Ref. Ares(2025)8724775 - 14/10/2025

aan	Europese Commissie
ons kenmerk	SPF20251014
datum	14 oktober 2025
onderwerp	Reactie Stichting Privacy First op de internetconsultatie inzake het digitale vereenvoudigingspakket

Geachte Commissie,

In het op https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Simplification-digital-package-and-omnibus_en gepubliceerde consultatieverzoek met betrekking tot de Digitale Omnibus verzoekt u om reacties inzake een grote diversiteit aan onderwerpen, die niet alleen gevolgen hebben voor bedrijven. Hoewel wij begrip hebben voor de behoefte van bedrijven aan vereenvoudiging, moet het niet zo zijn dat de grondrechten van Europese burgers en van kleine organisaties (midden- en kleinbedrijf en middelgrote en kleine non-profitorganisaties) worden aangetast.[1]

Achtergrond

Toename risico's voor consumenten en kleine organisaties

De digitalisering zorgt niet alleen voor 'gemak' en soms voor efficiency, maar ook voor een exponentiële toename van de risico's voor consumenten en kleine organisaties, onder meer door de toename van desinformatie, onjuiste risicoprofilering door witwasbestrijdingsplichtige grote ondernemingen, verspreiding van grote hoeveelheden persoonsgegevens via advertentiebedrijven (Google, Meta c.s.) en datahandelaren, het gebruik van AI door criminelen en de schade die optreedt als gevolg van het maken van deepfakes.

[1] In dit verband verwijst Privacy First allereerst naar de door ons mede-ondertekende brief van EDRi aan de Europese Commissie d.d. 19 mei 2025, https://edri.org/wp-content/uploads/2025/05/Final-EDRI-letter-against-GDPR-simplification.pdf .

Stichting Privacy First
Nieuwe Herengracht 49
1011 RN Amsterdam

https://privacyfirst.nl
info@privacyfirst.nl
+31 20 810 0279

KvK 34298157
ANBI erkend

Het wordt voor consumenten en kleine organisaties steeds moeilijker om deze risico's te begrijpen en te beperken.

Ontbrekende handhaving

Dat komt bij dat op dit moment het al een probleem is dat veel regels die voor burgers relevant zijn, niet worden gehandhaafd, onder meer door capaciteitsgebrek en gebrek aan middelen van de toezichthouders.

Dit wordt onder andere geconstateerd in het recent gepubliceerde rapport van Interface over bescherming van kinderen[2], waarin de auteurs opmerken:

> *Over the past fifteen years, though, the EU has adopted an increasingly dense set of measures and instruments to protect minors online. The General Data Protection Regulation (GDPR), the Audiovisual Media Services Directive (AVMSD), the Digital Services Act (DSA), and the Artificial Intelligence Act (AI Act) all contain provisions that specifically address children's vulnerabilities. Complementary non-binding instruments—such as the Better Internet for Kids+ (BIK+) Strategy—reinforce the EU's commitment to providing a safe and empowering digital environment for minors. At the Member State level, governments have introduced their own rules and enforcement models, notably France with its Loi SREN and Germany with its long-standing Jugendmedienschutz-Staatsvertrag.*
>
> *However, despite these initiatives, minors remain insufficiently protected. The gap between what the existing framework requires and what happens in practice is striking. This paper's central argument is that the key problem today is not a lack of legislation or awareness but a failure of implementation and enforcement.*

Het voorgaande betreft de bescherming van kinderen in het digitale domein. Het ontbreken

[2] *Mind the Gap | Age Assurance and the Limits of Enforcement under EU Law*, https://www.interface-eu.org/publications/age-assurance-gap.

van handhaving is aan de orde op een groot aantal andere terreinen, zoals door diverse organisaties (onder meer Noyb[3]) wordt geconstateerd.

Daar komt nog bij dat tegen partijen van buiten de EU niet kan worden opgetreden, aldus de EDPB in een rapport uit 2024.[4]

Gegevensdeling, volgtechnologieën en de AI-verordening

Aanbevelingen Privacy First

In dit onderdeel gaan wij in op de volgende onderwerpen: het *acquis* met betrekking tot gegevens, volgtechnologieën en de AI-verordening.

Vanwege de groeiende risico's waarmee consumenten en kleine organisaties worden geconfronteerd adviseert Privacy First het volgende:

1. Neem met spoed maatregelen waarmee het toezicht en de handhaving van de Europese regels in het digitale domein worden versterkt, bijvoorbeeld door de EU-lidstaten te verplichten tot vergroting van het budget van de nationale toezichthouders. Daarbij kan er aan gedacht worden om in riskante sectoren zoals die van de advertentiebedrijven en de datahandelaren het toezicht door de bedrijven te laten financieren (op dezelfde wijze als in heel de EU al in het financiële toezicht gebeurt).

2. Draag er zorg voor dat bedrijven van buiten de EU de Europese digitale regels naleven, zodat er in de EU een gelijk speelveld (*level playing field*) ontstaat voor ondernemingen uit de EU. In dat verband kan worden gedacht aan het vragen van een forse bankgarantie aan partijen van buiten de EU die persoonsgegevens van Europese burgers willen verwerken of aan andere nieuwe maatregelen.

3. Vereenvoudig de regels op het gebied van volgtechnologieën (cookies, IP-adres herkenning en apparaatherkenning en dergelijke) op een zodanige manier dat burgers

[3] Zie bijvoorbeeld *EU pledged to improve GDPR cooperation - and made it worse*, https://noyb.eu/en/eu-pledged-improve-gdpr-cooperation-and-made-it-worse.

[4] Aankondiging EDPB: https://www.edpb.europa.eu/our-work-tools/our-documents/other/report-extraterritorial-enforcement-gdpr_en; rapport EDPB https://www.edpb.europa.eu/system/files/2024-10/edpb_20240417_report_extraterritorial_enforcement_gdpr_en.pdf.

beter worden beschermd. In onze optiek vloeit reeds uit de huidige regels voort dat het ongewenst is dat de overheid gebruikmaakt van de diensten van advertentiebedrijven zoals Meta (Facebook, Instagram en dergelijke) en Google, dan wel via overheidswebsites en andere uitingen naar deze advertentiebedrijven verwijst. Overheden horen geen gebruik te maken van volgtechnologieën. Een goede vereenvoudiging is verder dat het verboden is voor aanbieders van essentiële diensten, zoals banken, energiebedrijven en telecombedrijven, om van volgtechnologieën gebruik te maken. Deze essentiële diensten heeft iedereen nodig, zodat het van belang is dat consumenten en kleine organisaties optimaal worden beschermd. Er ontstaat door vereenvoudiging op deze wijze ook een gelijk speelveld voor Europese bedrijven.

4. Maak alle bedrijven die op grote schaal persoonsgegevens en gegevens van kleine organisaties verwerken (zoals kredietwaardigheidsbeoordelaars, advertentiebedrijven en andere datahandelaren) vergunningplichtig, met eisen aan de integriteit van het personeel van voormelde ondernemingen en controle op de genomen maatregelen ter naleving van gegevensbeschermingsregels en andere digitale regels.

5. Vereenvoudig de regels op het gebied van gegevensuitwisseling[5] op een zodanige wijze dat daarmee de risico's voor consumenten en kleine organisaties worden beperkt en het toezicht en de handhaving (zie boven onder 1) op orde zijn. Juist gegevensuitwisseling vormt een enorm risico voor betrokkenen, als dit op een onzorgvuldige en onveilige wijze gebeurt.

6. Werk met spoed de nadere regels inzake de AI-verordening (AI Act) uit en maak zo spoedig mogelijk een diepgaande analyse van de terreinen waarop AI de grootste risico's voor burgers en kleine organisaties oplevert. Wij denken dat één van de risicoterreinen de bestrijding van witwassen en terrorismefinanciering (AML/CFT) door grote ondernemingen (onder andere financiële instellingen en accountantskantoren) is. Nu al is de maatschappelijke schade die AML/CFT veroorzaakt aanzienlijk, voor de Nederlandse situatie verwijzen wij daartoe naar onze deelname aan een Nederlandse

[5] Onder de in de consultatieuitnodiging genoemde Europese regels, te weten de datagovernanceverordening, verordening inzake een kader voor het vrije verkeer van niet-persoonsgebonden gegevens en de richtlijn open data.

consultatie over de implementatie van de nieuwe antiwitwasverordening[6], meer in het bijzonder naar bijlage 1, '*De schaduwkant van de privatisering van de misdaadbestrijding*'.

Op identificatie en vertrouwensdiensten gaan we afzonderlijk in.

Identificatie en vertrouwensdiensten

Aanbevelingen Privacy First

Identificatie (of verificatie van de identiteit) is één van de riskantste activiteiten die er zijn voor consumenten en kleine organisaties.

Aan dat onderwerp hebben wij meerdere malen aandacht besteed, onder meer door middel van een verzoek dat wij in september 2024 hebben gedaan aan de Nederlandse minister van Financiën en De Nederlandsche Bank om de identificatiepraktijken van financiële instellingen te verbeteren.[7] In ons verzoek hebben wij toegelicht waarom de huidige identificatieaanpak van financiële instellingen risicovol is voor burgers en verandering behoeft. In juni 2025 nam Privacy First deel aan een consultatie van de Europese Banken Autoriteit (EBA)[8] en besteedde in het consultatiecommentaar aandacht aan het voorstel van de EBA om het Europese digitale identificatiemiddel (ook wel EDI-wallet of EUDI-wallet genoemd) verplicht te stellen in de AML/CFT.[9]

---

[6] Artikel: https://privacyfirst.nl/artikelen/permanente-surveillance-dreigt-onder-nieuwe-anti-witwasregels/, consultatiereactie: https://privacyfirst.nl/wp-content/uploads/consultatie_Iwt_PrivacyFirst_29aug2025.pdf.

[7] Artikel: https://privacyfirst.nl/artikelen/privacy-first-verzoekt-aanpassing-identificatiepraktijken-van-financiele-instellingen/, document: https://privacyfirst.nl/wp-content/uploads/Wwft_identificatie_verzoek_PrivacyFirst_sept2024.pdf.

[8] Artikel: https://privacyfirst.nl/artikelen/implementatieregels-dienen-de-nadelen-van-antiwitwasregels-te-beperken/; consultatiecommentaar: https://privacyfirst.nl/wp-content/uploads/Privacy-First-response-EBA-consultation-on-additional-AMLR-rules-June-2025.pdf.

[9] Lees het artikel *Digitale identiteit wordt sluipenderwijs toch verplicht*, https://privacyfirst.nl/artikelen/digitale-identiteit-wordt-sluipenderwijs-toch-verplicht/.

Het is essentieel dat burgers en kleine organisaties alleen tot identificatie verplicht zijn als daar zeer goede redenen voor zijn, het met passende waarborgen is omgeven en er rekening wordt gehouden met de grote groep EU-burgers die onvoldoende digitale vaardigheden heeft.

In Nederland is de Autoriteit Financiële Markten toezichthouder voor de Europese Toegankelijkheidsrichtlijn (European Accessibility Act, EAA)[10] en heeft in dat kader bekendgemaakt dat er in Nederland ongeveer 5,5 miljoen mensen zijn die onvoldoende vaardig zijn om met digitale omgevingen om te gaan.[11] Dat is een grote groep, die in andere EU-landen verhoudingsgewijs niet kleiner zal zijn.

In aansluiting op de aanbevelingen die wij al gedaan hebben aan het Nederlandse ministerie van Financiën in september 2024 en aan de EBA in juni 2025, doen wij de volgende aanbevelingen die tevens vereenvoudigingen inhouden:

1. Schrijf identificatie alleen voor als de noodzaak kan worden onderbouwd.
2. Verbied organisaties om van hun wederpartijen (klanten, burgers) te verlangen dat zij gebruikmaken van het Europese digitale identificatiemiddel op straffe van het niet krijgen van een product of dienst.[12]

---

[10] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=celex:32019L0882

[11] Zie https://www.afm.nl/nl-nl/sector/themas/dienstverlening-aan-consumenten/toegankelijkheid en https://www.afm.nl/nl-nl/sector/actueel/2025/apr/sb-eaa-update%201.

[12] Zie ook onze consultatiereactie aan de EBA, p. 12: *"Article 6 is not in line with the explicit principle laid down in Regulation (EU) No 910/2014 (the eIDAS Regulation) that the use of eIDAS compliant solutions shall be voluntary and that access to public and private services, and freedom to conduct business shall not in any way be restricted or made disadvantageous to natural or legal persons that do not use these solutions.*

The non-mandatory character of eIDAS compliant solutions means that it is always the voluntary choice of the relevant natural or legal person to (not) use the digital identity. The decision whether to use or not use the electronic identity is free and can consequently not be made mandatory by imposing an obligation on public or private service providers to require electronic identification as a standard in non-face-to-face contexts. Imposing such an obligation would effectively render the use of electronic identification mandatory and make this principle of the eIDAS regulation illusory."

3. Verplicht degenen die gebruikmaken van het Europese digitale identificatiemiddel om aan te tonen dat het gebruik van het middel vrijwillig is en dat de betrokkene de risico's verbonden aan elektronische identificatie begrijpt.[13]

4. Zorg ervoor dat het Europese digitale identificatiemiddel ook kan worden gebruikt zonder dat betrokkene een apparaat (bijvoorbeeld smartphone of tablet) heeft met een besturingssysteem van een bedrijf van buiten de EU. Dit is van belang ter voorkoming van digitale afhankelijkheid van bedrijven en systemen van buiten de EU en biedt nieuwe kansen voor Europese bedrijven.

5. Schrijf in situaties waar identificatie wenselijk is voor dat degene die moet identificeren daar altijd een fysiek alternatief voor biedt.

6. Verbied het gebruik van biometrie als identificatiemiddel of als onderdeel van het identificatieproces. Verbied het maken van foto's en video's van mensen ter identificatie.[14] In zeer bijzondere situaties kan daar met wettelijke grondslag van worden afgeweken, maar mogen de biometrische gegevens slechts kort worden bewaard.[15]

---

[13] In onze EBA consultatiereactie schreven wij op p. 15: *"In Article 31(1) it should be made clear that the use of electronic identification means is voluntary and that it is the responsibility of the obliged entity to verify if the customer and the natural person understand the risks of this means of verification."*

[14] Biometrie is riskant, onder meer omdat de kwaliteit van de biometrische authenticatie wisselend is en omdat vervanging van een uitgelekte pincode of wachtwoord mogelijk is, wat niet geldt voor een biometrisch authenticatiemiddel zoals de vingerafdruk of het gezicht. Biometrische gegevens kunnen eenvoudig door kwaadwillenden geoogst worden voor malafide gebruik, want biometrische gegevens zijn niet geheim. Zie daarover onder meer het rapport van het Maatschappelijk Overleg Betalingsverkeer van mei 2017, https://www.dnb.nl/media/h2dpz3ia/biometrie-in-betalingsverkeer-mob-eindrapport.pdf en het document van EDPS uit 2020, https://www.edps.europa.eu/sites/edp/files/publication/joint_paper_14_misunderstandings_with_regard_to_identification_and_auuthentication_en.pdf.

[15] In onze consultatiereactie aan de EBA, p. 12, schreven wij: *"Privacy First proposes that the EBA creates a new draft of Article 6 expressing:*

7. Verbied het maken van kopieën van identiteitsbewijzen, het gebruik daarvan en het verzenden van kopieën per post of e-mail. Dit is een gevaarlijke praktijk die op dit moment een grote omvang heeft en in strijd is met de AVG als geen origineel identiteitsbewijs is ingezien.

8. Verbied dat persoonsgegevens ten behoeve van identificatie langer worden bewaard dan twaalf maanden na het identificatiemoment. Daarna mogen alleen nog basisgegevens worden bewaard.

9. Zorg voor een simpel en herkenbaar systeem aan de hand waarvan burgers en kleine organisaties kunnen vaststellen dat zij met een legitieme identificatiepartij (vertrouwensdienst)[16] van doen hebben, of en wanneer en door wie deze partij op integriteit en op afdoende gegevensbeschermingsmaatregelen is getoetst.

10. Als een fysieke identificatiedienstverlener wordt ingeschakeld (zoals bijvoorbeeld in Nederland AMP) en de identificatie met technische middelen (bijvoorbeeld een apparaat of een app op een smartphone) plaatsvindt, wordt de burger in de gelegenheid gesteld te verifiëren of dat middel aan alle gegevensbeschermingseisen voldoet. De medewerker van de identificatiedienstverlener dient zichzelf te kunnen identificeren en de burger dient zekerheid te kunnen verkrijgen over het gebruikte apparaat en over de wijze van gegevensuitwisseling met de opdrachtgever.

11. In het ecosysteem van het Europese digitale identificatiemiddel zijn een groot aantal rollen ('EUDI-rollen') gedefinieerd, sommige rollen worden vervuld door overheden. In het schema op github[17] zijn tien EUDI-rollen te zien. Met de private partijen die een EUDI-rol

---

• the use of an eIDAS solution and remote solutions shall only take place on a completely voluntary basis and if such a solution is used, it is the responsibility of the obliged entity to verify that the person that is going to use this solution understands the risks of the digital mode of operation;

• a physical alternative shall always be offered at a trusted party, with the customer being enabled to verify the reliability of that party and the reliability of the equipment used."

[16] Met de benodigde vergunningen en dergelijke.

[17] Zie https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/2.0.0/architecture-and-reference-framework-main/, paragraaf 3.1, figure 1: *Overview of the EUDI Wallet ecosystem roles.*

spelen, kan een burger of kleine organisatie te maken krijgen. Voor zover wij hebben kunnen zien, worden aan de private partijen die een EUDI-rol hebben alleen technische eisen gesteld, maar vindt geen integriteitstoetsing plaats. Evenmin wordt getoetst of de private partijen commerciële conflicterende belangen hebben, wat betekent dat Microsoft, Google, Oracle, Meta en andere grote IT-partijen een EUDI-rol kunnen gaan spelen en de afhankelijkheid van burgers en kleine organisaties van het grootbedrijf kunnen vergroten. Dat is in strijd met de Europe First-intenties van de EU. Over de EUDI-rollen hebben wij op de algemene informatiesite van de Commissie geen informatie aangetroffen, terwijl dit te zijner tijd wel voor burgers en kleine organisaties van belang is voor hun keuze van een onderneming die het gebruik van het Europese digitale identificatiemiddel faciliteert. Onze aanbevelingen zijn daarom als volgt:

- Zorg voor een Europees digitaal identificatiemiddel dat digitaal veilig is.[18]
- Stel integriteitseisen aan private partijen die een EUDI-rol hebben en zorg ervoor dat internationale grootbedrijven met conflicterende commerciële belangen, zoals advertentiebedrijven, buiten de deur worden gehouden.
- Zorg voor adequate informatie over de private partijen met EUDI-rollen (inclusief informatie over periodieke audits en beoordelingen) die goed toegankelijk is, zodat burgers en kleine organisaties in staat worden gesteld om te kiezen voor de aanbieder met een passend profiel.

Tot slot

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

[18] Technische experts hebben de nodige kritiek, onder andere Denis Roio, interview: https://www.nrc.nl/nieuws/2024/12/22/europese-digitale-identiteit-is-straks-niet-veilig-genoeg-waarschuwen-experts-a4877532 en Jaap-Henk Hoepman, https://blog.xot.nl/2024/09/05/feedback-on-the-consultation-on-the-eid-implementing-regulations/index.html.

Hoogachtend,
namens Stichting Privacy First,

Vincent Böhre
directeur