderingsgronden die verder reiken dan Europees recht toestaan,
- het [ANBI-regime als overmatig nieuw toezichtsregime](#) en overmatige geografische belastingheffing aan niet-ANBI's in strijd met EU-rechtsprincipes,
- de oneigenlijke toepassing van sanctieregimes en de geopolitieke noodzaak om de oude FATF-structuur en concepten snel los te laten en EU-rechtelijke principes en grondrechten te laten prevaleren (niet toegeven aan VS-druk).

²⁷ <https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2021:2968>.

²⁸ <https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2023:9153> en <https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBROT:2023:9157>.

²⁹ Algemene Rekenkamer, 'Gevolgen groot, opbrengsten onbekend. Onderzoek naar de anti-witwasaanpak in de bankensector', 11 maart 2026: <https://www.rekenkamer.nl/documenten/2026/03/11/gevolgen-groot-opbrengsten-onbekend---onderzoek-naar-de-anti-witwasaanpak-in-de-bankensector>.

³⁰ Zie jaarverslag HRIF.EU 2024 - <https://hrif.eu/wp-content/uploads/2026/02/2025-HRIF2024-JV-vastV2.pdf>