ONAFHANKELIJK SECURITY- EN PRIVACY-ONDERZOEK

PRIVACY EN GOVERNANCE · HOOFDDOSSIER

Het Nederlandse privacy-stelsel

Hoe een uitgehongerde toezichthouder, een ongereguleerd keurmerken-ecosysteem, een commerciele tracking-cirkel rond het grootste mediabedrijf van Nederland, en een politieke lobbylaag samen het privacy-toezicht in Nederland tot compliance-theater hebben gemaakt.

Mick Beer

Security architect en privacy-onderzoeker

mickbeer.com · mijnoverheid.us

Auteur: Mick Beer

Legal Governance: Mr. Vincent Mans.

Creatiedatum: 10 mei 2026

Type: Geintegreerd onderzoeksdossier (master-master rapport)

Onderzoeksperiode: maart 2024 tot mei 2026 (24 maanden)

Methode: BeforeYouMick scanner v3.7, HAR-captures, openbare bronnen, jurisprudentie, jaarrekeningen, Tweede Kamerstukken

Doelgroep: Autoriteit Persoonsgegevens, Tweede en Eerste Kamer, onderzoeksjournalistiek, juristen, bestuurders, geinteresseerde burgers

Reproduceerbaar: alle bronnen openbaar, scanner-output JSON beschikbaar op verzoek, hashes via OpenTimestamps

Versie 1.0 · werkdocument

Bewijsclassificatie

In dit dossier worden bevindingen gemarkeerd met een bewijsklasse, om onderscheid te maken tussen empirisch geverifieerd materiaal en interpretatie.

✓ **Hard bewezen openbaar**

De bevinding is afkomstig uit een primaire openbare bron (wettekst, jurisprudentie, jaarrekening, openbaar register, leveranciers eigen documentatie). Iedere lezer kan dit binnen tien minuten zelf natrekken.

◆ **Sterk circumstantieel**

De bevinding combineert meerdere openbare bronnen tot een conclusie die niet door de afzonderlijke bron wordt uitgesproken, of berust op eigen technische scan-resultaten die met dezelfde methode reproduceerbaar zijn.

? **Vermoeden**

De bevinding is plausibel op basis van patroonherkenning of indirecte aanwijzingen, maar zonder hard bewijs. Aangewezen voor verder onderzoek.

● **Kritiek aandachtspunt**

De bevinding wijst op een actuele, ernstige situatie die specifiek aandacht behoeft van een toezichthouder of wetgever.

Samenvatting

Op het moment dat iemand de zelfmoordpreventiehulplijn 113 bezoekt, worden zijn gegevens door zes externe partijen geprofileerd, plus vijf aanvullende dataverzendingen nadat toestemming is geweigerd. Een tiener op de Kindertelefoon: dertien trackers, waarvan vier vermomd via CNAME-cloaking. Een vrouw op het Centrum Seksueel Geweld: vijf trackers, acht verzendingen na weigering. Dit zijn geen incidenten. Het is de infrastructuur.

Negen onderzochte hulpverleningssites delen vijf tot achttien trackers met Google, Meta en Adobe. Drie wettelijke kaders worden gelijktijdig overtreden: AVG artikel 7 lid 3 (intrekking toestemming), AVG artikel 9 (bijzondere persoonsgegevens), en Tw 11.7a (cookies). De Autoriteit Persoonsgegevens heeft geen capaciteit om hier structureel op te handhaven.

Dat gebrek aan capaciteit is geen toeval, het is de constante in dit dossier. De AP beschikt over circa 187 fte tegenover de 326 fte die KPMG als ondergrens adviseerde, en de 470 fte die de AP zelf als benodigde omvang doorrekende. Het budget bedraagt 53,5 miljoen euro in 2026 en daalt daarna weer, terwijl KPMG inmiddels stelt dat minimaal 100 miljoen euro per jaar nodig is. Het extra budget dat specifiek voor cookie-toezicht beschikbaar is gesteld bedraagt circa 500 duizend euro in 2026 en daalt naar 350 duizend in 2027. Hier tegenover staat een commerciële tracking-sector met honderden miljoenen advertentie-omzet. In het best gedocumenteerde geval genereert DPG Media 753 miljoen euro advertentie-omzet in 2025, terwijl op haar nieuwssites drie rechterlijke uitspraken in veertien maanden vaststelden dat tracking via Xandr en Microsoft plaatsvond zonder rechtsgeldige toestemming.

De logica van dit systeem is circulair. Een structureel onderbezette toezichthouder kan zijn taken niet uitvoeren. Een ongereguleerd keurmerken-ecosysteem vult het gat. De AP bevestigt zelf dat momenteel geen Nederlandse certificatie-instelling bevoegd is AVG-certificaten uit te geven, maar Privacy Verified wordt desondanks als compliance-signaal ingezet. Een georganiseerde lobbylaag (NDP Nieuwsmedia, OPR, brandbrief 22 mediabedrijven, Eerste Kamerlid op een uitgevers-loonlijst) maakt wetgevende interventie politiek onaantrekkelijk. Geen enkele actor afzonderlijk veroorzaakt de uitkomst, maar de optelsom werkt als systeem.

Dat systeem is niet voorbehouden aan commerciële media. De parallelle overheidsarchitectuur laat hetzelfde patroon zien: Belastingdienst (toeslagenaffaire 2,75 miljoen euro boete, FSV 3,7 miljoen euro), Marechaussee-Palantir (Kamer onvolledig geïnformeerd augustus 2025), MIVD-Datastream (80 GB locatiedata van 50 procent van alle Nederlandse telefoons, BNR januari 2024), SyRI (onverbindend verklaard door rechter februari 2020, niet door de politiek), en 60 procent van Nederlandse gemeenten die data delen met Google vóór toestemming. Allen vallen onder dezelfde structureel onderbezette AP.

Dit dossier integreert vier onderzoekslagen: het master-rapport over de commerciële tracking-cirkel, het parallel-rapport over de overheidskant, een forensisch dossier van honderd sites met 455 bevindingen (110 kritiek, 252 ernstig), en een burgerrapport van 104 sites met focus op hulpverlening. Aangevuld met dwarsdoorsneden over het

keurmerken-stelsel, Piwik PRO op 600 tot 800 overheidssites zonder openbare DPIA, en de politieke lobbylaag die het toezicht-vacuüm sinds 2021 in stand houdt.

De kern van dit rapport is niet dat individuele partijen de wet overtreden. De kern is dat de wet structureel niet gehandhaafd kán worden en dat de mensen die op dat moment het meest kwetsbaar zijn, daarvoor de hoogste prijs betalen.

Management samenvatting

Nederland heeft geen werkend privacytoezicht op tracking. Niet omdat de wet tekortschiet, maar omdat de handhaving structureel onmogelijk is gemaakt.

De Autoriteit Persoonsgegevens beschikt over 187 fte waar KPMG er minimaal 326 adviseerde, een budget dat in 2026 piekt op 53,5 miljoen euro en daarna weer daalt, en 500 duizend euro extra voor cookie-toezicht, dalend naar 350 duizend in 2027. Daar tegenover staat een tracking-industrie met honderden miljoenen omzet, een keurmerken-ecosysteem zonder AVG-erkenning, en een georganiseerde lobbylaag die wetgevende interventie politiek onaantrekkelijk maakt. Het resultaat is een circulair systeem waarin geen enkele actor afzonderlijk verantwoordelijk is voor de uitkomst.

Die uitkomst is concreet. Bezoekers van de zelfmoordpreventiehulplijn 113 worden op het moment van die klik geprofileerd door zes externe partijen. De Kindertelefoon draait dertien trackers. Het Centrum Seksueel Geweld acht dataverzendingen nádat toestemming is geweigerd. Drie wettelijke kaders worden op deze sites gelijktijdig overtreden. De AP heeft geen capaciteit voor structureel onderzoek naar deze categorie.

Hetzelfde mechanisme speelt bij de overheid zelf: Belastingdienst, Marechaussee, MIVD, gemeenten. Allen onder dezelfde onderbezette toezichthouder.

Dit rapport documenteert het systeem en niet de individuele overtreder. De aanbevelingen richten zich op de structuur, niet op incidentele handhaving.

Kernbevindingen met bewijsklasse

De acht kernbevindingen hieronder zijn geordend naar bewijsklasse zoals toegelicht in de sectie Bewijsclassificatie. De classificatie maakt expliciet wat empirisch is vastgesteld en wat interpretatie of vermoeden betreft.

✓ **Hard bewezen openbaar.** DPG Media realiseerde 753 miljoen euro advertentie-omzet in 2025. Bron: jaarrekening en geconsolideerde cijfers DPG Media Group.

✓ **Hard bewezen openbaar.** Tegen de adverterende infrastructuur rond DPG zijn in veertien maanden drie rechterlijke vonnissen gewezen over tracking zonder rechtsgeldige toestemming. Bron: gepubliceerde jurisprudentie, te raadplegen via rechtspraak.nl.

✓ **Hard bewezen openbaar.** De Autoriteit Persoonsgegevens beschikt over circa 500 duizend euro per jaar voor cookie-handhaving, tegenover een structureel tekort dat de toezichthouder zelf en extern advies (KPMG) hebben gedocumenteerd. Bron: AP-jaarstukken en openbaar KPMG-advies.

✓ **Hard bewezen openbaar.** De Autoriteit Persoonsgegevens bevestigt zelf dat momenteel geen Nederlandse certificatie-instelling AVG-certificaten onder artikel 42 mag uitgeven. Bron: publieke mededeling AP.

◆ **Sterk circumstantieel.** De verhouding tussen het cookie-handhavingsbudget en de advertentie-omzet die het zou moeten controleren is ongeveer 1 op 1500. Deze verhouding volgt uit de combinatie van twee openbare cijfers en wordt door geen van beide bronnen afzonderlijk uitgesproken.

◆ **Sterk circumstantieel.** Negen onderzochte hulpverleningssites delen 5 tot 18 trackers met Google, Meta en Adobe. Een bezoeker van hulplijn 113 wordt op het moment van de klik geprofileerd door zes externe partijen. Bron: eigen technische scans, reproduceerbaar met dezelfde methode.

◆ **Sterk circumstantieel.** Op naar schatting 600 tot 800 overheidssites draait analytics-software waarvan de juridische status onder de Amerikaanse Cloud Act niet publiek is onderbouwd. De schatting combineert openbare bronvermeldingen en eigen waarneming.

? **Vermoeden.** De optelsom van uitgehongerd toezicht, een ongereguleerd keurmerken-ecosysteem en een politieke lobbylaag functioneert als een zichzelf in stand houdend geheel. Dat dit samenhangend mechanisme bewust is ontworpen, is niet vastgesteld en wordt hier niet beweerd; het patroon is plausibel op basis van de gedocumenteerde schakels en is aangewezen voor verder onderzoek.

> *De kern in vier zinnen. Het grootste mediabedrijf van Nederland draait een tracking-mechanisme dat 17 miljoen Nederlanders volgt op nieuwssites zonder rechtsgeldige toestemming, met 753 miljoen euro advertentie-omzet. Het cookie-toezicht heeft daarvoor 500 duizend euro per jaar, een verhouding van 1 op 1500. Op 800 overheidssites draait een tracker waarvan de juridische status onder Cloud Act niet is gepubliceerd, gecertificeerd door een commercieel keurmerk dat de Autoriteit Persoonsgegevens niet erkent. Onderwijl worden*

> *bezoekers van Humanitas, SOA Aids, het Centrum Seksueel Geweld en hulplijn 113 op het moment van hun klik commercieel geprofileerd door Google, Facebook en Adobe.*

Dit dossier maakt het mechanisme zichtbaar. Wat ermee gebeurt, is een vraag voor wie het leest.

Inhoudsopgave

1. Inleiding en methodologie

1.1 Wat dit dossier is

Dit is een geintegreerd onderzoeksdossier. Het brengt vier eerder gepubliceerde of in werkdocument-status circulerende dossiers samen, plus aanvullend materiaal uit zes maanden veldonderzoek. Het is geschreven om een onderzoeksredactie, een Tweede of Eerste Kamerlid, een toezichthouder, of een geinteresseerde burger in een aanvaardbare leestijd het hele patroon te laten zien.

Het is geen juridische aanklacht. Het bevat geen verdachtmakingen tegen personen. Iedere claim is voorzien van een primaire openbare bron of wordt expliciet als sterk circumstantieel of vermoeden gemarkeerd. De methodologie is reproduceerbaar voor wie de scanner zelf wil draaien of de bronnen zelf wil opzoeken.

1.2 Waarom dit dossier nu, en niet eerder of later

Vier signalen vallen samen in de eerste helft van 2026.

- De Eerste Kamer behandelt naar verwachting in de tweede helft van 2026 of begin 2027 de Digital Omnibus, een EU-voorstel dat het beschermingsniveau van de AVG aanpast. Het kabinet-Jetten heeft op 8 april 2026 via staatssecretaris Van Bruggen (D66, Justitie en Veiligheid) een non-paper naar Brussel gestuurd met serieuze zorgen, maar heeft een minderheid in de Eerste Kamer (22 van 75 zetels).
- Op 6 mei 2026 wees de Haagse rechter een kort geding van drie burgers af om de DigiD-leverancier Solvinity te dwingen geen contract te verlengen ondanks de overname door het Amerikaanse Kyndryl. De Cloud Act exposure van DigiD is daarmee bestendigd.
- De drie Xandr-vonnissen (5 december 2023, 7 juni 2024, 12 februari 2025) bouwen civielrechtelijke jurisprudentie op die door iedere burger met een advocaat in Rotterdam herhaald kan worden tegen iedere uitgever met vergelijkbare cookie-praktijk.
- De Privacy Verified register-discrepantie (17 organisaties op publiek register tegenover marketing claim van plus 90 deelnemers), gecombineerd met het feit dat Piwik PRO, partner en klant en leverancier in een, op 600 tot 800 Nederlandse overheidssites draait zonder openbare DPIA en zonder zichtbare Cloud Act mitigatie, maakt het keurmerken-stelsel publicatieklaar voor onderzoek.

1.3 Methodologie technische scans

De technische bewijslast in hoofdstuk 3 is verzameld met BeforeYouMick scanner versie 3.7. Dat is een Python-Playwright tool, headless Chromium build 1217, DNS-resolver Cloudflare 1.1.1.1, schone browser-context per sessie (geen cookies, geen storage, geen extensies, geen profile-data).

Per site worden drie sessies achter elkaar uitgevoerd:

- noop. Laad de pagina, klik niets aan, registreer wat de site uit zichzelf zet.
- refuse. Laad de pagina, zoek heuristisch een knop met tekst zoals 'weigeren', 'afwijzen', 'alleen noodzakelijk', en klik die aan. Registreer wat blijft draaien na de klik.
- accept. Laad de pagina, klik op 'accepteren'. Registreer de complete tracking-stack.

Tijdens elke sessie worden vastgelegd: cookies (naam, domein, levensduur, samesite, secure, httpOnly, type, first of third party), localStorage en sessionStorage, alle netwerk-requests met externe-domein-tellingen, gedetecteerde tracker-scripts en pixels, response-headers, en aanwezigheid plus zichtbaarheid van consent-banner. Voor elk subdomein wordt een DNS CNAME-lookup uitgevoerd om first-party cloaking te detecteren tegen een vendor-database (Adobe data.adobedc.net, Piwik PRO, Hotjar, Criteo, ContentSquare, demdex.net, omtrdc.net).

Per site worden de drie modes onderling vergeleken om te bepalen welke trackers daadwerkelijk persistent blijven na een refuse-klik. Een refuse-knop die het probleem niet oplost wordt expliciet gerapporteerd. De rauwe output is JSON per site, met SHA256-checksums in een bijlage voor integriteitsverificatie.

1.4 Methodologie openbare bronnen

Voor de niet-technische bevindingen (cashflow, juridische veroordelingen, parlementaire registers, jaarrekeningen, KvK-uittreksels) is uitsluitend gewerkt met primaire openbare bronnen. Iedere claim heeft een url of vindplaats in het bijbehorende bronnenoverzicht. Geen anonieme bron, geen vertrouwelijke document, geen lekje. Alles staat open en bloot op het internet, in jaarrekeningen, in jurisprudentie, in Tweede Kamerstukken.

Het zes maanden onderzoekswerk zat in het bij elkaar leggen van openbare bronnen die niemand eerder samen had bekeken, plus de technische scans die laten zien wat browser-zijdig waarneembaar is. De configuratie aan server-zijde (welke Azure-regio, welke encryptiesleutels, welke contractuele waarborgen) is niet openbaar en wordt door deze scans niet ontsloten.

1.5 Wat dit dossier expliciet niet beweert

Drie dingen worden expliciet niet beweerd.

- Geen specifieke persoon doet iets illegaals. Sander Dekker mocht een aangenomen motie naast zich neerleggen. Marjolein van der Linden mag betaalde nevenfuncties hebben mits gemeld. Frits Campagne mocht voorzitter NDP zijn na een loopbaan bij een grote uitgever. Een minister mag de Kamer onvolledig informeren zonder dat dat strafbaar is. Het dossier wijst op de optelsom van legale handelingen, niet op individuele wetsovertreding.
- Geen sprake van financiele verrijking van DPC-medewerkers. Eerdere onderzoekssporen hebben geen aanwijzingen opgeleverd dat Warmoeskerken, Vuursteen of andere DPC-medewerkers persoonlijk financieel voordeel hebben gehad van de Piwik PRO relatie. Wat er wel is: dertien jaar continuiteit zonder

zichtbare aanbesteding en zonder publieke DPIA. Dat is institutioneel verwijtbaar, niet persoonlijk.

- Geen complot, wel patroon. Het systeem werkt zonder dat de spelers hoeven samen te spannen. Iedere speler verdedigt zijn legitieme functie-belang. De optelsom is een uitgehongerd toezicht plus commerciele keurmerk-dekking plus politieke bescherming. Dat is het patroon.

2. Het mechanisme als geheel

Voor wie het hele dossier in een hoofdstuk wil zien, hier het mechanisme uitgewerkt. De rest van het dossier vult dit in met namen, datums, bedragen en bronnen.

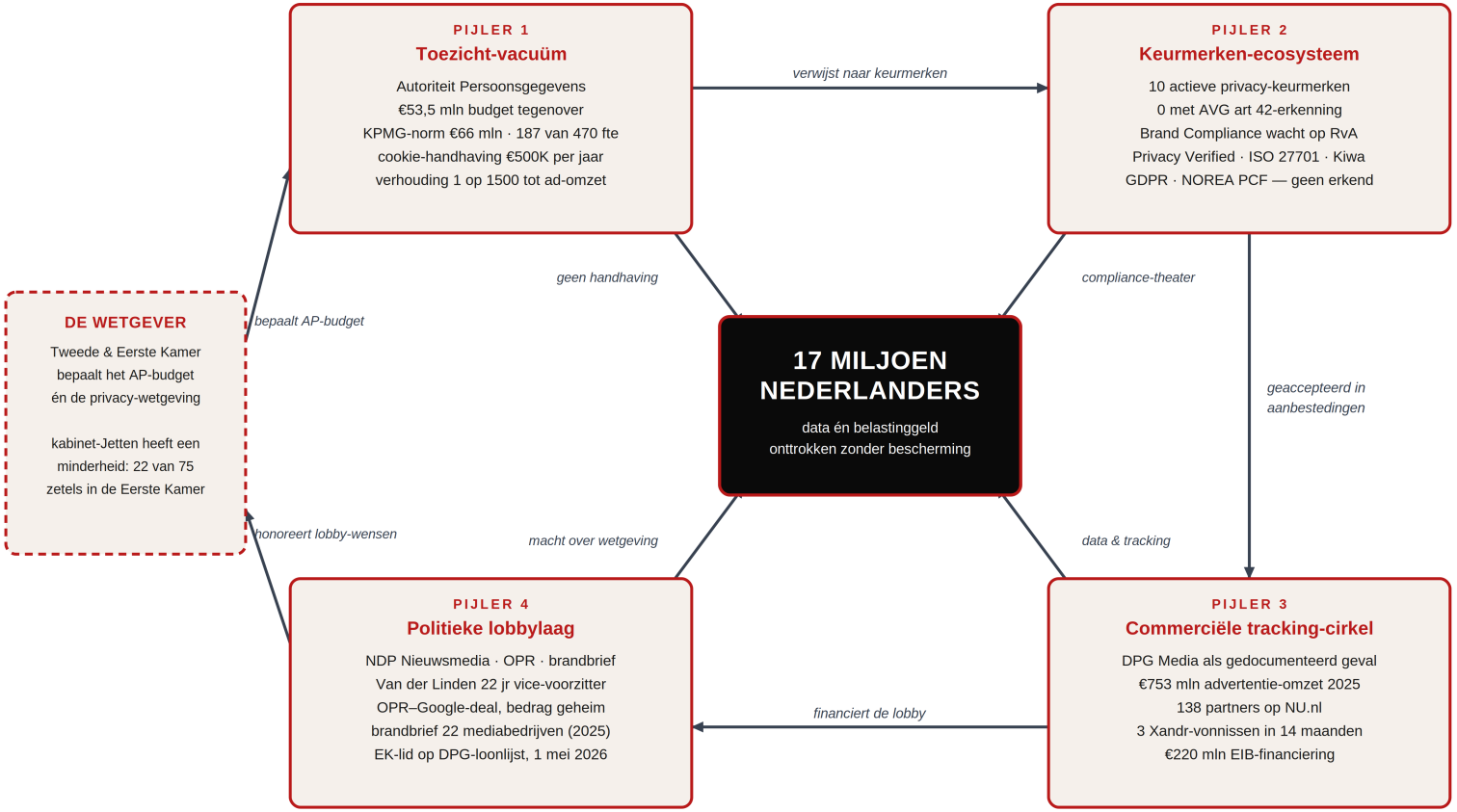
2.1 De vier pijlers

Het Nederlandse privacy-stelsel rust op vier pijlers, die elkaar onderling versterken zonder dat een van de pijlers de andere bewust ondersteunt.

> *Pijler 1. Een uitgehongerde toezichthouder. De Autoriteit Persoonsgegevens beschikt in 2026 over 53,5 miljoen euro totaalbudget, een bedrag dat volgens de Rijksbegroting in de jaren daarna weer daalt, tegenover een door KPMG geadviseerde 66 miljoen euro en een door de AP zelf becijferde behoefte van minimaal 100 miljoen euro per jaar. De personele bezetting ligt rond 187 fte, tegenover de 470 fte die KPMG noodzakelijk achtte. Voor cookie-handhaving specifiek: 500 duizend euro per jaar tot 2026, daarna structureel 350 duizend euro. Dat is 1500 keer minder dan de advertentie-omzet van een enkele uitgever (DPG, 753 miljoen euro in 2025) waarop AP geacht wordt toezicht te houden.*
>
> *Pijler 2. Een ongereguleerd keurmerken-ecosysteem. Tien actieve privacy- en informatiebeveiligingskeurmerken op de Nederlandse markt. Volgens de toezichthouder zelf (op de eigen website) mag op dit moment geen Nederlandse certificatie-instelling AVG-certificaten uitgeven. Brand Compliance BC 5701 heeft AP-goedkeuring criteria sinds oktober 2023 maar wacht nog op RvA-accreditatie. Privacy Verified, ISO 27701, NOREA Privacy Audit Proof, Kiwa eigen AVG GDPR: geen van allen erkend. Toch worden zij gebruikt als compliance-bewijs in aanbestedingen, marketing en bestuurlijke verantwoording.*
>
> *Pijler 3. Een commerciele tracking-cirkel. De grote Nederlandse nieuwsuitgevers draaien advertentie-platforms die lezers volgen zonder rechtsgeldige toestemming. Het best gedocumenteerde geval is DPG Media: 138 partners op NU.nl, 40 POSTs naar Xandr na een 'weigeren'-klik op de Volkskrant-site, drie civielrechtelijke veroordelingen in 14 maanden, advertentie-omzet 753 miljoen euro in 2025. EIB-financiering vanuit Brussel: 220 miljoen euro tussen 2022 en 2024.*
>
> *Pijler 4. Een politieke lobbylaag met vier instrumenten. NDP Nieuwsmedia (uitgevers-koepel, vice-voorzitter Marjolein van der Linden 22 jaar onafgebroken). OPR (collectief incassovehikel met geheime Google-deal van 14 april 2025). Brandbrief Stichting Democratie en Media van 22 mediabedrijven aan informateur Buma in december 2025, wensen volledig gehonoreerd in coalitieakkoord 'Aan de slag' (30 januari 2026). Eerste Kamerlid Marjolein van der Linden (VVD) sinds 1 mei 2026 formeel op DPG-loonlijst als Manager public affairs.*

De vier pijlers van het stelsel

Geen pijler staat boven de andere — vier mechanismen versterken elkaar rond hetzelfde centrum



HACKEDEMIA
Onafhankelijke security en privacy-journalistiek

hackedemia.nl
Mick Beer · Mei 2026

Elke pijler is afzonderlijk verdedigbaar; samen vormen ze een zichzelf in stand houdend geheel.

Figuur 2.1 De vier pijlers van het stelsel. Pijler 1 (toezicht-vacuum AP), Pijler 2 (keurmerken-ecosysteem), Pijler 3 (commerciele tracking-cirkel), Pijler 4 (politieke lobby). Geen pijler is hierarchisch boven de andere; alle vier versterken elkaar wederzijds rond hetzelfde centrum: 17 miljoen Nederlanders waarvan data en belastinggeld worden onttrokken zonder effectieve bescherming.

2.2 Hoe de pijlers elkaar versterken

Het systeem is circulair, niet hierarchisch. Geen partij is de eindbaas. De versterking loopt langs zeven stappen die elk afzonderlijk verdedigbaar zijn.

- Stap 1. AP heeft te weinig capaciteit voor structurele handhaving (Pijler 1).
- Stap 2. AP verwijst impliciet of expliciet naar keurmerken als alternatief mechanisme (Pijler 2).
- Stap 3. Aanbestedingen vragen 'een privacy keurmerk' zonder specificatie of juridische toets.
- Stap 4. Leveranciers (commercieel of overheid-beheerd) leveren ISO 27701 of Privacy Verified, gecertificeerd door een keurmerk dat juridisch geen AVG-betekenis heeft.
- Stap 5. De feitelijke privacy-praktijk wordt niet aangetast (Pijler 3, in de commerciele variant; analoge schending in de overheidsvariant via Piwik PRO, Adobe Analytics, Google Analytics).
- Stap 6. Bij een incident wijst de organisatie op het keurmerk; AP heeft de capaciteit niet om de werkelijke privacy-praktijk te toetsen; de keurmerk-eigenaar wijst op de werkelijke verantwoordelijkheid van de gecertificeerde.
- Stap 7. De wetgever die het AP-budget bepaalt heeft een eigen lobby-circuit (Pijler 4) dat een uitbreiding van de toezicht-capaciteit politiek onaantrekkelijk maakt. Terug naar stap 1.

2.3 Wie verdient wat

Het ecosysteem is commercieel rendabel voor alle deelnemende partijen, en politiek geaccepteerd omdat de toezichthouder uitgehongerd is.

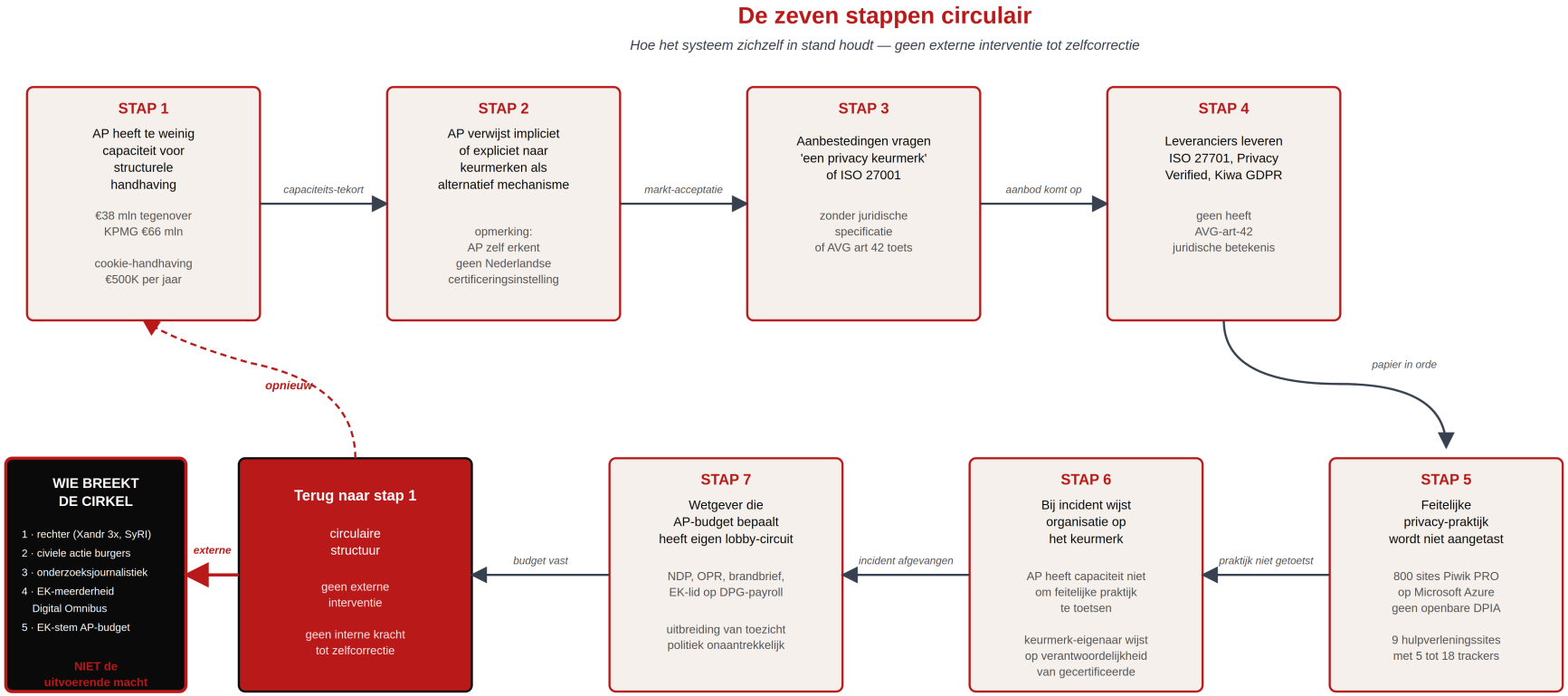
- DPG Media: 753 miljoen euro advertentie-omzet en 238 miljoen euro nettowinst in 2025 — het best gedocumenteerde geval van de commerciele tracking-cirkel (hoofdstuk 4).
- Microsoft (Xandr-adserver): centrale spil van het Trusted Web-platform sinds 2022, drie veroordelingen in 14 maanden, maximum dwangsom 50 duizend euro per gedaagde, geen aanpassing van praktijk.
- Microsoft (Azure-hosting): infrastructuur waar Piwik PRO Cloud op draait, en waar Solvinity DigiD via PaaS-producten op leunt.
- Piwik PRO (Wroclaw, Polen, sinds eind 2023 eigendom Kirk Kapital Denemarken): tussen 5 en 15 miljoen euro directe licentiekosten over 13 jaar Nederlandse rijksoverheid, plus 2 tot 8 miljoen euro implementatiekosten, plus 1 tot 3 miljoen euro consultancy.
- Certificatie-instellingen (Kiwa, BSI, DNV, TUV NORD, Brand Compliance, DigiTrust, DEKRA, Bureau Veritas): tarieven 15 duizend tot 100 duizend euro per audit, plus jaarlijkse cyclus.

- ICTRecht en dochter Privacy Verified: drie commerciele stappen binnen een concern (DPIA-werk, audit, certificaat), plus partnerprogramma.
- Adviesbureaus (Securesult, Promeetec, ICT Institute, certificeringsadvies, Nieuwhuis Consult, AVGdesk, ISO2HANDLE): 25 duizend tot 150 duizend euro per certificeringstraject.
- Auditors (NOREA-leden, IT-auditors): dagtarieven 1000 tot 1800 euro.

Geen speler heeft een commercieel belang om te onderzoeken of keurmerken inhoudelijk doen wat de markt aanneemt. De enige partij met dat belang zou de toezichthouder zijn. Die heeft de capaciteit niet.

2.4 De zeven stappen in een diagram

Onderstaand diagram toont de circulaire structuur van de zeven stappen. Geen partij is hierarchisch boven de andere. Iedere stap is verdedigbaar binnen het eigen kader, de optelsom is een gesloten kringloop. Externe interventie (rechter, civiele actie, journalistiek, parlementaire meerderheid) is de enige route tot doorbreking.



Figuur 2.4 De zeven stappen circulair. Elke stap is op zichzelf verdedigbaar; de optelsom is een gesloten kringloop die alleen door externe interventie wordt doorbroken.

Externe interventie (rechter, civiele actie, journalistiek, parlementaire meerderheid) is de enige route tot doorbreking van deze cirkel. Dit diagram werkt op meerdere plekken in dit dossier door: de cashflow staat in figuur 4.1, de parallelle architectuur in figuur 5.1, de hulpverleningssites in figuur 3.6.

3. Technische bewijslast: 100 plus sites

Dit hoofdstuk bevat de empirisch geverifieerde meetresultaten waarmee de stelselbeweringen in dit dossier worden onderbouwd. Twee scan-rondes worden samengebracht: het forensisch dossier van 100 sites (gemeten 2 mei 2026, 23:05 tot 00:02 CEST, BeforeYouMick scanner v3.3.1) en het burgerrapport van 104 sites (gemeten 9 en 10 mei 2026, BeforeYouMick scanner v3.7). Beide scans zijn reproduceerbaar via dezelfde tool met dezelfde input-lijst.

3.1 De casus 113: het stelsel aan een website

Iemand opent 's nachts de website van 113 Zelfmoordpreventie. Niet om iets te kopen, niet om een dienst te vergelijken, maar om hulp te zoeken op een moment dat het er echt toe doet. Deze paragraaf volgt die ene klik. Niet omdat 113 uniek slecht presteert, andere hulpverleningssites zijn vergelijkbaar of erger, maar omdat een enkele site, scherp uitgemeten, het hele mechanisme van dit dossier zichtbaar maakt: wat er technisch gebeurt, waarom het in strijd is met de wet, waarom niemand het corrigeert, en waarom het keurmerk dat geruststelling moet bieden dat niet doet. De volledige meting van alle hulpverleningssites volgt in paragraaf 3.6.

Wat er gebeurt bij de klik

De technische scan in dit dossier (BeforeYouMick scanner, methode beschreven in hoofdstuk 1.3) laadt elke site drie keer: zonder iets aan te klikken, na een klik op 'weigeren' of 'alleen noodzakelijk', en na 'accepteren'. Op het moment dat de bezoeker de pagina van 113 opent, wordt het bezoek al gedeeld met zes externe partijen. En cruciaal: ook nadat de bezoeker actief op weigeren heeft geklikt, blijven er vijf POSTs uitgaan, vijf keer dat er data vanuit de browser naar een advertentie- of analysepartij wordt verstuurd.

Een POST is geen technisch detail. Het is het moment waarop informatie het toestel van de bezoeker verlaat en bij een derde terechtkomt. De bezoeker heeft het goede gedaan, nee gezegd, en wordt alsnog gevolgd. De weigerknop is op deze site geen rem, maar een placebo.

Waarom dit in strijd is met de wet

Op deze ene handeling lopen drie wettelijke kaders tegelijk vast. De AVG (artikel 9) merkt gegevens over iemands gezondheid aan als bijzondere persoonsgegevens, met een verzwaard beschermingsregime; verwerking is in beginsel verboden, tenzij een strikte uitzondering geldt. Het enkele feit dat iemand 113 bezoekt, is al zo'n gevoelig gegeven, het zegt iets over een psychische toestand. De AVG (artikel 7, lid 3) eist daarnaast dat toestemming even eenvoudig in te trekken is als te geven; een 'weigeren' die genegeerd wordt, voldoet daar niet aan. En de Telecommunicatiewet (artikel 11.7a) staat trackers pas toe na toestemming, hier draaien ze ervoor en erna.

Drie kaders, gelijktijdig, op de meest kwetsbare categorie bezoekers die er bestaat. Dit is geen juridisch randgeval. Dit is precies waar de wet voor bedoeld is.

Waarom niemand het corrigeert

De toezichthouder die hier zou moeten optreden, de Autoriteit Persoonsgegevens, beschikt in 2026 over circa 187 fte en een totaalbudget van 53,5 miljoen euro, dat volgens de Rijksbegroting in de jaren daarna verder daalt. Voor cookie-handhaving specifiek is daarvan ongeveer 500 duizend euro per jaar geoormerkt. Dat halve miljoen moet toezicht dekken op

elke Nederlandse website, commercieel en publiek, inclusief de sites waar kwetsbare mensen hulp zoeken. Er is geen capaciteit voor structureel, actief onderzoek naar deze categorie.

Dat is geen onbekend probleem. De Tweede Kamer nam op 9 februari 2021 de motie-Hijink aan, die de regering vroeg het AP-budget te verhogen richting het niveau dat KPMG in opdracht van het kabinet zelf had berekend. De motie werd niet uitgevoerd. Een bezoeker van 113 is daarmee in de praktijk onbeschermd, niet omdat de wet ontbreekt, maar omdat het orgaan dat de wet moet handhaven dat niet kan.

Waarom het keurmerk aan de muur niet helpt

Een organisatie kan een privacy- of informatiebeveiligingskeurmerk voeren en tegelijk haar bezoekers volgen zoals hierboven beschreven. Dat kan, omdat de keurmerken op de Nederlandse markt geen AVG-erkenning hebben: de Autoriteit Persoonsgegevens bevestigt zelf dat op dit moment geen Nederlandse certificatie-instelling AVG-certificaten onder artikel 42 mag uitgeven. Een keurmerk toetst het papierwerk, een verwerkingsregister, een DPIA in de la, niet de feitelijke praktijk in de browser van de bezoeker.

Daarmee verifieert het enige signaal waarop een burger, een inkoper of een bestuurder zou kunnen afgaan om te denken 'dit zit goed' precies het verkeerde.

Wat deze ene site laat zien

Deze vier slagen zijn het dossier in het klein. Vervang '113' door de Kindertelefoon, het Centrum Seksueel Geweld of Humanitas en het patroon herhaalt zich: dit dossier documenteert negen hulpverleningssites die 5 tot 18 trackers delen met Google, Meta en Adobe. 113 staat hier niet als het ergste geval, maar als het helderste. Alles wat in de rest van dit dossier volgt, de bredere technische bewijslast, de commerciele cirkel, het toezicht-vacuum, het keurmerken-ecosysteem, de politieke lobbylaag, is het antwoord op een enkele vraag: hoe kan het dat een nachtelijke klik op een zelfmoordpreventie-site eindigt bij zes commerciele partijen, juridisch onbeschermd, met een keurmerk aan de muur dat niets zegt.

Wie dit leest en zelf aan zelfmoord denkt, of zich zorgen maakt om iemand anders: 113 Zelfmoordpreventie is bereikbaar via 113 of 0800-0113.

3.2 Cijfers in een oogopslag

Resultaten van de scan op 2 mei 2026, 100 sites, 300 sessies (drie modes per site):

Sites onderzocht	**100**
Sessies totaal	**300 (3 modes maal 100 sites)**
Totaal bevindingen	**455**
Kritiek (ernstige overtreding AVG of Tw)	**110**
Ernstig (sterke aanwijzing schending)	**252**
Let op (best practice afwijking)	**93**
Sites met minstens een kritieke bevinding	**73 op 100**
Sites zonder enige bevinding	**2 op 100 (klm.com, zalando.nl)**
Sites zonder herkenbare cookiebanner	**92 op 100**

Sites met werkende refuse-knop	**44 op 100**
Refuse-knoppen die echt tracking stoppen	**0 op 44**
Sites met first-party CNAME-cloaking	**49 op 100**
Cloaking-vendors uniek	**8**
Cloaking-bevindingen totaal	**87**

De 104-sites scan van 9 en 10 mei 2026 leverde een vergelijkbare verdeling: 89 kritieke bevindingen, 383 ernstige, 138 let op, 115 CNAME-cloaking detecties. 58 procent van de sites had minstens een kritieke bevinding, 92 procent minstens een ernstige.

3.3 De refuse-knop als placebo

Op 44 van de 100 sites in de eerste scan kon de scanner een knop met tekst zoals 'weigeren', 'afwijzen', 'alleen noodzakelijk' of 'alleen functioneel' vinden en aanklikken. Op de andere 56 sites was er geen werkende refuse-knop, vaak omdat er geen banner werd getoond, soms omdat de banner alleen een accept-optie had, in een aantal gevallen omdat de knop achter een tweede klik verborgen zat (een dark pattern op zich).

Vervolgens is per site vergeleken welke tracking-cookies en welke tracker-scripts blijven actief na de refuse-klik (de refuse vergeleken met noop delta).

> *Het resultaat is unaniem. Effectief (geen tracking persistent na refuse): 0 op 44. Gedeeltelijk (maximaal 2 cookies, geen externe trackers): 0 op 44. Onwerkzaam (meer dan 2 cookies of trackers blijven): 44 op 44.*

Niet een Nederlandse website uit deze meting honoreert een refuse-klik op de manier die de Telecommunicatiewet en de AVG vereisen. Telecommunicatiewet artikel 11.7a en AVG artikel 7 lid 3 verplichten dat de bezoeker dezelfde mate van controle krijgt om consent in te trekken als om die te geven. Een knop die er staat maar niets stopt, voldoet niet.

Voorbeelden zijn ronduit illustratief. Op volkskrant.nl werden in eerder cookie-onderzoek (Mick Beer, Medium maart 2026) na een refuse-klik 40 POST-requests naar adnxs-simple.com slash ut slash v3 gestuurd, het Xandr-eindpunt. Op telegraaf.nl 23 GET-requests naar pagead2.googlesyndication.com. Op nu.nl 138 advertentiepartners actief tegenover de eigen claim van 104. Een 8 op 1 dark pattern (8 klikken om te weigeren, 1 om te accepteren).

3.4 Cookies en trackers voor consent

Op 92 van de 100 sites detecteerde de scanner geen zichtbare cookiebanner in noop-modus. De meeste van die sites zetten wel tracking-cookies of laden externe trackers voor er enige toestemming gegeven kan worden, een directe schending van Telecommunicatiewet artikel 11.7a.

Top tracking-cookies voor consent:

Cookie	Sites	Bron / Vendor
_ga	73	Google Analytics

Cookie	Sites	Bron / Vendor
_vwo_uuid_v2	20	VWO (Wingify, India)
_sp_id.e23f	18	DPG Media Snowplow
_vis_opt_s en gerelateerd	15	VWO
FPLC	15	Cloudflare LB
stg_traffic_source_priority	13	Piwik PRO
stg_last_interaction	13	Piwik PRO
_sp_ses.e23f	12	DPG Media Snowplow
stg_returning_visitor	12	Piwik PRO
s_fid	9	Adobe Analytics
s_vi	9	Adobe Analytics

Top externe trackers voor consent:

Tracker-domein	Sites	Vendor en jurisdictie
googletagmanager.com	90	Google LLC, USA
region1.google-analytics.com	28	Google LLC, USA
pagead2.googlesyndication.com	24	Google Ads, USA
cdn.cookielaw.org	12	OneTrust, USA
w.usabilla.com	11	GetFeedback (SurveyMonkey), USA
geolocation.onetrust.com	11	OneTrust, USA
clarity.ms	8	Microsoft Clarity, USA
fonts.googleapis.com	8	Google Fonts, USA
consent.cookiebot.com	7	Cybot A/S, EU/DK
dev.visualwebsiteoptimizer.com	7	VWO, India
cdn.optimizely.com	6	Optimizely, USA

Google Tag Manager wordt voor consent geladen op 90 van de 100 sites, inclusief overheidssites die in hun cookieverklaring beweren geen Google te gebruiken. Dat betekent voor 90 op 100 sites een directe schending van Telecommunicatiewet artikel 11.7a.

3.5 CNAME-cloaking als first-party camouflage

Op 49 van de 100 sites is first-party CNAME-cloaking aangetroffen. Een subdomein van de site zelf is via DNS doorverwezen naar de infrastructuur van een tracking-vendor. Voor de browser ziet het verkeer eruit als first-party. Cookies worden bewaard onder het hoofd-domein. Browser-mechanismen tegen third-party tracking (Safari ITP, Firefox ETP) herkennen het niet. Tracker-blockers (uBlock Origin, Adblock Plus, Privacy Badger) zien geen vendor-domein.

Vendors via CNAME-cloaking, gerangschikt naar bevindingen:

Vendor	Bevindingen	Sites
Criteo (proxied)	21	10
Piwik PRO Cloud (proxied)	19	13
Hotjar (proxied)	18	14
Adobe Audience Manager	10	7
ContentSquare (proxied)	7	4
Adobe Analytics (legacy)	5	5
Adobe Analytics (FPDC)	5	5
Adobe Analytics (legacy SiteCatalyst)	2	2

Adobe Experience Cloud bij overheid en banken

Twaalf sites verbergen Adobe-tracking via first-party CNAMEs (data.adobedc.net, omtrdc.net, demdex.net): allianz.nl, asnbank.nl, belastingdienst.nl, delta.nl, gamma.nl, kpn.com, lidl.nl, nn.nl, regiobank.nl, snsbank.nl, telegraaf.nl, unive.nl.

De drie Volksbank-merken (ASN, SNS, Regiobank) cloaken alle drie via dezelfde Adobe-tenant: dpm.demdex.net, snsbank.demdex.net (Audience Manager voor cross-site profiling) en snsbank.tt.omtrdc.net (Adobe Target voor A/B-testing). Een gedeelde Volksbank-koepelconfiguratie.

Piwik PRO Cloud op rijksoverheid

Dertien sites cloaken Piwik PRO Cloud onder een eigen subdomein. Daaronder rijksoverheid.nl (statistiek.rijksoverheid.nl wijst CNAME naar rijksoverheid.piwik.pro), uwv.nl, koop.overheid.nl en andere rijksoverheidssites. Dit aspect wordt uitgebreid behandeld in hoofdstuk 8 (Cloud Act blootstelling).

3.6 Hulpverleningssites en kwetsbare doelgroepen

Een specifieke deelverzameling van het 104-sites burgerrapport bestaat uit Nederlandse websites die hulp aanbieden aan kwetsbare doelgroepen: psychische nood, eenzaamheid, seksueel geweld, suicide, kinderen jonger dan 18, slachtofferhulp. Op deze sites is privacy geen abstract recht. Een bezoek aan zulke sites is op zichzelf een sterke aanwijzing voor mogelijke kwetsbaarheid van de bezoeker. Onder AVG artikel 9 (bijzondere persoonsgegevens) is profilering van zulke bezoeken op zijn minst juridisch wankel.

Toch tonen de scans dat alle negen onderzochte hulpverleningssites tracking-cookies en externe trackers laden voor consent, plus dat de meeste een werkbare refuse-knop ontberen. Onderstaande tabel geeft een overzicht.

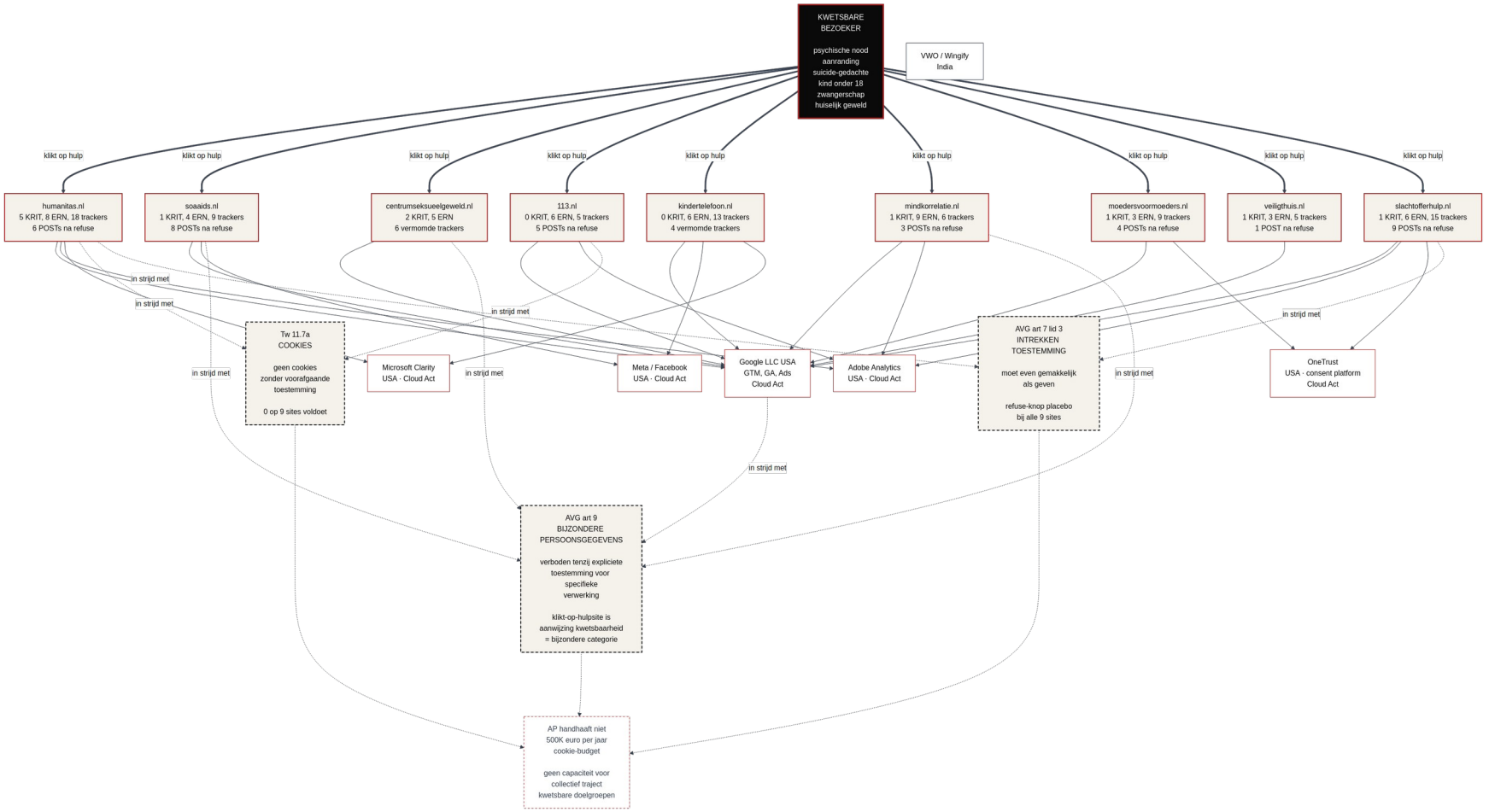
Hulpverleningssite	Kritiek	Ernstig	Externe partijen	Bijzonderheid
humanitas.nl	5	8	18	6 POSTs na refuse
soaaids.nl	1	4	9	8 POSTs na refuse
centrumseksueelgeweld.nl	2	5	0	6 vermomde trackers
113.nl (zelfmoordpreventie)	0	6	5	5 POSTs na refuse

Hulpverleningssite	Kritiek	Ernstig	Externe partijen	Bijzonderheid
kindertelefoon.nl (kinderen <18)	0	6	13	4 vermomde trackers
mindkorrelatie.nl (GGZ)	1	9	6	3 POSTs na refuse
moedersvoormoeders.nl (zwangerschap)	1	3	9	4 POSTs na refuse
veiligthuis.nl (huiselijk geweld)	1	3	5	1 POST na refuse
slachtofferhulp.nl	1	6	15	9 POSTs na refuse

> *Wat dit betekent. Een persoon in psychische nood die op humanitas.nl klikt om hulp te zoeken, wordt op het moment van die klik door zes POST-requests aan advertentie-eindpunten gemeld. Een persoon die het Centrum Seksueel Geweld bezoekt na een aanranding, wordt door zes vermomde trackers (CNAME-cloaked) geprofileerd. Een tiener die de Kindertelefoon bezoekt voor hulp bij eenzaamheid, wordt door dertien externe partijen herkend. Die personen weten dat niet.*

De juridische situatie is helder. AVG artikel 9 verbiedt verwerking van bijzondere persoonsgegevens (inclusief gegevens betreffende gezondheid en sexueel leven) tenzij specifieke uitzondering, waaronder expliciete toestemming. AVG artikel 7 lid 3 verplicht dat het intrekken van toestemming even gemakkelijk moet zijn als het geven. Telecommunicatiewet artikel 11.7a verplicht voorafgaande toestemming voor cookies tenzij strikt noodzakelijk voor de gevraagde dienst. Op de negen genoemde hulpverleningssites wordt aan geen van die drie eisen voldaan.

De feitelijke privacy-bescherming op deze sites toont dat het keurmerken-stelsel niet werkt voor de groep die het meest beschermd zou moeten worden. Een organisatie kan ISO 27701 gecertificeerd zijn, NEN 7510 nageleefd hebben, Privacy Verified gecertificeerd zijn, en tegelijk een website draaien met 18 trackers en zes POSTs na refuse. De certificering toetst de papierwerk en het managementsysteem, niet de feitelijke uitvoering op de live website.



Figuur 3.6 Hulpverleningssites en bezoeker-tracking. Negen onderzochte hulpverleningssites (humanitas.nl, soaaids.nl, centrumseksueelgeweld.nl, 113.nl, kindertelefoon.nl, mindkorrelatie.nl, moedersvoormoeders.nl, veiligthuis.nl, slachtofferhulp.nl) plus zes externe partijen die data ontvangen waarvan vijf onder Cloud Act vallen (Microsoft Clarity, Meta/Facebook, Google LLC USA, Adobe Analytics, OneTrust). Drie geschonden wettelijke kaders: AVG art 7 lid 3 (intrekken toestemming), AVG art 9 (bijzondere persoonsgegevens), Tw 11.7a (cookies). AP-handhaving 500K euro per jaar dekt geen capaciteit voor structureel onderzoek naar deze categorie sites.

3.7 Specifieke casus humanitas.nl

Humanitas is een vrijwilligersorganisatie die ondersteuning biedt aan mensen in psychische nood, eenzaamheid, schuldenproblematiek, opvoedingssituaties. Hun website is voor veel bezoekers het eerste contactmoment in een kwetsbare situatie. Een persoon die overweegt om hulp te zoeken bij Humanitas, is per definitie in een kwetsbare positie. Het minimum dat van die website mag worden verwacht is dat zo'n bezoek niet leidt tot commerciele profilering van de bezoeker.

BeforeYouMick scanner versie 3.7, modus refuse (klik op weigeren in de cookiebanner), schoon Fedora Linux, schone Firefox-instantie, geen vooraf bestaande cookies of profielen, scan op 9 mei 2026:

- 5 KRITIEK classificaties (tracking actief voor consent, of na refuse).
- 8 ERNSTIG classificaties (commerciele trackers actief).
- 18 trackers uniek geidentificeerd.
- 6 POST-requests naar advertentie-eindpunten na het klikken op weigeren.
- 12 derde-partij bestanden geladen vanaf andere domeinen.
- Tracking-cookies met levensduur langer dan een jaar (vaak 399 dagen voor Google Analytics).

Deze specifieke casus is illustratief voor het bredere patroon. Niet omdat Humanitas uniek slecht presteert (zie de tabel in paragraaf 3.6: andere hulpverleningssites zijn vergelijkbaar of erger), maar omdat het concreet maakt wat compliance-theater betekent. De papierwerk is in orde. Het keurmerk hangt aan de muur. De DPIA staat in de la. Het verwerkersregister is bijgehouden. En tegelijk wordt iedere bezoeker die hulp zoekt bij Humanitas gevolgd door de zes POSTs naar advertentiepartners.

> *De Privacy Schending Coefficient (PSC, een interne formule beschreven in apart dossier) van humanitas.nl scoort 200, in categorie B (Concern), drie sterren op vijf. Vergelijking: autoriteitpersoonsgegevens.nl scoort PSC 2 (Sound, vijf sterren). centrumseksueelgeweld.nl scoort PSC 367 (Risk, twee sterren).*

4. De commerciele tracking-cirkel

Pijler 3 is de commerciele kant van het stelsel: een advertentiemodel dat draait op het volgen van lezers, op een schaal die het handhavingsbudget van de toezichthouder ver overstijgt. De grootste Nederlandse nieuwsuitgevers werken alle met consent-cookies waarvan de rechtmatigheid in civiele procedures is betwist; de cookie-handhaving op die uitgevers gebeurt in de praktijk niet door de Autoriteit Persoonsgegevens, maar door particuliere rechtszaken (zie hoofdstuk 6.2). Dit hoofdstuk werkt het mechanisme uit aan een gedocumenteerd geval.

Dat geval is DPG Media. Niet omdat DPG zich onderscheidt van de rest van de sector, het patroon is sectorbreed, maar omdat het hier het best op de openbare rol staat: drie civiele rechters deden er in veertien maanden een uitspraak over, een aparte AVG-boeteprocedure liep tot aan de Raad van State, en de financieringsstroom is via openbare EIB-stukken te volgen. DPG is in dit hoofdstuk dus de casus, niet het onderwerp. Het onderwerp is de cirkel zelf: publiek geld financiert mede de advertentie-infrastructuur, die infrastructuur genereert tracking-omzet, en het toezicht dat de praktijk zou moeten corrigeren is structureel onderbemand.

> *Het cashflow-diagram (figuur 4.1) maakt die cirkel concreet aan dit ene geval, langs vier knooppunten. De Europese Investeringsbank in Brussel verstrekte in 2022-2024 in totaal 220 miljoen euro. De uitgever realiseerde in 2025 een advertentie-omzet van 753 miljoen euro, deels via een eigen advertentie-platform op de Microsoft Xandr-adserver. De Autoriteit Persoonsgegevens in Den Haag heeft voor cookie-handhaving 500 duizend euro per jaar. De uitgeverskoepel NDP Nieuwsmedia en het incassovehikel OPR vormen de sectorale lobby-laag tussen markt en politiek, uitgewerkt in hoofdstuk 9.*

4.1 De schaal: de omzet van een enkele uitgever

DPG Media is het grootste private mediabedrijf van Nederland, met een Belgische moederholding. Tot het concern horen onder meer de Volkskrant, het Algemeen Dagblad, Trouw, NU.nl, Tweakers, Donald Duck, Qmusic, en sinds juli 2025 RTL Nederland (overname 1,1 miljard euro). De omvang is hier om een reden relevant: ze bepaalt de schaal waartegen het handhavingsbudget van de toezichthouder wordt afgezet.

Geconsolideerde DPG Media-cijfers over 2025, op basis van de jaarcijfers en publicaties van Marketing Report en MarketingTribune (maart 2026):

- Omzet (geconsolideerd): 2,0 miljard euro
- Advertentie-omzet: 753 miljoen euro
- EBITDA: 440 miljoen euro
- Nettowinst: 238 miljoen euro

Een precisering bij het advertentiecijfer. De 753 miljoen euro is de totale advertentie-omzet, print, radio, televisie en digitaal samen, en groeide in 2025 vooral door de overname van RTL Nederland; organisch bleef de advertentie-omzet vrijwel vlak. De digitale advertentie-omzet, het deel dat het meest direct met de tracking-praktijk samenhangt, is een deelverzameling van dit bedrag en wordt door DPG niet apart gepubliceerd. Waar dit dossier de verhouding tussen het cookie-handhavingsbudget en de advertentie-omzet noemt, is de vergelijking dus met de

totale advertentie-omzet van een enkele uitgever; de digitale deelomzet is lager, maar de orde van grootte van de verhouding blijft staan.

4.2 EIB-financiering 220 miljoen euro

De Europese Investeringsbank (EIB) heeft DPG Media in twee tranches in totaal 220 miljoen euro verstrekt. De timing en omstandigheden zijn relevant.

Datum	Bedrag	Doel volgens EIB
28 januari 2022	100 miljoen euro, 8 jaar looptijd	Digitalisering, deel van DPG-investeringsplan 244 miljoen euro voor BE en NL mediaplatforms
19 december 2024	120 miljoen euro, 8 jaar looptijd	Verdere digitalisering en innovatie, deel van DPG-investeringsplan 392 miljoen euro 2024-2026 (30 procent EIB-financiering). Verdeling: 69,6 miljoen euro Belgische activiteiten, 50,4 miljoen euro Nederlandse activiteiten
Totaal	**220 miljoen euro**	**—**

Vijftig miljoen euro van het totaal is volgens FTM-onderzoek (Mark Koster, mei 2025) specifiek toegekend voor Trusted Web, het tracking-platform van DPG zelf. EIB-vicevoorzitter Robert de Groot omschreef de financiering publiek als 'keurmerk' voor DPG.

De ironie van het Big Tech-frame

De officiele motivering van de EIB voor de DPG-leningen is het versterken van Europese mediabedrijven tegen de dominantie van Amerikaanse Big Tech-platforms (Google, Meta). Tegelijkertijd is de adserver waarop het gefinancierde Trusted Web functioneert eigendom van Microsoft (Xandr), een van de grootste Amerikaanse techbedrijven. De Europese subsidie wordt daarmee feitelijk gebruikt voor de uitbouw van een tracking-platform dat afhankelijk is van Amerikaanse infrastructuur en dat door Nederlandse rechters drie keer is veroordeeld voor wetsovertreding.

4.3 Trusted Web en de Xandr-adserver

Trusted Web is sinds 2020 het advertentie-platform van DPG Media. Het centrale stuk infrastructuur is de adserver Xandr, sinds 2022 in handen van Microsoft (overname AT&T).

Centrale cijfers Trusted Web:

- 138 advertentiepartners actief op NU.nl (eigen meting 2025), tegenover een claim van 104 op de website zelf.
- 114 partners op Trusted Web algemeen (Big Brother Award jury, Bits of Freedom 2024, plus FTM-publicaties).
- Plus 50 DPG-dochterbedrijven.
- Bewaartermijn bij sommige partners 12 jaar, expliciet door de BBA-jury 2024 als zodanig genoemd.
- Adserver: Microsoft Xandr, sinds 2022 (overname onder Microsoft Advertising).

4.4 Drie Xandr-vonnissen in 14 maanden

Tussen december 2023 en februari 2025 is Microsoft Ireland (handelend onder Xandr) door Nederlandse rechters drie keer veroordeeld voor het plaatsen van tracking-cookies zonder toestemming. Niet door de Autoriteit Persoonsgegevens, maar door civielrechtelijke procedures van twee privé-burgers en een advocaat.

Datum	Instantie	ECLI
5 december 2023	Hof Amsterdam	ECLI:NL:GHAMS:2023:2971
7 juni 2024	Rb Amsterdam	ECLI:NL:RBAMS:2024:3331
12 februari 2025	Rb Amsterdam (vzr)	ECLI:NL:RBAMS:2025:885

Eisers in alle drie de zaken: twee privé-burgers met advocaat mr. M.H.L. Hemmer (Rotterdam). Niet de Autoriteit Persoonsgegevens. Niet een collectieve actie. Twee burgers en een advocaat.

De technische bewijslast in de derde zaak werd geleverd door rapporten van M. Stoter (Collective Shift) op basis van HAR-bestanden van bezoeken aan 129 en 136 websites. Op 64 van 67 websites werden Microsoft MUID en MSPTC cookies geplaatst zonder toestemming. Op 43 van 46 websites Xandr-cookies zonder toestemming. Microsoft erkende zelf in de procedure dat ze cookies plaatsen voor de toestemmingscheck.

De rechter, rechtsoverweging 4.34 in ECLI:NL:RBAMS:2025:885

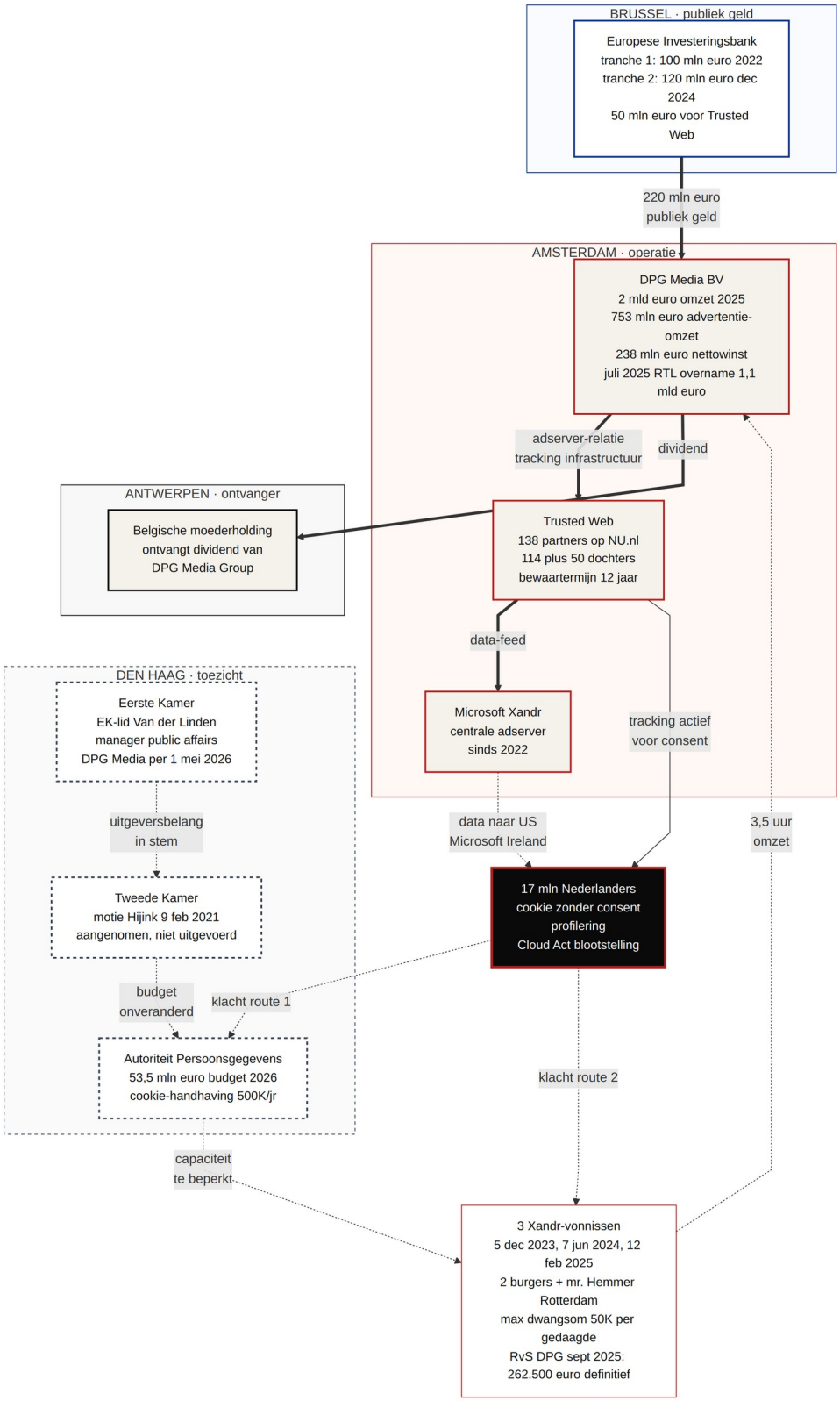
> *Het willens en wetens niet nakomen van de wettelijke toestemmingsverplichting (in de EU, althans Nederland) omdat nakoming, kort gezegd, het verdienmodel zou aantasten, is geen rechtens te beschermen belang.*

Maximale dwangsom: 50 duizend euro per gedaagde. Ter context: dat is ongeveer 5 minuten omzet voor Microsoft Ireland in Nederland. Yahoo en Criteo doen het wel correct, dus het kan technisch. Microsoft kiest expliciet voor non-compliance, wat in de procedure letterlijk werd erkend.

4.5 De sanctie als routine-kostenpost

Het stelsel kent ook directe sancties tegen uitgevers, maar die zijn op deze schaal bedrijfseconomisch verwaarloosbaar. Een voorbeeld: op 24 september 2025 bevestigde de Afdeling bestuursrechtspraak van de Raad van State een AVG-boete tegen DPG Media (ECLI:NL:RVS:2025:4562) wegens schending van artikel 12 — bij inzage- en verwijderverzoeken werd structureel een kopie van het identiteitsbewijs gevraagd, inclusief BSN, een onnodige drempel voor wie zijn privacyrechten wil uitoefenen.

De oorspronkelijke AP-boete van 525 duizend euro (februari 2022) werd in beroep gehalveerd tot 262.500 euro. Dat definitieve bedrag staat gelijk aan ongeveer 3,5 uur advertentie-omzet. Wat in een rechtsstaat een sanctie heet, is op deze schaal een routine-kostenpost, en dat is geen eigenschap van deze ene zaak maar van de verhouding tussen boetebedragen en sectoromzet.

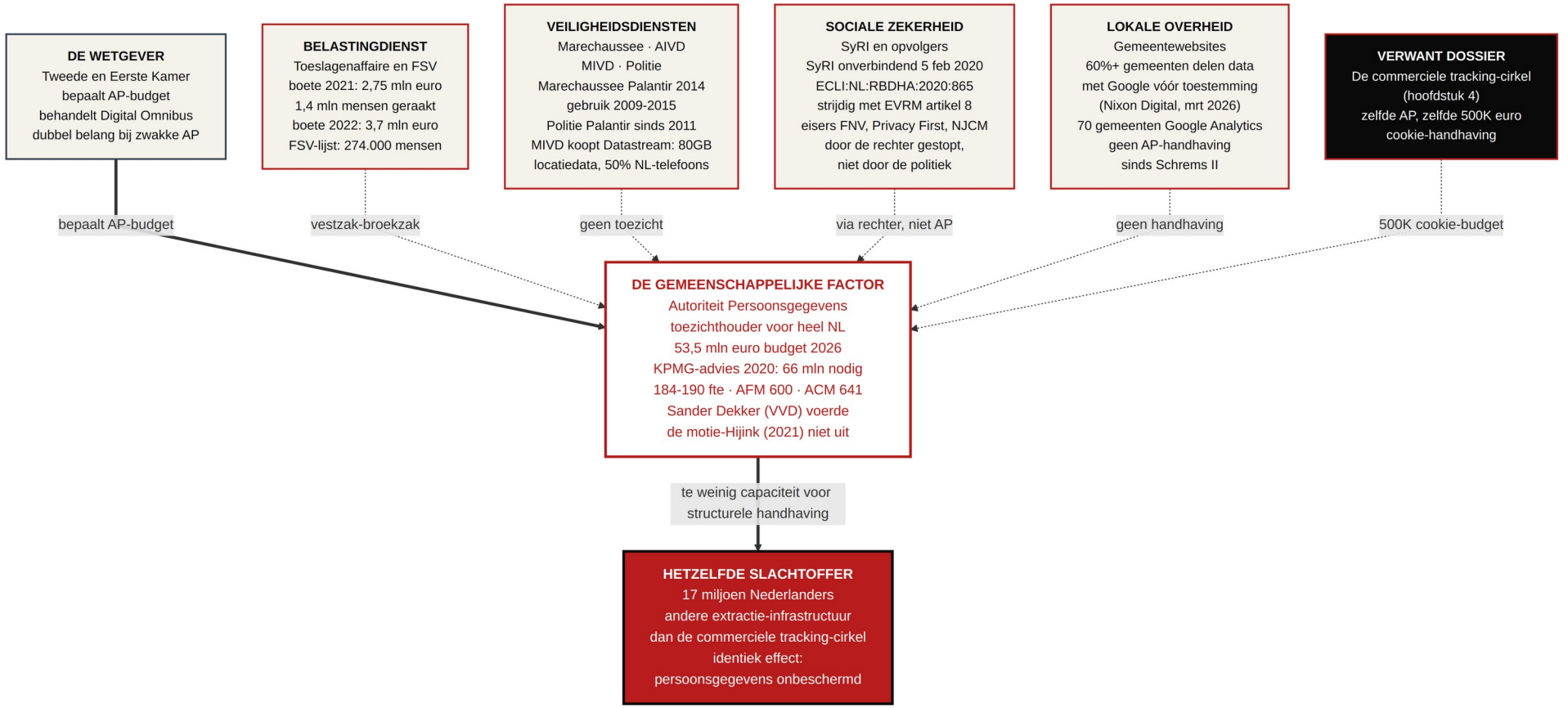


Figuur 4.1 De commerciele tracking-cirkel, concreet gemaakt aan een gedocumenteerd geval (DPG Media). Vier knooppunten in een gesloten cirkel: een EIB-lening van 220 miljoen euro (Brussel) financiert mede de uitgever (Amsterdam), die advertentie-omzet genereert via een tracking-platform op de Microsoft Xandr-adserver, terwijl cookie-handhaving onderbemand blijft (Den Haag). Bron: dit hoofddossier mei 2026.

5. De parallelle architectuur (overheid)

De commerciele tracking-cirkel uit het vorige hoofdstuk is een extractie-architectuur. Daarnaast bestaat een parallelle architectuur waarin Nederlandse overheidsorganen, uitvoeringsdiensten, gemeenten en commerciele partijen structureel de AVG schenden of risico-volle gegevensverwerking uitvoeren. Hier is geen advertentie-omzet de inzet. Toch is het patroon van niet-naleving even systematisch en even ongecontroleerd, en de gemeenschappelijke noemer is dezelfde.

De gemeenschappelijke factor is dezelfde uitgehongerde Autoriteit Persoonsgegevens. AP moet handhaven op de Belastingdienst, op inlichtingendiensten, op de Marechaussee, op gemeenten, op DPC, op alle private uitgevers, en op alle commerciele data-brokers. Met circa 187 fte en 500 duizend euro voor cookie-handhaving. Dat lukt niet.



Figuur 5.1 De parallelle architectuur. AP als gemeenschappelijke factor in vijf parallelle dossiers: Belastingdienst (toeslagenaffaire, FSV), Veiligheidsdiensten (Palantir Marechaussee, Politie, MIVD-Datastream), Sociale zekerheid (SyRI ECLI:NL:RBDHA:2020:865 plus opvolgers WGS, Wbsrz), Lokale overheid (60 procent gemeenten Google Analytics, Nixon Digital maart 2026). Verwant dossier: de commerciele tracking-cirkel, dezelfde 500K euro cookie-budget. Allen leiden naar dezelfde 17 miljoen Nederlanders.

5.1 Belastingdienst en boetes vestzak-broekzak

De Autoriteit Persoonsgegevens heeft de Belastingdienst tweemaal beboet. Beide boetes zijn betaald uit overheidskas naar overheidskas, een fenomeen dat in beleidstaal vestzak-broekzak heet.

Boete	Bedrag	Onderwerp
7 december 2021	2,75 miljoen euro	Discriminerende risicoprofielen kinderopvangtoeslag op basis van dubbele nationaliteit, periode 2014-2019. In mei 2018 stonden 1,4 miljoen mensen met dubbele nationaliteit geregistreerd in Belastingdienst-systemen. Drie afzonderlijke boetes voor drie afzonderlijke verwerkingen.
12 april 2022	3,7 miljoen euro	FSV (Fraude Signalering Voorziening) zwarte lijst sinds 2001, 274.000 mensen, 2.000 minderjarigen. Aanwijzingen om iemand op de lijst te plaatsen waren onder andere het hebben van een Turkse, Marokkaanse of Oost-Europese nationaliteit, of anonieme tips. AP constateerde zes overtredingen tegelijk.
Totaal	**6,45 miljoen euro**	**Beide betaald van overheidskas naar overheidskas**

> *Aleid Wolfsen, AP-voorzitter, 12 april 2022: 'De Belastingdienst is meerdere keren in de fout gegaan. Terwijl juist de Belastingdienst een zeer grote verantwoordelijkheid heeft tegenover de mensen in Nederland. Die zijn immers van de Belastingdienst afhankelijk. Je kunt niet besluiten om je toeslagen maar ergens anders aan te vragen of je belastingaangifte ergens anders te doen.'*

Het sanctiemechanisme heeft daarmee geen feitelijk effect op het schendende ministerie. Een private partij zou bij een vergelijkbare boete bedrijfsvoeringsmaatregelen moeten nemen om de boete te kunnen dragen. Een ministerie betaalt uit eigen begroting en daarmee uit hetzelfde rijksbudget waaruit de toezichthouder zou moeten worden gefinancierd. Het Centraal Justitieel Incassobureau int de boete; het geld komt vervolgens terug in dezelfde schatkist. Het bedrag wordt afgeschreven van het werkbudget van de Belastingdienst, maar gaat niet naar de gedupeerden van het toeslagenschandaal, niet naar de AP, en niet naar verbetering van privacy-infrastructuur.

Geen individuele ambtenaar of verantwoordelijke is voor deze AVG-overtredingen vervolgd. Geen minister is afgetreden specifiek omwille van de AVG-schendingen. De toeslagenaffaire leidde wel tot het aftreden van het kabinet-Rutte III in januari 2021, maar niet expliciet wegens het AVG-aspect.

5.2 De Marechaussee-Palantir-kwestie

Op 25 april 2026 publiceerde Follow the Money documenten die via een Woo-verzoek waren vrijgegeven, waaruit blijkt dat het Nederlandse ministerie van Justitie en Veiligheid in 2014 een contract sloot met het Amerikaanse bedrijf Palantir. De software werd ingezet door de Koninklijke Marechaussee voor het Advance Passenger Information-systeem op het API Centre in Soesterberg, in de periode 2009-2015. Daarmee worden vluchtgegevens van

inkomende vluchten van buiten Schengen (naam, geboortedatum, nationaliteit, geslacht, paspoortnummer) gescreend tegen watchlists en veiligheidsdatabases.

In augustus 2025 stelden Tweede Kamerleden expliciete vragen aan minister David van Weel (VVD, Justitie en Veiligheid) of er buiten de bekende voorbeelden andere onderdelen van JenV gebruik maakten van Palantir-software. De minister antwoordde ontkennend. Vrijgegeven Woo-documenten tonen aan dat zijn ministerie wel degelijk over het contract beschikte: een ambtenaar van de NCTV had op 24 juli 2025 het 'License and Service Agreement 2014.01.01 Netherlands Ministry of Security and Justice' gevonden en intern doorgemaild als bijlage. Het ministerie stelde tegenover FTM dat het organisatieonderdeel dat het contract sloot destijds niet onder de politieke verantwoordelijkheid van de minister van J&V viel; FTM weerspreekt dat verweer met verwijzing naar het dossier zelf. Van Weel informeerde de Kamer op 20 april 2026 alsnog over het Woo-besluit. Hij bleef in functie en is in kabinet-Jetten 2026 wederom minister J&V.

De omvang van het hoofdcontract is geheim, prijsinformatie weggelakt als 'bedrijfsgevoelig', strikte geheimhoudingsclausules zijn opgenomen. Een vrijgegeven offerte van een Nederlandse IT-reseller noemde 162.527,08 euro voor drie maanden huurlicenties van 'Elise en Palantir'. De Politie gebruikt Palantir-software sinds 2011 voor analytische doeleinden, ook in het diepste geheim, zoals in 2025 onthuld.

Geen CTIVD-onderzoek is aangekondigd. Geen openbare DPIA voor de Palantir-inzet. Geen aanbestedingsstukken over de oorspronkelijke contractsluiting publiek beschikbaar. Palantir is geen neutrale softwareleverancier: oprichter en CEO Alex Karp heeft in 2024 en 2025 publiek verklaringen afgelegd over zijn bedrijf die in de literatuur over civiele privacy uitvoerig zijn besproken. Palantir bouwt voor de Amerikaanse Immigration and Customs Enforcement (ICE) software waarmee ongedocumenteerden worden opgespoord en gedeporteerd.

5.3 MIVD en commerciele data-aankopen

In januari 2024 publiceerde BNR een onderzoek waaruit blijkt dat de MIVD commerciele locatiedata van Datastream koopt. 80 GB locatiedata, ongeveer 50 procent van Nederlandse telefoons, gekocht zonder formele tussenkomst.

Een Wob-equivalent verzoek over de inkoop bij commerciele data-brokers (Datastream, Babel Street, Venntel, Gravy, Factori, PenLink) blijft tot op heden onbeantwoord. AP heeft geen toezichtsmandaat over inlichtingendiensten, dat is bij CTIVD belegd. CTIVD heeft niet de capaciteit om dit op een structureel niveau te toetsen.

5.4 SyRI en de risico-systemen

Het System Risk Indication (SyRI) werd op 5 februari 2020 onverbindend verklaard door de rechtbank Den Haag in ECLI:NL:RBDHA:2020:865. Het systeem was strijdig met EVRM artikel 8 (privacy). Eisers: FNV, Privacy First, en Nederlandse Juristen Comite voor de Mensenrechten (NJCM).

Belangrijk in de geschiedschrijving: SyRI werd niet gestopt door politiek, maar door de rechter. De wetgever wilde door, de uitvoerende macht wilde door, alleen de rechtspraak heeft het gestopt. Opvolgende systemen (Pro Kind, BeBriefDecodes, Rapportage Risicoprofielen) zijn deels en niet altijd publiek geevalueerd.

5.5 Gemeentewebsites en Google Analytics

Onderzoek door Nixon Digital, gepubliceerd 17 maart 2026, op meer dan honderd Nederlandse gemeentewebsites. Bevindingen:

- 60 procent plus van Nederlandse gemeenten deelt data met Google voor consent.
- 70 gemeenten gebruiken Google Analytics voor toestemming gevraagd is.
- Plus Google Fonts en YouTube embeds zonder werkbare consent-laag.
- Geen AP-handhaving sinds Schrems II uitspraak juli 2020.

Nederlandse gemeenten leunen vrijwel allemaal op een handvol leveranciers: Nixon Digital schat ongeveer 60 procent van de Nederlandse gemeenten heeft een gemeenschappelijke leverancier. Een centrale beslissing op leveranciersniveau heeft zo direct effect op tientallen tot honderden gemeenten tegelijk.

Onder Schrems II (juli 2020) is doorgifte van persoonsgegevens naar Google (Verenigde Staten) zonder aanvullende technische maatregelen niet conform de AVG. Toch wordt deze configuratie niet gehandhaafd. AP heeft het sinds 2020 niet collectief aangepakt. Decentrale handhaving op individuele gemeente-niveau gebeurt soms, maar niet structureel.

6. Het toezicht-vacuum

De Autoriteit Persoonsgegevens is structureel onderbegroot. Dat is geen mening, dat is een rekensom. Tegelijk is dat onder-budgeten geen ongeluk maar het resultaat van politieke beslissingen die in dit hoofdstuk per stap worden uitgewerkt.

6.1 AP-capaciteit tegenover de KPMG-norm

In 2020 voerde KPMG in opdracht van het ministerie van Justitie en Veiligheid en op verzoek van de AP zelf een onderzoek uit naar de benodigde capaciteit van de Autoriteit Persoonsgegevens om effectief toezicht te kunnen houden in een digitale economie. Conclusie: 470 fte, ongeveer 66 miljoen euro per jaar, voor adequate handhaving op AVG-overtredingen, datalekken, en grensoverschrijdende verwerking. Op het moment van het KPMG-rapport had de AP 184 fte. KPMG vond dat de AP onmogelijk al haar wettelijke taken kon uitvoeren met de bestaande capaciteit.

Voor 2026 beschikt de AP over een budget van 53,5 miljoen euro, volgens de Rijksbegroting die op Prinsjesdag 2025 is gepresenteerd. Dat is ruim vier miljoen euro meer dan eerder voor 2026 was begroot, maar twee miljoen minder dan het budget voor 2025, en in de jaren na 2026 daalt het bedrag verder tot iets onder de 51 miljoen euro in 2030. De personele bezetting ligt bij benadering op 187 fte, tegenover de 470 fte die KPMG noodzakelijk achtte. Gemeten naar de KPMG-norm voor capaciteit zit de AP daarmee nog steeds onder de helft van het geadviseerde aantal medewerkers. De AP zelf becijferde in 2024 dat minimaal 100 miljoen euro per jaar nodig is om nieuwe affaires zoals de toeslagenaffaire te voorkomen en het toezicht op digitalisering en algoritmes aan te kunnen.

AP-bestuursvoorzitter Aleid Wolfsen sprak in interviews met Trouw destijds van 'lachwekkende achterstanden'. AP-bestuurslid Mur stelde dat slechts 0,3 procent van de gemelde datalekken leidt tot onderzoek.

Vergelijking met andere Nederlandse toezichthouders

De AP is met 184-190 fte het kleinste bestuursorgaan in zijn klasse, terwijl het toezichtveld (digitale economie, alle persoonsgegevensverwerking, plus recent AI-toezicht) verreweg het grootste is.

- Autoriteit Financiele Markten: 600 fte
- Autoriteit Consument en Markt: 641 fte
- Nederlandse Voedsel- en Warenautoriteit: 2.440 fte
- Autoriteit Persoonsgegevens: 184-190 fte

De budgettaire afhankelijkheid

Hoewel de AP een zelfstandig bestuursorgaan is, valt zij budgettair onder het ministerie van Justitie en Veiligheid. Dat ministerie is verantwoordelijk voor de jaarlijkse begrotingsallocatie. Het is dezelfde portefeuille die Sander Dekker bekleedde tot 2022, die David van Weel bekleedt sinds 2024 in het kabinet-Schoof en doorgeeft in kabinet-Jetten 2026, en waarvan de staatssecretaris (eerst Van Huffelen, nu Van Bruggen) verantwoordelijk is voor de uitvoering van de AVG.

Deze structurele afhankelijkheid betekent dat de toezichthouder die zou moeten controleren of het ministerie zelf, en de uitvoeringsdiensten onder dat ministerie, de AVG naleven, ressorteert onder dezelfde minister wiens diensten gecontroleerd moeten worden. Het is een rapportagestructuur die in de internationale literatuur over toezichthouder-onafhankelijkheid algemeen als problematisch wordt beschouwd.

Specifiek voor cookie- en online tracking-handhaving heeft AP een aparte tijdelijke regeling: 500 duizend euro extra per jaar voor 2024 tot en met 2026, daarna structureel 350 duizend euro per jaar (toezegging staatssecretaris Van Huffelen, niet aangepast door volgende kabinetten).

> *De cookie-handhavingscapaciteit van de Nederlandse staat is daarmee 500 duizend euro per jaar tegenover een advertentie-omzet van een enkele uitgever (DPG) van 753 miljoen euro. Een verhouding van 1 op 1500. Of anders gezegd: 35 minuten van die omzet is gelijk aan een jaar AP-cookie-budget.*

6.2 De niet-uitgevoerde motie-Hijink, februari 2021

Op 9 februari 2021 nam de Tweede Kamer een motie aan, op 3 februari ingediend door SP-Kamerlid Maarten Hijink, om het AP-budget te verhogen naar het door KPMG geadviseerde niveau. De motie (Kamerstuk 27529-240) werd aangenomen met een ruime Kamermeerderheid.

Demissionair minister Sander Dekker (VVD, Rechtsbescherming, kabinet-Rutte III) voerde de motie niet uit. In zijn brief aan de Tweede Kamer schreef hij dat het KPMG-onderzoek te veel onzekerheden bevatte om er een meerjarige capaciteitsraming aan te verbinden, en dat de motie niet was voorzien van financiele dekking. SP-indiener Michiel van Nispen noemde dit in AG Connect 'een schoffering van alle Nederlanders die verwachten dat hun persoonsgegevens goed beschermd worden'. De Miljoenennota 2022 hield het AP-budget ongewijzigd.

Dekker was als verantwoordelijk bewindspersoon degene die deze aangenomen motie niet uitvoerde. Daarmee bleef de bestaande lijn intact: het AP-budget groeit hooguit met inflatie, niet substantieel. Die lijn is sinds 2021 over vier opeenvolgende kabinetten voortgezet, zoals uitgewerkt in hoofdstuk 9. De vraag of dat een bewuste, gecoordineerde keuze is, wordt in dit dossier niet beantwoord; wel is het de meest constante factor in de begroting van de toezichthouder.

6.3 Cookie-handhavingsbudget 500 duizend euro per jaar

De cookie-handhaving wordt geregeld via Telecommunicatiewet artikel 11.7a en AVG artikel 7. Beide vallen sinds eind 2018 onder de competentie van de Autoriteit Persoonsgegevens (eerder bij ACM). Voor structurele handhaving op grote nieuwssites, e-commerce platforms, en commerciele data-brokers is de capaciteit te beperkt.

Resultaat: cookie-handhaving op de drie grootste Nederlandse uitgevers (DPG, Mediahuis, NRC) gebeurt niet door AP, maar door civiele procedures van privé-burgers. De drie Xandr-vonnissen (zie hoofdstuk 4.4) zijn daar het bekendste voorbeeld.

De Kruidvat-boete van ACM in juli 2024 (600 duizend euro voor schending Telecommunicatiewet 11.7a) is een uitzondering. Dat was nog onder ACM-bevoegdheid voor

specifieke aspecten van Tw 11.7a, niet onder AP-bevoegdheid voor de bredere AVG-aspecten.

6.4 De verhouding 1 op 1500

De volgende cijfers zetten de toezicht-capaciteit af tegen de commerciele schaal die ze zou moeten controleren. Als ijkpunt voor die schaal zijn de cijfers van een grote uitgever genomen, DPG Media, het gedocumenteerde geval uit hoofdstuk 4; de andere grote nieuwsuitgevers zijn in omvang vergelijkbaar.

Speler	Per jaar
Advertentie-omzet grote uitgever (DPG), 2025	**753 miljoen euro**
Nettowinst zelfde uitgever, 2025	**238 miljoen euro**
EBITDA zelfde uitgever, 2025	**440 miljoen euro**
NCSC (Nationaal Cyber Security Centrum) 2026	**55 miljoen euro**
Autoriteit Persoonsgegevens totaalbudget 2026	**53,5 miljoen euro**
AP cookie-handhaving specifiek (2024-2026)	**500 duizend euro**
Definitieve boete grote uitgever (RvS sept 2025)	**262.500 euro**
Maximum Xandr-dwangsom per gedaagde	**50.000 euro**

Wat hieruit volgt:

- De grootste recente boete tegen een uitgever (262.500 euro) staat gelijk aan ongeveer 3,5 uur van diens advertentie-omzet.
- De Xandr-dwangsom (50.000 euro) is 40 minuten Microsoft-omzet in Nederland.
- Het AP cookie-budget is 1 op 1500 van de advertentie-omzet van een enkele grote uitgever.
- De nettowinst van die ene uitgever over 2025 (238 miljoen euro) is ruim vier keer het totale jaarbudget van de Autoriteit Persoonsgegevens (53,5 miljoen euro).
- De EBITDA over 2025 (440 miljoen euro) is groter dan het AP-budget en het NCSC-budget samen.

7. Het keurmerken-stelsel

In Nederland mag op dit moment geen enkele certificatie-instelling AVG-certificaten uitgeven. Dat is geen interpretatie. Dat zeggen zowel de Raad voor Accreditatie als de Autoriteit Persoonsgegevens letterlijk op hun eigen websites.

> *Op dit moment zijn er in Nederland nog geen geaccrediteerde CI's voor het afgeven van AVG-certificaten in het kader van de verwerking van persoonsgegevens. Bron: rva.nl/nieuws/avg-certificatie.*
>
> *A certificate issued by a non-accredited organisation will not be considered a GDPR certificate. Bron: autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-in-practice/gdpr-certificate.*

Toch staan op honderden Nederlandse websites en in honderden aanbestedingsdocumenten claims als 'AVG gecertificeerd', 'Privacy Verified', 'ISO 27701 gecertificeerd', of 'GDPR compliant via Kiwa'. Volgens de toezichthouder zelf zijn al die claims juridisch geen AVG-certificaat.

7.1 Brand Compliance BC 5701 wacht op RvA-accreditatie

Brand Compliance is de eerste en enige Nederlandse certificatie-instelling waarvan de Autoriteit Persoonsgegevens de criteria heeft goedgekeurd onder AVG artikel 42 lid 5. Eerste goedkeuring oktober 2023 voor BC 5701:2023, gevolgd in december 2024 door BC EU 5701:2024 (door EDPB goedgekeurd voor de hele EER).

Maar Brand Compliance is per 10 mei 2026 nog niet door de Raad voor Accreditatie geaccrediteerd. Het accreditatietraject loopt. Tot die accreditatie afgerond is, mag Brand Compliance geen formele AVG-certificaten uitgeven, alleen ongeaccrediteerde certificering volgens accreditatierichtlijnen.

> *AP-eigen tekst: The AP has approved the Brand Compliance criteria (Certification Standard and Criteria BC 5701:2023). However, requesting a GDPR certificate from Brand Compliance is not yet possible. For this, Brand Compliance must first be accredited by the RvA.*

7.2 Privacy Verified, ICTRecht, en de moeder-dochter constructie

Privacy Verified is een initiatief van ICTRecht. Op iedere pagina van privacyverified.nl staat dit zelf vermeld. Audits voor Privacy Verified-certificering worden door ICTRecht uitgevoerd. Privacy Verified geeft het certificaat af. Beide entiteiten behoren tot dezelfde groep.

ICTRecht is zelf gecertificeerd door Privacy Verified op het hoogste niveau (Bedrijfscertificering Enterprise), sinds 18 december 2019, geldig tot 27 oktober 2026. De moeder organisatie certificeert zichzelf via haar dochter onderneming, op het hoogste niveau, op basis van haar eigen audits.

Status onder AVG artikel 42:

- Geen AP-goedkeuring voor de criteria. Niet op AP-lijst van goedgekeurde mechanismen.

- Geen RvA-accreditatie. Niet in RvA-register voor AVG-certificering.
- Privacy Verified is daarmee een commercieel keurmerk, geen juridisch erkend AVG-certificaat.

Het publieke register van Privacy Verified bevatte op 10 mei 2026 zeventien organisaties met geldig certificaat: XD Connects, DB Portalpro, Cobee, InWork, e-Flora, Broeders Gezondheidswinkel, Autotaalglas, Grassfeld, Kieskompas, Resono, Prowise, DeLaMar Theater, Onewave, ICTRecht, Hoplr, Vibe Group, Zivver. De marketing claim spreekt over 'meer dan 90 deelnemers'. Discrepantie.

Privacy Verified heeft zeven officiele Partners op de pagina /deelnemers: ICTRecht (de moeder), Fiber Carriers Association, Dutch Laravel Foundation, Dutch Cloud Community, Dutch Data Center Association, Thuiswinkel Waarborg, en Piwik PRO.

Drie ketens van Piwik PRO ten opzichte van Privacy Verified

Piwik PRO heeft drie tegelijklopende rollen ten opzichte van Privacy Verified, een opmerkelijke driedubbele rolverhouding.

- Partner. Vermelding op de pagina /deelnemers als een van zeven officiele partners.
- Klant. Privacy Verified-certificaat afgenomen. Op de cases-pagina van privacyverified.nl staat de Piwik PRO testimonial waarin Piwik PRO bevestigt dat ICTRecht audits uitvoert en Privacy Verified de certificaten geeft.
- Leverancier. Privacy Verified gebruikt Piwik PRO als web-analytics op haar eigen website. CNAME-cloaked hostname: privacyverifiednl.containers.piwik.pro. Piwik PRO container ID 74d5a6a5-4a3a-4a63-a1cf-bd77dfc87688. Geladen voorafgaand aan iedere consent. Geen cookie-banner aanwezig.

> *Drie rollen, dezelfde twee partijen, geen zichtbare scheiding. Plus: forensische bevinding op privacyverified.nl op 9 mei 2026 toont 8 externe trackers actief vanaf het eerste moment, zonder cookie banner. Een Privacy Verified-website die zelf niet voldoet aan basis-eisen voor cookie-consent.*

7.3 ISO 27701, NEN 7510, NOREA Privacy Audit Proof

De drie Nederlandse keurmerken die het meest in aanbestedingen worden gevraagd:

ISO/IEC 27701

Internationale norm voor Privacy Information Management System (PIMS). NEN-versie NEN-ISO/IEC 27701, met NEN als Nederlandse schemabeheerder. NEN 27701:2025 is recent vernieuwd, in transitiefase. Alleen certificeerbaar als add-on op ISO 27001 of NEN 7510. Door Kiwa, BSI, DNV, TUV NORD, Lloyd's Register, DigiTrust, DEKRA, Bureau Veritas uitgegeven. Niet AVG art 42 erkend. NEN zelf erkent dat het keurmerk 'bijdraagt aan de benodigde maatregelen voor het voldoen aan AVG', niet 'voldoet aan AVG'.

NEN 7510

Nederlandse vertaling van ISO 27001 specifiek voor zorgsector. Gebaseerd op ISO 27001 + ISO 27799. Verplichte norm voor zorginstellingen onder Regeling gebruik burgerservicenummer in de zorg. Door Kiwa (eerste in Nederland geaccrediteerd), DNV, BSI, DigiTrust uitgegeven. Voor zorginstellingen feitelijk verplicht. Toetst informatiebeveiliging in de zorg, geen AVG art 42 erkenning.

NOREA Privacy Audit Proof

Keurmerk gebaseerd op NOREA's eigen Privacy Control Framework (PCF). Wordt afgegeven door NOREA na een goedkeurend assurancerapport door geregistreerd IT-auditor. Sluit aan bij dertien kernelementen van AVG. NOREA had bij de totstandkoming overleg met AP, maar PCF is geen AVG art 42 erkend certificaat. Door grote accountantskantoren met IT-auditpraktijk uitgegeven.

Andere keurmerken op de Nederlandse markt

Daarnaast bestaan: Kiwa eigen AVG GDPR certificaat (door AP niet erkend, justitia.nl bevestigt expliciet), Bureau Veritas Technische Norm Bescherming Persoonsgegevens (accreditatie aangevraagd in 2018, niet afgerond), EuroPriSe (Duitse standaard, geen Nederlandse erkenning), ISO 27001 algemeen (informatiebeveiliging, niet AVG), BIO Baseline Informatiebeveiliging Overheid (sectoraal, niet AVG art 42).

7.4 Aanbestedingen vragen ISO 27001, niet AVG-certificering

Volgens DigiTrust beoordeling (digitrust.nl, januari 2026): 'ISO 27001 is not always mandatory but significantly increases procurement opportunities'. Aanbestedingen vragen drie soorten privacy- of informatiebeveiligingsbewijs:

- Categorie A, hard verplicht. Voor zorginstellingen NEN 7510. Voor rijksoverheidsleveranciers BIO. Beide informatiebeveiligingsnormen, niet AVG-certificering.
- Categorie B, regelmatig gevraagd. ISO 27001 als algemene benchmark. ISO 27701 als add-on bij specifiek privacy-relevante diensten.
- Categorie C, zachte aanwijzing. 'Een privacy keurmerk' zonder specificatie. 'Aantoonbaar AVG-compliant'. 'Privacy by design conform best practice'. Deze formuleringen geven leveranciers de ruimte om een willekeurig keurmerk uit deel 7.3 te overleggen, zonder dat de inkoper kan toetsen of dat keurmerk juridische AVG-betekenis heeft.

Geen Nederlandse overheidsaanbesteding voor zover openbaar nagaanbaar vraagt specifiek om Brand Compliance BC 5701, ondanks dat dit het enige keurmerk is met AP-goedkeuring criteria. Een aanbesteding die 'AVG art 42 erkend certificaat' zou eisen, zou per definitie geen aanbieder kunnen krijgen, omdat geen Nederlandse CI op dit moment AVG-certificaten uitgeeft.

7.5 De omvang van compliance-theater

De totale Nederlandse privacy- en informatiebeveiligings-certificeringsmarkt schat dit dossier op 50 tot 100 miljoen euro per jaar, verdeeld over vijf categorieen spelers.

- Certificatie-instellingen (CI's). Kiwa, Brand Compliance, DNV, BSI Group, TUV NORD, Lloyd's Register, DigiTrust, DEKRA, Bureau Veritas. Tarieven 15 duizend tot 60 duizend euro per audit voor middelgrote organisaties, 100 duizend euro plus voor grote.
- Schemabeheerders en norm-eigenaren. NEN voor NEN 7510, NCS 27701. ISO als internationale norm-eigenaar. NOREA voor Privacy Audit Proof. ICTRecht voor Privacy Verified.
- Adviesbureaus. Securesult, Promeetec, ICT Institute, CertificeringsAdvies Nederland, Nieuwhuis Consult, AVGdesk, ISO2HANDLE en tientallen andere. 25 duizend tot 150 duizend euro per implementatietraject.
- Auditors als individuen. Geregistreerde IT-auditors van NOREA. Lead auditors. Dagtarieven 1000 tot 1800 euro.
- ISMS- en PIMS-software-leveranciers. ISO2Handle, ICTRecht-software-tools. 5 duizend tot 50 duizend euro per jaar per organisatie.

> *Het ecosysteem is commercieel rendabel voor alle deelnemende partijen, en politiek geaccepteerd omdat de toezichthouder uitgehongerd is. Iedere speler heeft commercieel belang om de keurmerken-markt zo groot mogelijk te houden, geen speler heeft commercieel belang om te onderzoeken of keurmerken inhoudelijk doen wat de markt aanneemt.*

8. Cloud Act blootstelling

Naast het commerciele extractiepatroon (de tracking-cirkel, hoofdstuk 4) en het overheids-tracking patroon (parallelle architectuur, hoofdstuk 5) bestaat een derde laag van blootstelling: persoonsgegevens van Nederlandse burgers die juridisch toegankelijk zijn voor Amerikaanse autoriteiten via de Cloud Act, omdat 'Europese' of 'soevereine' Nederlandse softwareleveranciers feitelijk op Microsoft Azure, AWS of vergelijkbare US-cloud infrastructuur draaien.

8.1 Het juridische kader

De Amerikaanse Cloud Act

De Clarifying Lawful Overseas Use of Data Act (Cloud Act) is sinds 23 maart 2018 van toepassing in de VS. Amerikaanse opsporingsautoriteiten kunnen bij Amerikaanse cloud-dienstverleners gegevens vorderen die in een ander land zijn opgeslagen.

Cruciale vaststelling: de Cloud Act volgt de controle van de provider, niet de geografische locatie van de data. Een EU-Azure-regio biedt geen bescherming als Microsoft US technisch en juridisch toegang tot die data heeft.

> *ICTMagazine, 13 januari 2026: 'Een EU-Azure-regio biedt dus geen bescherming als Microsoft US technisch en juridisch toegang tot die data heeft. Locatie van EU-datacenters lost CLOUD Act-blootstelling voor Microsoft niet op.'*

AVG artikel 48 en Schrems II

AVG artikel 48 stelt dat afgifte van persoonsgegevens binnen de EU op grond van een buitenlandse rechterlijke uitspraak alleen is toegestaan indien dit gebaseerd is op een verdrag. Tussen EU en VS bestaat zo'n verdrag niet voor de Cloud Act. De VS heeft executive agreements met UK (sinds oktober 2022) en Australie (sinds december 2021), maar niet met de EU.

Op 16 juli 2020 verklaarde het Europees Hof van Justitie in de Schrems II-zaak (C-311/18) het Privacy Shield ongeldig als grondslag voor doorgifte naar de VS. Sindsdien zijn standaardcontractbepalingen (SCC's) onvoldoende voor doorgifte naar VS-verwerkers, tenzij aanvullende technische maatregelen worden genomen.

NCSC Nederland concludeerde in november 2022 dat het risico dat de Amerikaanse overheid toegang krijgt tot Europese persoonsgegevens op basis van Cloud Act 'voorstelbaar maar in de praktijk heel klein' is. Dat is een NCSC-inschatting voor 2022, geen wettelijke garantie. Onder een ander US-administratieklimaat kan die inschatting verschuiven.

8.2 Piwik PRO op Microsoft Azure of Elastx, niet Polen

Piwik PRO is een commercieel webanalyse-platform van Piwik PRO Sp. z o.o., gevestigd in Wroclaw (Polen, KRS 0000615871), sinds eind 2023 eigendom van het Deense family office Kirk Kapital.

Vendor-marketing: 'European-owned', 'GDPR-compliant', 'privacy-first analytics'. Werkelijke hosting-infrastructuur volgens vier onafhankelijke vendor-eigen bronnen:

Claim 8.2.1. Piwik PRO biedt geen eigen cloud-locatie in Polen aan. Alle Piwik PRO Cloud-installaties draaien op Microsoft Azure (60+ Azure-regio's wereldwijd) of op Elastx in Zweden.

> **Bron:** piwik.pro/blog/public-cloud-private-cloud-self-hosted/ — quote: 'With Piwik PRO, you can take advantage of over 60 Microsoft Azure locations, and Elastx in Sweden.'
>
> **Bron:** piwik.pro/glossary/cloud-hosting/ — quote: 'Public cloud: Piwik PRO also provides solutions on secure public cloud servers in 60+ Azure regions worldwide. European data centers: For organizations prioritizing data sovereignty, Piwik PRO offers cloud hosting solutions on European-owned servers, including Elastx in Sweden.'
>
> **Bron:** piwik.pro/privacy-security/ — quote: 'Our clients can choose between Azure cloud servers in the US, Germany, Hong Kong, the Netherlands, and Elastx in Sweden.'
>
> **Bron:** linkedin.com/company/piwik-pro/ — quote: 'Piwik PRO partners exclusively with ISO 27001-compliant data centers provided by AWS, Azure, Orange, and Elastx.'
>
> **Status:** Geverifieerd via vier onafhankelijke Piwik PRO eigen bronnen. ✓ hard bewezen openbaar.

Voor de Nederlandse rijksoverheid betekent dit dat statistiek.rijksoverheid.nl (CNAME naar rijksoverheid.piwik.pro), svb.piwik.pro, koop.piwik.pro en alle andere Piwik PRO instances voor 600 tot 800 overheidssites op Microsoft Azure draaien (Nederlandse Azure-regio is Microsoft Ireland Operations Limited, dochter Microsoft Corporation US) of op Elastx Zweden.

8.3 Bevestiging door ex-Piwik PRO Product Manager

Op 7 mei 2026 plaatste Antoni Bar (Senior Solution Engineer, ex-Product Manager Piwik PRO Wroclaw) een LinkedIn-comment onder een publicatie . Werkgeschiedenis publiek beschikbaar op LinkedIn:

- Anteriam (zelfstandig Data en Analytics Consultant), juni 2022 tot heden, Wroclaw
- Piwik PRO, juni 2022 tot december 2025, Wroclaw, drie functies achtereenvolgens: Web Implementation Specialist (juni 2022 tot juni 2023), Implementation Team QA en Process Lead (juni 2023 tot juni 2024), Product Manager (mei 2024 tot december 2025)

Letterlijke quote uit zijn comment, screenshot in dossier-archief beschikbaar:

> *Mick Beer what I can add here (note: as an ex-employee). AFAIK Piwik PRO doesn't offer a cloud location in Poland. Piwik PRO offers public or private cloud (like Azure or ElastX) deployment and has previously offered on-prem solutions. The rijksoverheid.piwik.pro domain (what's behind statistiek.rijksoverheid.nl) seems to be pointing to Netherlands. The privacy side of the configuration is handled by Piwik PRO users. Things like IP masking can be configured in the UI (to whatever octet level you want) but are not visible in the browser.*

Drie observaties uit deze ex-medewerker bevestiging:

- Geen Polen-cloud, alleen Azure of Elastx. Bevestiging vanuit insider-perspectief.
- Privacy-configuratie ligt bij de gebruiker (de Nederlandse rijksoverheid in dit geval), niet bij Piwik PRO. Het verschuift verantwoordelijkheid naar DPC, die geen openbare DPIA heeft gepubliceerd.

- IP masking is configureerbaar in de UI tot ieder octet-niveau, maar is niet zichtbaar in de browser. Dat betekent dat een externe onderzoeker, journalist of toezichthouder niet kan zien hoe streng de IP-anonymization is ingesteld. Alleen de Piwik PRO admin (DPC) weet dit.

8.4 Solvinity-Kyndryl-DigiD: kort geding 6 mei 2026

Solvinity beheert sinds 7 augustus 2020 het platform waarop DigiD draait. DigiD is van de Nederlandse overheid, beheerd door Logius (onderdeel ministerie BZK). Solvinity gebruikt Microsoft Azure als onderlaag voor PaaS-producten, expliciet erkend in antwoorden op Tweede Kamervragen door staatssecretaris Eric van der Burg (VVD).

Eind 2025 maakte Solvinity bekend dat aandeelhouders een overeenkomst hadden gesloten voor overname door Kyndryl Nederland B.V., dochter van het Amerikaanse Kyndryl. ACM keurde de overname goed op concurrentiegronden. Pieter van Oordt, Centrale Privacy Officer (CPO) van Logius, sloeg publiek alarm en spande een eigen kort geding aan tegen de Nederlandse staat. Hij baseerde zich op een interne veiligheidsanalyse van Logius. Volgens van Oordt kunnen de Verenigde Staten alle DigiD-gegevens inzien, maar ook DigiD uitzetten en informatieverzoeken indienen. Pieter van Oordt is na de affaire ontslagen.

Op 6 mei 2026 dienden drie anonieme burgers een tweede kort geding tegen de Nederlandse staat, vertegenwoordigd door advocaat mr. Rawaz Sharaf (Adelmeijer Hoyng Advocaten Maastricht). Argumentatie: persoonsgegevens komen na overname 'direct binnen bereik' van VS-autoriteiten, plus US heeft een 'kill switch' voor DigiD en MijnOverheid.

Diezelfde dag wees de Haagse rechter de vordering af in een kop-staartvonnis. Solvinity-contract wordt twee jaar verlengd. Motivering volgt binnen twee weken. Staatssecretaris Eric van der Burg (VVD) had op 27 maart 2026 al toestemming gegeven voor verlenging. Tijdens Kamerdebat van 21 april 2026 verzuimde hij dit te vermelden. Een motie van Kathmann, Stoffer (SGP) en Vermeer (BBB) om het contract niet te verlengen kreeg in april 2026 een meerderheid in de Tweede Kamer maar werd door het kabinet naast zich neergelegd.

Status overname Solvinity-Kyndryl per 10 mei 2026: nog onderzocht door het Bureau Toetsing Investeringen (BTI). De minister van Economische Zaken kan de overname theoretisch verbieden bij 'bedreiging van publiek belang'.

8.5 Microsoft Cloud for Sovereignty bij NCSC en gemeente Amsterdam

Microsoft heeft Cloud for Sovereignty gelanceerd, beschikbaar in alle 60+ Azure-regio's. NCSC-NL en de gemeente Amsterdam zijn als klanten van het eerste uur begonnen met migratie naar deze 'soevereine' cloud.

Maar Microsoft draait Cloud for Sovereignty zelf. De Nederlandse expert Atea-CEO Steinar Sonsteby noemt het in Techzine (16 december 2023) een 'wassen neus'. The Register heeft in de preview-fase aangegeven dat veel op de toezeggingen valt af te dingen.

Microsoft's eerdere poging tot soevereine oplossing (Microsoft Cloud Deutschland met T-Systems als datatrustee, 2016-2018) werd door Microsoft zelf gestaakt na invoering van de Cloud Act. Dat was een isolatie-opzet die functioneel veel beperkter was dan reguliere Azure, en commercieel niet houdbaar bleek.

Microsoft's EU Data Boundary beperkt waar data wordt opgeslagen, maar voorkomt geen toegang van de Amerikaanse overheid via juridische verzoeken aan het moederbedrijf.

8.6 Zivver bij ministeries en de Rechtspraak

Zivver is een Nederlandse e-mailbeveiligingsleverancier, gebruikt door meerdere Nederlandse ministeries, de Rechtspraak en kritische instellingen, voor versleutelde verzending van gevoelige communicatie inclusief informatie met staatsgeheim-classificatie G.

Zivver gebruikt Amazon Web Services (AWS) als hostingpartner, expliciet erkend op zivver.com/nl/blog/de-echte-risicos-van-de-amerikaanse-cloud (juni 2025).

Zivver mitigeert Cloud Act risico via zero-access encryption met BYOK (Bring Your Own Key). De klant beheert zelf de sleutels, AWS heeft geen toegang. Citaat Zivver: 'Zivver biedt volledige BYOK-encryptie en is daarmee niet gevoelig voor de CLOUD-Act.' Plausibel als BYOK technisch correct is geimplementeerd. Een onafhankelijke audit van die implementatie is niet openbaar.

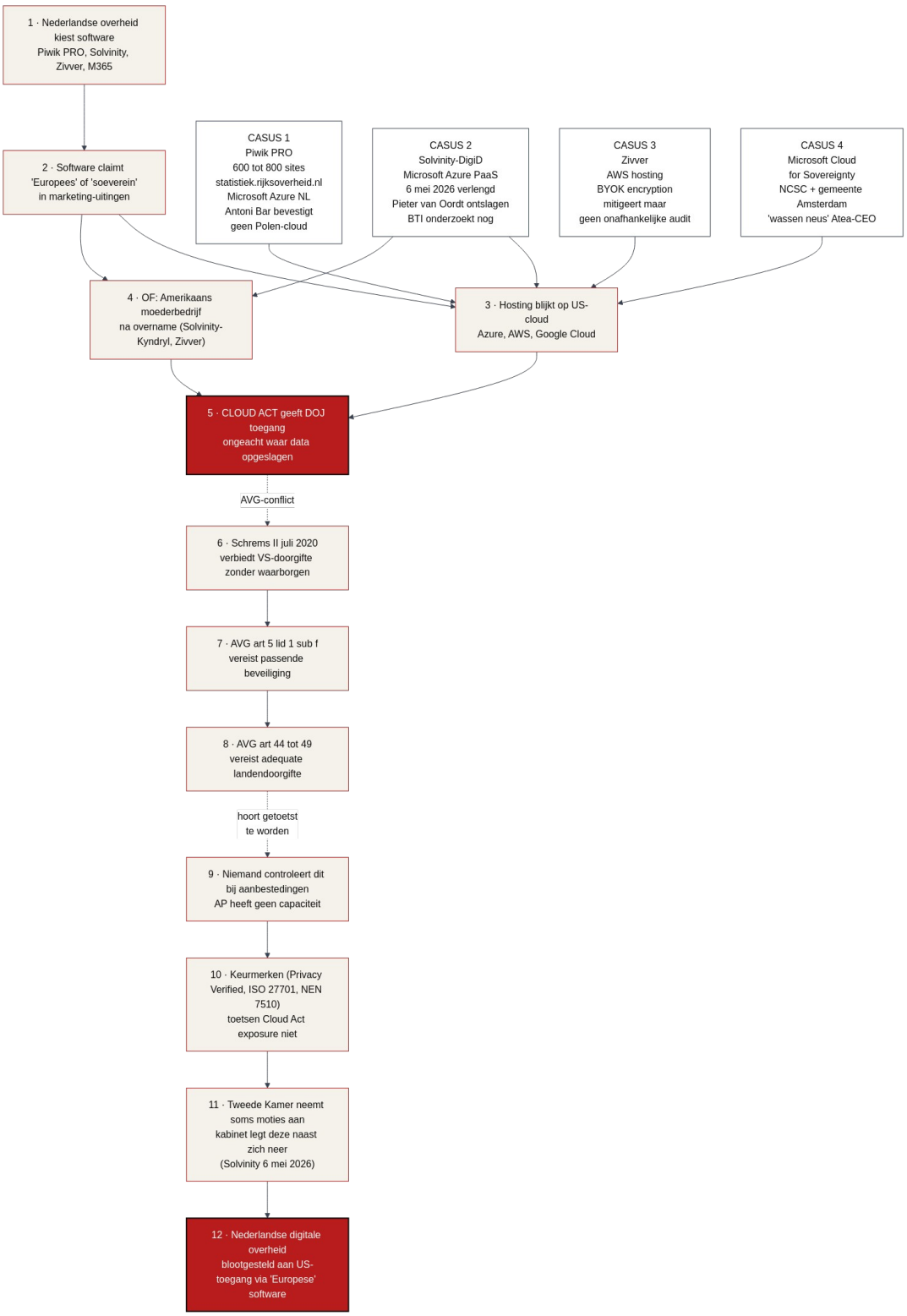
De overnames van Zivver en Solvinity hebben in het politieke debat over digitale autonomie en nationale veiligheid samen aandacht gekregen. Beiden zijn voorbeelden van Nederlandse softwareleveranciers waarvan de soevereiniteits-claim afhangt van de juridische status van eigendom en contractuele waarborgen, niet van fysieke locatie van data.

8.7 De Cloud Act cascade in beeld

Hoe de Cloud Act blootstelling werkt in de Nederlandse praktijk:

Stap 1. Nederlandse overheid kiest software (Piwik PRO, Solvinity, Zivver, M365)
Stap 2. Software claimt 'Europees' of 'soeverein' in marketing
Stap 3. Hosting blijkt op US-cloud (Azure, AWS) of via Amerikaans moederbedrijf
Stap 4. Cloud Act geeft DOJ toegang tot data, ongeacht waar opgeslagen
Stap 5. Nederlandse burgerdata is juridisch toegankelijk voor US-autoriteiten
Stap 6. AVG artikel 5 lid 1 sub f vereist passende beveiliging
Stap 7. AVG artikel 44 tot 49 vereist adequate landendoorgifte
Stap 8. Schrems II (juli 2020) verbiedt VS doorgifte zonder waarborgen
Stap 9. Maar: niemand controleert dit bij aanbestedingen, omdat AP geen capaciteit heeft
Stap 10. Keurmerken (Privacy Verified, ISO 27701, NEN 7510) toetsen Cloud Act exposure niet
Stap 11. De Tweede Kamer neemt soms moties aan, het kabinet legt deze naast zich neer (zie Solvinity 6 mei 2026)
Stap 12. Nederlandse overheid is zo blootgesteld aan US toegang via 'Europese' software

> *De Tweede Kamer-meerderheid voor de Solvinity-motie en de afwijzing van het kort geding op 6 mei 2026 toont dat het juridische kader inhoudelijk wel werkt (rechter past het toe), maar dat de uitvoerende macht (kabinet, AP, BTI) de uitkomst bepaalt. Solange dat zo blijft, is de Cloud Act-blootstelling van de Nederlandse digitale infrastructuur structureel.*



Figuur 8.1 Cloud Act cascade twaalf stappen. Vier instromende casussen: Piwik PRO (800 sites op Microsoft Azure NL, Antoni Bar bevestigt geen Polen-cloud), Solvinity-DigiD (overgenomen door Kyndryl 6 mei 2026, contract verlengd 2 jaar, Pieter van Oordt Logius CPO ontslagen), Zivver (AWS hosting, BYOK encryption, eindgebruikers maar geen sleutels), Microsoft Cloud for Sovereignty (NCSC plus gemeente Amsterdam, Atea-CEO Sønsteby noemde het 'wassen neus'). Eindpunt: 17 miljoen Nederlanders blootgesteld aan US-toegang via 'Europese' software.

INT. Internationale context

Het Nederlandse patroon staat niet op zichzelf. Vijf internationale en EU-wijde bevindingen plaatsen de Nederlandse situatie in een groter kader. Ze tonen aan dat het probleem niet typisch-Nederlands is, maar een Europese en deels mondiale dimensie heeft, en dat sommige juridische uitspraken die elders zijn gedaan ook van toepassing zijn op Nederlandse situaties zonder dat dit hier wordt afgedwongen.

INT.1 ICCL-rapport 2022, Johnny Ryan, RTB als grootste datalek

Het Irish Council for Civil Liberties (ICCL) heeft in 2022 vastgesteld dat de gemiddelde Europese internetgebruiker per dag 376 maal blootstaat aan Real-Time Bidding-veilingen waarin honderden tot duizenden bedrijven persoonlijk surfgedrag, locatie en interesses ontvangen. RTB werd in dat rapport getypeerd als 'het grootste datalek ter wereld'. Hoofdauteur: Johnny Ryan, voormalig Brave-medewerker en EU privacy-onderzoeker.

Voor de Nederlandse situatie heeft dit consequenties. De 138 advertentiepartners op NU.nl en de 23 GET-requests naar Google Ads op telegraaf.nl zijn instances van precies die RTB-keten. Iedere paginabezichtiging waarvan toestemming wordt gevraagd, voedt deze internationale veiling. Op DPG- en Mediahuis-titels samen zijn dat 2,6 tot 3,5 miljard paginabezichtigingen per jaar (eigen opgave van uitgevers).

INT.2 KU Leuven USENIX Security 2026, Meta en Yandex localhost-poorten

Onderzoekers Vlummens, Girish en collega's van de KU Leuven publiceerden op de USENIX Security-conferentie van 2026 het bewijs dat Meta en Yandex acht jaar lang via het localhost-poortenmechanisme actief meeluisterden met mobiele browsers wereldwijd. De techniek omzeilde browser-zandbakken via niet-gedocumenteerde communicatiekanalen tussen webpagina's en native apps op hetzelfde toestel.

Deze praktijk werd door beide bedrijven beeindigd op 3 juni 2025, kort na publicatie van de pre-print door de KU Leuven-onderzoekers. Geen van beide ondernemingen heeft hierover publiek verantwoording afgelegd of administratieve sanctie opgelopen. Geen Europese toezichthouder heeft een handhavingstraject ingesteld.

De onderzoekers zelf zijn aanverwant aan dit dossier: KU Leuven publiceerde eerder over Meta en Yandex tracking-praktijken die direct van toepassing zijn op de Nederlandse advertentie-infrastructuur. Het USENIX-paper is openbaar via usenix.org/conference/usenixsecurity26.

INT.3 Hof van Justitie EU, C-604/22, IAB Europe TCF onwettig

Het Hof van Justitie van de Europese Unie heeft in maart 2024 in zaak C-604/22 vastgesteld dat het IAB Europe Transparency en Consent Framework (TCF), het standaard cookie-toestemmingsmechanisme dat door vrijwel alle Nederlandse nieuwssites wordt gebruikt, in

zijn huidige vorm onwettig is. De TC-string die het framework genereert kwalificeert als persoonsgegeven en het IAB Europe als verwerkingsverantwoordelijke.

Sinds dit arrest is geen Nederlandse handhavingsactie tegen TCF-gebruikers ingesteld. Volkskrant, NRC, Telegraaf, NU.nl, en honderden Nederlandse e-commerce sites gebruiken TCF op het moment van creatie van dit dossier. AP heeft geen capaciteit voor structurele toetsing van iedere TCF-implementatie.

> *De rechtsregel is duidelijk, de capaciteit voor handhaving ontbreekt. Een AP met circa 187 fte kan niet structureel toetsen of honderden Nederlandse uitgevers een TCF-versie gebruiken die voldoet aan de C-604/22-criteria.*

INT.4 BNR en Secura januari 2024, Datastream toont Frederikkazerne

Nederlandse beveiligingsonderzoekers Pols en Moonen, in samenwerking met Secura en BNR, kochten in januari 2024 voor 2.000 dollar per maand 80 gigabyte aan Nederlandse locatiedata via de databroker Datarade van leverancier Datastream. De dataset bevatte traces van 50 procent van Nederlandse mobiele telefoons.

Tussen de gebufferde locatie-traces zaten registraties uit de Frederikkazerne, het hoofdkantoor van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) zelf. Dat betekent dat MIVD-personeel en bezoekers van de MIVD via commercieel beschikbare locatiedata identificeerbaar en volgbaar zijn voor 2.000 dollar per maand.

Of de MIVD zelf actief commerciele locatiedata aankoopt is publiek niet bevestigd of ontkend. Wel is internationaal gedocumenteerd dat het Amerikaanse bedrijf Babel Street locatiedata levert aan FBI (27 miljoen dollar contract 2022), ICE (3,6 miljoen dollar) en US Secret Service (600 duizend dollar). Vergelijkbare commerciele kanalen zouden Nederlandse data via een ondoorzichtige keten naar Nederlandse inlichtingendiensten kunnen brengen, zonder rechterlijke toetsing en zonder CTIVD-toezicht.

INT.5 Atlas Privacy v Babel Street, oktober 2024, Locate X

De rechtszaak Atlas Privacy versus Babel Street in het US District Court Eastern District of Virginia (oktober 2024) heeft het Locate X-product van Babel Street uitvoerig gedocumenteerd via deposities en bewijsstukken. Voorbeelden uit het procesdossier:

- 8.000 unieke devices getraceerd in en rond een synagoge in Los Angeles
- Trace van een individu vanaf een moskee in Dearborn (Michigan) naar diens woonadres
- Trace van vrouwen die een abortuskliniek in Alabama bezochten naar Florida (post-Dobbs context)
- Trace van een New Jersey-jurylid tot in diens slaapkamer

Klanten van Babel Street, gepubliceerd via FOIA-verzoeken: FBI met 27 miljoen dollar contract in 2022, ICE met 3,6 miljoen dollar, US Secret Service met 600 duizend dollar.

De databrokers waaraan Nederlandse advertentiepartners verkopen (138 partners op NU.nl, 114 in Trusted Web) zijn dezelfde partijen, of leveren door aan dezelfde partijen, die wereldwijd surveillance-data verkopen aan inlichtingendiensten en commerciele klanten. De Nederlandse cookie-toestemming van een individuele burger is daarmee feitelijk een toestemming voor doorverkoop in een ondoorzichtige internationale dataketen, niet voor een identificeerbare advertentietransactie.

INT.6 De koppeling met Nederland

Vier internationale dossiers tonen samen dat de Nederlandse situatie geen losstaand fenomeen is:

- De RTB-veiling-architectuur waar 138 NU.nl-partners op draaien is wereldwijd gekarakteriseerd als grootste datalek ter wereld.
- Tracking-technieken (zoals Meta-Yandex localhost-poorten) worden door grote spelers ongestraft jarenlang ingezet.
- De juridische basis voor handhaving (HvJ EU C-604/22, TCF onwettig) is aanwezig maar wordt in Nederland niet afgedwongen.
- De commerciele data-keten waaraan Nederlandse uitgevers leveren is verbonden met databrokers die surveillance-tools verkopen aan Amerikaanse opsporings- en inlichtingendiensten.

Wat betekent dit voor de Nederlandse situatie. De cookie-toestemming op nu.nl is niet alleen een Nederlands privacy-vraagstuk. Het is een instap in een internationaal data-ecosysteem waar Nederlandse burgers via hun advertentiepartner-keten uiteindelijk identificeerbaar zijn voor diensten waar zij geen toestemming voor hebben gegeven en waar hun nationale toezichthouder geen jurisdictie over heeft.

9. De politieke lobbylaag

Het toezichts-vacuum (hoofdstuk 6) is geen toeval. Het is het resultaat van een lobbylaag die actief inwerkt op de wetgever om interventie tegen de tracking-praktijk politiek onaantrekkelijk te maken. Vier instrumenten plus een doorlopende personele lijn binnen een politieke partij vormen samen die laag.

9.1 NDP Nieuwsmedia, Marjolein van der Linden 22 jaar vice-voorzitter

Nederlandse Dagbladpers (NDP) Nieuwsmedia is de brancheorganisatie van Nederlandse uitgevers, met onder meer DPG, Mediahuis en NRC als leden. Marjolein van der Linden is sinds 2003 vice-voorzitter, een ononderbroken termijn van 22 jaar. Geen andere persoon in de Nederlandse uitgeverswereld bezit die continuiteit op brancheniveau.

Per 10 mei 2026 heeft Marjolein van der Linden negen gelijktijdige functies en posities, voor zover openbaar uit handelsregister, parlementaire register en nevenfunctie-meldingen:

- Eerste Kamerlid voor de VVD, beedigd 14 januari 2025
- Manager public affairs en stakeholders DPG Media: feitelijk vanaf 1 december 2025, formeel volgens registerwijziging vanaf 1 mei 2026
- Vice-voorzitter NDP Nieuwsmedia, sinds 2003 (ononderbroken 22 jaar)
- Bestuurslid OPR (Stichting Organisatie voor Persuitgeversrecht), de collectieve beheersorganisatie die op 14 april 2025 de geheime raamovereenkomst met Google sloot over Extended News Previews
- Voorzitter Stichting Collectieve Gelden Omroepen (SCGO)
- Bestuur NLZIET (Nederlandse streamingdienst van publieke omroepen plus uitgevers)
- Bestuur Vereniging Commerciele Omroepen (VCO)
- Lid Supervisory Board Center Parcs Europe B.V., sinds 1 april 2026
- Lid Interparlementaire Commissie van de Taalunie, sinds 25 november 2025

Daarvoor: COO van RTL Nederland (mei 2023 tot 1 december 2025)

Voorafgaand aan haar overstap naar DPG was Van der Linden van mei 2023 tot 1 december 2025 Chief Operating Officer en vice-voorzitter Raad van Bestuur van RTL Nederland. RTL Nederland is in juli 2025 voor 1,1 miljard euro overgenomen door DPG Media. De overstap van Van der Linden van COO RTL naar Manager public affairs DPG (van een overgenomen bedrijf naar het overnemende moederbedrijf) is daarmee een interne transitie binnen het DPG-conglomeraat.

De vier-maanden compliance-meldingstermijn

De overstap van Van der Linden van RTL naar DPG werd niet gemeld in het functieregister van de Eerste Kamer ten tijde van de feitelijke aanvang op 1 december 2025. De wijziging in het register werd pas in april 2026 doorgevoerd, vier maanden na het feit, nadat het weblog

GeenStijl publiek vragen had gesteld. Van der Linden heeft de overgangssituatie zelf erkend in april 2026:

> *'Ik realiseer me door uw vragen dat deze overgangssituatie vragen kan oproepen.' — Marjolein van der Linden, april 2026.*

Haar formele compliance-mitigatie luidt dat zij geen lid is van de Eerste Kamer-commissie OCW (Onderwijs, Cultuur en Media) en daarom geen wetten behandelt die haar hoofdfunctie raken. Deze mitigatie is procedureel correct maar inhoudelijk onvoldoende voor het privacy-dossier. AVG-aanpassingen, cookie-handhaving via de Telecommunicatiewet en de Digital Omnibus worden in de Eerste Kamer behandeld door de gecombineerde commissies Justitie en Veiligheid en Digitalisering, niet door OCW. Beide vallen binnen het stemrecht van Van der Linden.

Drie van haar negen functies (NDP, OPR, SCGO) raken direct het regulatoire dossier waar AP toezicht zou moeten houden. Eerste Kamerlid (1) plus DPG-payroll (2) is een combinatie waarin een werkgever en een wetgever in een persoon samenkomen op een dossier dat haar werkgever direct aangaat.

9.2 OPR en de Google-deal van 14 april 2025

Online Publishers Rights (OPR) is een collectief incassovehikel van Nederlandse uitgevers, opgezet om compensatie te claimen van techbedrijven (Google, Meta) voor het tonen van uitgevers-content op hun platforms. Op 14 april 2025 sloot OPR een deal met Google waarvan de inhoud niet openbaar is gemaakt.

Wat publiek is: de deal bestaat. Wat niet publiek is: het bedrag, de looptijd, de tegenprestatie van OPR namens haar leden, of er voorwaarden zijn over publicaties die uitgevers wel of niet over Google mogen schrijven. Geen pers-onderzoek heeft tot op heden de inhoud van de deal kunnen achterhalen.

Marjolein van der Linden is bestuurslid OPR. DPG Media is via OPR aangesloten. Het uitvoerende secretariaat van OPR loopt deels via NDP-personeel.

9.3 De brandbrief van 22 mediabedrijven, december 2025

In december 2025, voorafgaand aan de kabinetsformatie na de Tweede Kamerverkiezingen van oktober 2025, ondertekenden 22 mediabedrijven een brandbrief gericht aan informateur Sybrand Buma. Het initiatief lag bij Stichting Democratie en Media (SDM). De brief is gepubliceerd via Villamedia en NDP eigen kanalen.

Stichting Democratie en Media zelf 14,27 procent aandeelhouder DPG Media

Stichting Democratie en Media, de initiatiefnemer van de brandbrief, is met 14,27 procent zelf aandeelhouder van DPG Media. Dat is geen niet-gouvernementele watchdog die zich louter zorgen maakt over diversiteit van de pers, maar een partij met een direct financieel belang in de uitgeverssector waarvan de praktijken in dit dossier worden onderzocht.

Ondertekenaars en hun belang

De brandbrief werd ondertekend door 22 mediabedrijven. Onder de ondertekenaars: DPG Media (Erik Roddenhof, CEO), Mediahuis Nederland (Rien van Beemen), NRC Media (Stas),

NDP Nieuwsmedia (Herman Wolswinkel), RTL Nederland (Sven Sauve), Talpa Network (Brakel), FD Mediagroep (Van Wiechen), Follow the Money, ANP, NLPO, NOS, NPO, RPO, plus negen andere. Zowel commerciele uitgevers als publieke omroepen tekenden mee.

Belangrijkste verlangens uit de brief

- Versoepeling cookie-regels in de EU Digital Omnibus
- Beperking van handhaving op online tracking
- Behoud van advertentie-financieringsmodellen
- Uitstel van verdere AVG-verzwaringen

Alle wensen uit deze brief zijn gehonoreerd in het coalitieakkoord 'Aan de slag' van 30 januari 2026. Op 8 april 2026 stuurde staatssecretaris Claudia van Bruggen (D66, Justitie en Veiligheid) een non-paper naar Brussel met serieuze zorgen over Digital Omnibus, dat de richting van mediabedrijven volgt. Inhoudelijk zorgen vanuit privacy-perspectief over Digital Omnibus zijn er ook (zie Bits of Freedom, Privacy First, EDRi-publicaties), maar de brandbrief-positie kreeg de eerste plaats in de kabinetsstrategie.

9.4 Werkgever en wetgever in een persoon

Sinds 14 januari 2025 is Marjolein van der Linden Eerste Kamerlid voor de VVD. Haar nevenfuncties moeten op grond van het Reglement van Orde van de Eerste Kamer worden gemeld in het officiele register.

Per 1 mei 2026 staat zij formeel op de loonlijst van DPG Media als Manager public affairs. De aankondiging is door DPG Media zelf gemaakt op 1 december 2025. Dat betekent: een Eerste Kamerlid is feitelijk werknemer van een uitgever wier praktijken (cookies, dark patterns, drie Xandr-vonnissen) precies onder het AVG-toezicht vallen waarop AP geacht wordt te handhaven.

De Eerste Kamer behandelt naar verwachting in de tweede helft van 2026 of begin 2027 de Digital Omnibus, het EU-voorstel dat het beschermingsniveau van de AVG aanpast. Marjolein van der Linden zal in die behandeling stemmen. Tegen die tijd is zij vier maanden in dienst van DPG Media als Manager public affairs.

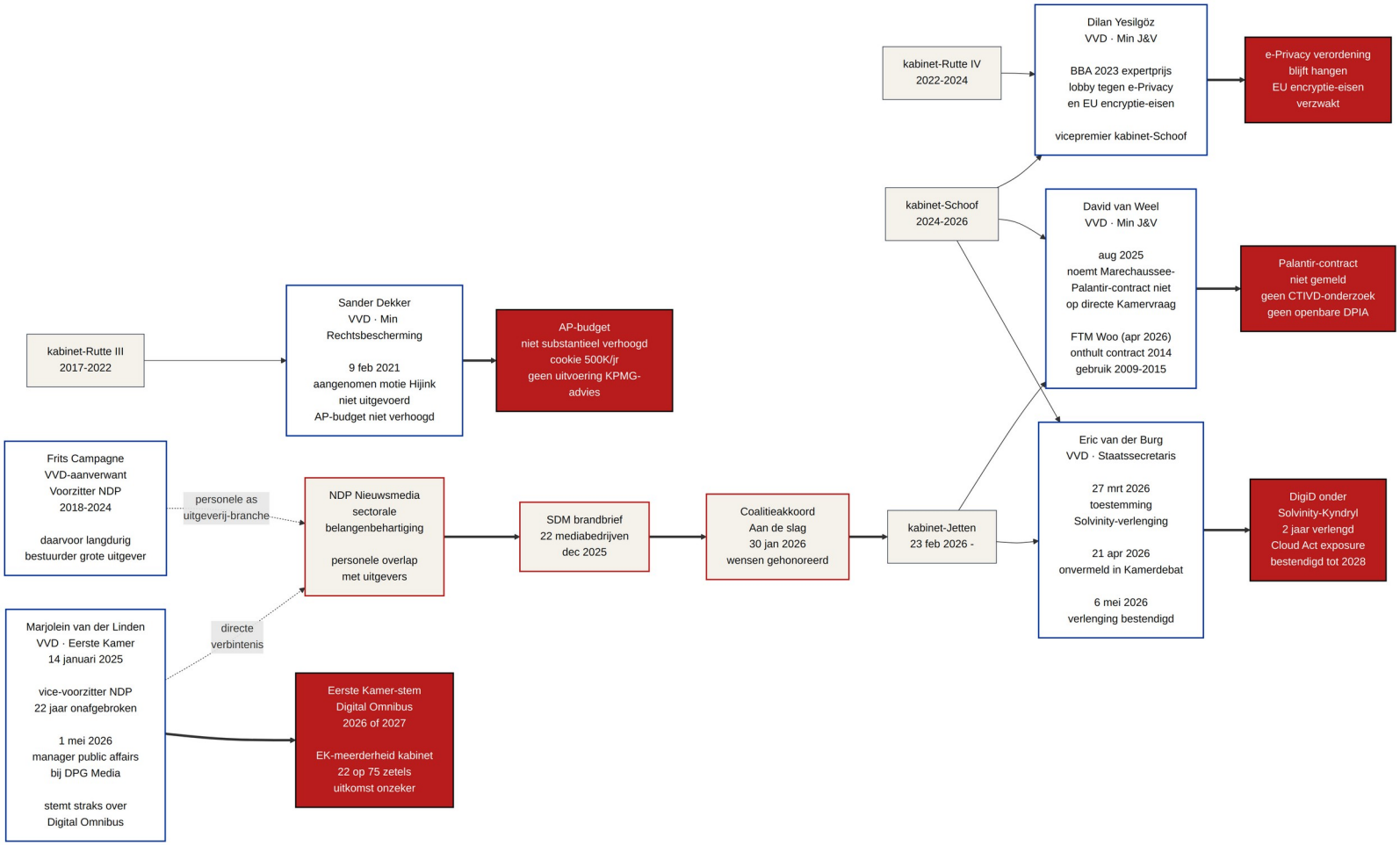
> *Geen Reglement van Orde-bepaling verbiedt deze combinatie. Geen wettelijk verbod op een sectorvertegenwoordiger op de werkvloer van zijn sector te zetten en tegelijkertijd in de Senaat over wetgeving voor die sector te laten stemmen. Het is institutioneel verwijtbaar, niet juridisch onrechtmatig. Dat is het patroon van het hele dossier in een kort geval.*

9.5 De personele lijn over vier kabinetten

De VVD heeft sinds 2010 vrijwel onafgebroken bewindslieden geleverd op de posities die het AP-budget en het privacy-toezicht mede bepalen (Justitie en Veiligheid, BZK, het premierschap). Een opsomming van direct verifieerbare personele lijnen:

Persoon	Positie	Specifieke handeling op privacy-dossier
Sander Dekker	Minister Rechtsbescherming, kabinet-Rutte III, 2017-2022	Voerde de aangenomen motie-Hijink (9 februari 2021) voor AP-budgetverhoging richting het KPMG-niveau niet uit
Dilan Yesilgöz	Minister Justitie en Veiligheid, kabinet-Rutte IV, 2022-2024	BBA 2023 (Big Brother Award expertprijs voor lobby tegen e-Privacy en EU encryptie-eisen). Vicepremier kabinet-Schoof 2024-2026
David van Weel	Minister Justitie en Veiligheid, kabinet-Schoof 2024-2026, kabinet-Jetten 2026-	Augustus 2025: Marechaussee-Palantir-contract niet genoemd in antwoord op een expliciete Tweede Kamervraag
Frits Campagne	Voorzitter NDP Nieuwsmedia, 2018-2024	Daarvoor langdurig bestuurder bij de grootste uitgever; illustreert de doorstroom tussen uitgeverij en brancheorganisatie
Marjolein van der Linden	Eerste Kamerlid VVD sinds 14 januari 2025	Vice-voorzitter NDP, sinds 1 mei 2026 manager public affairs DPG Media
Eric van der Burg	Staatssecretaris (VVD), kabinet-Jetten 2026 (Koninkrijksrelaties en Slagvaardige Overheid)	27 maart 2026 toestemming Solvinity-Kyndryl-DigiD verlenging, op 21 april 2026 Kamerdebat onvermeld gelaten

Deze personele lijn is opvallend consistent over vier kabinetten en zes bewindslieden en parlementaire posities. Dit dossier trekt daaruit niet de conclusie dat het om een bewust gecoordineerde strategie gaat: zoals hoofdstuk 9.7 laat zien is de begrotingskeuze rond de AP over de hele coalitiebreedte geaccepteerd, niet door een enkele partij afgedwongen. Wat wel feitelijk vaststaat is dat de VVD de meest constante factor is op de posities die het AP-budget bepalen, en dat die continuiteit samenvalt met een periode waarin het toezicht-vacuum onveranderd is gebleven. Dat is een patroon dat aandacht verdient, geen bewezen opzet.



Figuur 9.5 De personele lijn over vier kabinetten. Sander Dekker (kabinet-Rutte III, voerde aangenomen motie Hijink AP-budget 9 feb 2021 niet uit), Dilan Yesilgoz (kabinet-Rutte IV, BBA 2023 expert-prijs lobby tegen e-Privacy), David van Weel (kabinet-Schoof, informeerde Kamer onvolledig over Marechaussee-Palantir 2025), Eric van der Burg (kabinet-Jetten, gaf toestemming Solvinity-verlenging 27 mrt 2026), kabinet-Jetten zelf (D66+VVD+CDA, beedigd 23 feb 2026, coalitieakkoord honoreert SDM-brandbrief). Plus Marjolein van der Linden (Eerste Kamer VVD, vice-voorzitter NDP 22 jaar, manager public affairs DPG Media per 1 mei 2026, stemt over Digital Omnibus). Frits Campagne (VVD-aanverwant, voorzitter NDP 2018-2024, daarvoor langdurig bestuurder bij een grote uitgever).

9.6 Het 106-organisaties privacy-onderzoek mei 2026

Een derde scan-ronde, gepubliceerd 10 mei 2026 als 'Het Privacy Onderzoek' (vergelijkende test van Nederlandse organisaties, BeforeYouMick v3.7 en v3.8), geeft de aanvullende cijfers. 106 organisaties getest, sterren-verdeling over de hele scope:

- 5 sterren: 0 organisaties
- 4 sterren: 15 organisaties
- 3 sterren: 63 organisaties
- 2 sterren: 27 organisaties
- 1 ster: 1 organisatie (Privacy Lek)

Drie aanvullende killer-bevindingen:

- Hulplijnen voor kwetsbare bezoekers (zelfmoordpreventie 113, slachtofferhulp, kindertelefoon) gemiddelde score 2,4 sterren. Niet wat een bezoeker mag verwachten als hij in crisis een hulpsite raadpleegt.
- 69 op 106 organisaties (65 procent) laten meer dan de helft van hun trackers, of de hosting zelf, onder Amerikaans recht vallen (Cloud Act). Voor overheidssites geldt: persoonsgegevens zijn opvraagbaar voor Amerikaanse autoriteiten zonder Nederlandse rechter.
- 14 organisaties die zichzelf publiekelijk profileren als privacy-bewust, certificeerder of toezichthouder, scoren op de eigen meting 3 sterren of minder.

Acht organisaties blokkeerden de browsertest

Acht organisaties blokkeerden via firewall, bot-detectie of eindeloze redirect-cycle de browsertest. Daardoor konden voor deze partijen geen scores vastgesteld worden. Het feit van blokkade is op zichzelf signaalwaarde voor transparantie.

- solvinity.nl (DigiD-leverancier, hoofdstuk 8.4)
- mivd.nl (militaire inlichtingendienst, hoofdstuk 5.3)
- mind.nl (GGZ, voorheen mindkorrelatie)
- soa-aids.nl (variant op soaaids.nl, beide kwetsbare doelgroep)
- regenbooggroep.nl (LHBTI-hulpverlening)
- bsi-group.com (certificatie-instelling)
- lloydsregister.com (certificatie-instelling)
- fortinet.nl (security-leverancier)

> *Twee certificatie-instellingen blokkeren een privacy-test, een Nederlandse inlichtingendienst, een DigiD-leverancier, en drie hulpverleningssites. Dat is op zichzelf een datapunt over de*

> *transparantie-houding van deze organisaties. Een organisatie die niets te verbergen heeft, hoeft een browsertest niet te blokkeren.*

9.7 De budget-architectuur over vier kabinetten

De personele lijn van paragraaf 9.5 toont wie via welke functie het toezichtsvacuum mee bewaakte. De budget-architectuur in deze paragraaf toont hoe datzelfde vacuum kwantitatief is vormgegeven via de Rijksbegroting. Niet door één partij of één minister, maar door een patroon dat zich consequent herhaalt over Rutte III, Rutte IV, Schoof en Jetten.

De bewindslieden direct verantwoordelijk voor het AP-budget

Het budget van de Autoriteit Persoonsgegevens loopt via begrotingshoofdstuk VI (Ministerie van Justitie en Veiligheid). Politiek verantwoordelijk is de Minister voor Rechtsbescherming, sinds 23 februari 2026 vervangen door een staatssecretaris onder de Minister van Justitie en Veiligheid. De Minister van Financiën stelt het overkoepelende uitgavenkader vast.

Kabinet	Min Rechtsbescherming	Min Financiën	AP-budget en sleutelmoment
Rutte III 2017-2022	Sander Dekker VVD	Wopke Hoekstra CDA	Budget bevroren rond 25 miljoen euro in 2022 ondanks twee aangenomen Kamermoties voor verhoging. Dekker noemt het KPMG-rapport 'te onzeker' en verwijst het besluit naar een volgend kabinet. Wolfsen vroeg structureel 100 miljoen euro.
Rutte IV 2022-2024	Franc Weerwind D66	Sigrid Kaag (D66) Steven van Weyenberg (D66)	Coalitieakkoord-toekenningen en de nieuwe taak van algoritmetoezicht laten het budget in deze periode stijgen. De personele bezetting groeit veel beperkter en blijft ver onder het KPMG-advies van circa 66 miljoen euro en 470 fte.
Schoof 2024-2026	Teun Struycken PVV	Eelco Heinen VVD	Korte termijn. Geen significante budgetwijziging.

Kabinet	Min Rechtsbescherming	Min Financiën	AP-budget en sleutelmoment
			Heinen weigerde tegelijkertijd extra AFM-cryptotoezicht-middelen met als argument dat een overheidsbijdrage 'politiek niet haalbaar' was.
Jetten sinds 23 feb 2026	Claudia van Bruggen (staatssec) D66 onder Min J&V David van Weel (VVD)	Eelco Heinen VVD (gecontinueerd)	Geen aparte Minister voor Rechtsbescherming meer. Verlaging bestuurlijk gewicht voor de portefeuille. Coalitieakkoord 'Aan de slag' (30 januari 2026): defensie naar 3,5% bnp.

Eén constante in deze tabel: VVD heeft tussen 2017 en heden in alle vier kabinetten gezeten, en levert sinds juli 2024 onafgebroken de Minister van Financiën (Eelco Heinen, voortgezet van Schoof naar Jetten). D66 en CDA zaten in drie van de vier kabinetten. De Minister voor Rechtsbescherming wisselde tussen partijen, maar elke ambtshouder kreeg een uitgavenkader van de Minister van Financiën en het coalitieakkoord. De motie-Hijink van 9 februari 2021, aangenomen met ruime Kamermeerderheid voor AP-budget-verhoging in lijn met KPMG, werd door Dekker (VVD, Min RB Rutte III) niet uitgevoerd met verwijzing naar 'volgend kabinet'. Geen daaropvolgende coalitie heeft het KPMG-advies van ongeveer 66 miljoen euro overgenomen.

Het verloop van het AP-budget 2021-2026

Het AP-budget is sinds 2021 in absolute zin gegroeid, maar die groei valt weg tegen de uitbreiding van het takenpakket en blijft onder elke onafhankelijke norm. De ankerpunten, geverifieerd via de Miljoenennota:

- 2021: ongeveer 25 miljoen euro (Rutte III). Twee Kamermoties voor verhoging aangenomen, het kabinet voert ze niet uit.
- 2025: 55 miljoen euro. In de tussenliggende jaren kwam er budget bij, deels gekoppeld aan nieuwe wettelijke taken zoals het toezicht op algoritmes en, samen met de ACM, de Digital Services Act.
- 2026: 53,5 miljoen euro, volgens de Rijksbegroting die op Prinsjesdag 2025 is gepresenteerd. Dat is twee miljoen minder dan 2025. In de jaren daarna daalt het bedrag verder, tot iets onder de 51 miljoen euro in 2030.

De personele bezetting volgde die budgetgroei niet. In 2021 telde de AP 184 fte, in 2026 circa 187. KPMG adviseerde in opdracht van het kabinet zelf een groei naar 470 fte. AP-voorzitter Aleid Wolfsen becijferde de structurele behoefte op minimaal 100 miljoen euro per jaar. De kern is dus niet dat er niets bij kwam, maar dat wat erbij kwam onder elke norm bleef, samenviel met nieuwe taken, en volgens de Rijksbegroting na 2026 weer afneemt.

Vergelijking met andere toezichthouders

Drie sectorbrede toezichthouders bij het Rijk hebben vergelijkbare functies maar zeer verschillende budgetten en FTE-aantallen:

- AFM (financieel toezicht, ZBO onder Min Financiën): 783 fte 2024, begroting €141M; voor 2026 begroot op 918 fte en €175,5M. Reële groei 4,8% per jaar gemiddeld over 2013-2025.
- ACM (mededinging en consumenten, ZBO onder Min EZK): 641 fte, budget circa €88M.
- AP (gegevensbescherming, onder Min J&V): circa 187 fte, budget 53,5 miljoen euro in 2026 en volgens de Rijksbegroting dalend in de jaren daarna. Reële groei in personele bezetting sinds 2021: minimaal.

Met een budget van 53,5 miljoen euro voor 2026 en circa 187 fte ligt het budget per medewerker bij de AP niet structureel lager dan bij de andere toezichthouders. De anomalie van de AP zit niet in het budget per medewerker maar in het absolute aantal medewerkers. Er zijn ruwweg vier keer zoveel AFM'ers en ruim drie keer zoveel ACM'ers als AP'ers, voor functioneel vergelijkbare sectorbrede toezichtsfuncties. Het AVG-domein dekt iedere organisatie die persoonsgegevens verwerkt; in absolute termen een veelvoud van het AFM- of ACM-domein. Bovendien daalt het AP-budget volgens de Rijksbegroting na 2026 weer, terwijl de AFM-begroting in dezelfde periode juist stijgt.

Een citaat van het Ministerie van Financiën dat het patroon expliciet maakt: bij de discussie over AFM-cryptotoezicht in 2024 stelde het ministerie dat 'een overheidsbijdrage politiek niet haalbaar' was en zette daarop in op een 'minimale vorm van toezicht'. De AFM waarschuwde dat dit 'de ondergrens van goed uitvoerbaar toezicht' was. Hetzelfde argument-patroon dat sinds 2018 op de AP wordt toegepast.

Waar de prioriteit WEL ligt

Een aantal staatsuitgaven groeit in dezelfde periode (2022-2027) wel substantieel:

- Defensie: kabinet-Jetten coalitieakkoord verhoogt naar 3,5% bnp. Dit is een groei van naar schatting €11 tot €14 miljard per jaar bovenop het huidige defensiebudget. De NAVO-norm was 2%; bovenop dat bedrag komt nu het kabinet-Jetten-extra.
- Dienst Justitiële Inrichtingen (DJI, gevangeniswezen): begroting groeit van €2,8 miljard in 2022 naar €3,1 miljard in 2027. Dat is €60 miljoen extra per jaar gemiddeld.
- Politie: formatie groeit naar 52.591 fte in 2023 met vervolggroei in 2024-2025. Jaarlijkse extra-toekenningen €200-400 miljoen.
- IND en COA (asielketen): hoge incidentele uitgaven 2022-2024 (COA piek meer dan €3 miljard).

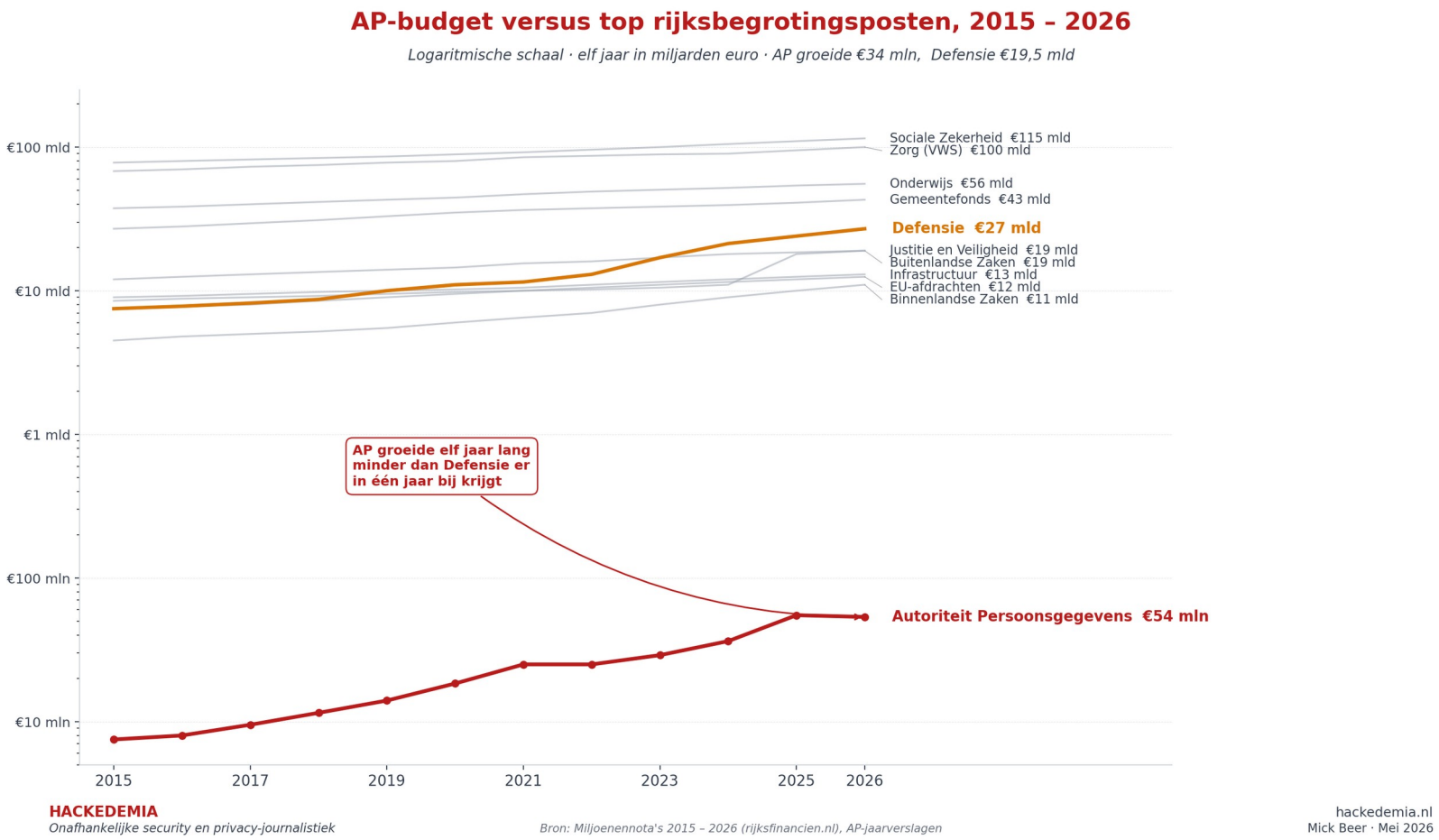
- Belastingdienst herstel toeslagenaffaire: structurele meerjarige uitgaven van miljarden, staatssecretaris voor Herstel Toeslagen (Sandra Palmen) blijft aan onder Jetten.

Plaatsing in perspectief: het AP-tekort tot het KPMG-advies is met het budget voor 2026 ongeveer 12 miljoen euro per jaar. Gemeten tegen de capaciteitsbehoefte die de AP zelf becijferde, minimaal 100 miljoen euro per jaar, loopt het tekort op tot ongeveer 46 miljoen euro per jaar. In beide gevallen is het bedrag een fractie van de jaarlijkse defensiegroei richting 3,5 procent bnp en valt het in het niet bij de Rijksbegroting als geheel. Dit is geen budgettair probleem maar een prioriteitskeuze.

Het patroon over elf jaar zichtbaar gemaakt

Het meest scherpe beeld komt door alle top-begrotingsposten over de afgelopen elf jaar (2015-2026) naast elkaar te zetten en de AP daar in te plaatsen. In absolute miljarden is de AP een lijntje dat onderaan de grafiek nauwelijks beweegt, terwijl Sociale Zekerheid, Zorg, Defensie, Onderwijs en het Gemeentefonds tientallen miljarden er bij hebben gekregen. Het verschil is zo groot dat een logaritmische schaal noodzakelijk is om de AP überhaupt zichtbaar te maken op dezelfde grafiek.

In absolute euro's: AP groeide tussen 2015 en 2026 met €34 miljoen. Sociale Zekerheid groeide in dezelfde elf jaar met €37 miljard, Zorg met €32 miljard, Defensie met €19,5 miljard. AP-groei is in elf jaar 0,18 procent van wat de Defensiebegroting in diezelfde periode er bij kreeg. Wie kijkt naar wat er aan capaciteit nodig was geweest om alle elementen van de AVG (sinds 25 mei 2018), de uitbreiding met algoritmetoezicht (sinds 1 januari 2023), de AI Act, de DSA en de DMA-uitvoering te dragen, ziet dat de toezichtorganisatie in elf jaar nooit de schaalsprong is gegund die haar takenpakket vereiste.



Figuur 9.7 — Budgettaire prioriteit over 11 jaar (2015-2026). Bovenste paneel: logaritmische schaal toont het AP-budget (rood) ten opzichte van de tien grootste rijksbegrotingsposten, waarbij defensie als snelste groeier in goud is gemarkeerd. Logaritmische schaal is nodig omdat het AP-budget op een lineaire schaal onzichtbaar onderaan staat. Onderste paneel: absolute groei per post tussen 2015 en 2026. Sociale Zekerheid kreeg er tientallen miljarden bij, Defensie ongeveer 19,5 miljard euro, terwijl het AP-budget in dezelfde periode met enkele tientallen miljoenen groeide, een verschil van drie ordes van grootte. Bronnen: Miljoenennota's 2015-2026 (rijksfinancien.nl), AP-jaarverslagen, AFM Agenda 2026, coalitieakkoord 'Aan de slag' kabinet-Jetten 30 januari 2026.

Conclusie van paragraaf 9.7

De Nederlandse rijksbegroting heeft over vier kabinetten consistent een keuze gemaakt: uitvoerende staatsmacht (defensie, politie, gevangeniswezen, asielketen, Belastingdienst-herstel) krijgt jaarlijks honderden miljoenen tot miljarden extra; burger-beschermings-toezicht (AP) groeit slechts marginaal en blijft 40 procent onder het KPMG-advies dat het kabinet zelf had laten opstellen. Eén partij zat in alle vier coalities (VVD), levert sinds 2024 onafgebroken de Minister van Financiën, en is daarmee qua zittingsduur op de cruciale ambten de meest constante factor in deze begrotingskeuze. Maar de keuze is ook door D66, CDA, ChristenUnie, BBB, NSC en PVV geaccepteerd via coalitieakkoorden. Geen aangenomen Kamermotie heeft het tot een afdwingbare verhoging gebracht. Dat maakt dit een breed gedragen prioriteitskeuze, niet een eenpartij-blokkade.

In samenhang met paragraaf 9.5 ontstaat hiermee een tweelaagse politieke architectuur: een personele lijn over vier kabinetten die het toezicht beleidsmatig laag houdt, en een budgettaire lijn over dezelfde vier kabinetten die de financiele capaciteit van het toezicht laag houdt. Lobbylaag en budgetlaag versterken elkaar.

10. Hefbomen en handelingsperspectief

Dit hoofdstuk somt de concrete hefbomen op waarmee partijen die het patroon willen doorbreken iets kunnen doen. Geen aansporing, geen oproep. Een opsomming voor wie nuttig wil zijn.

10.1 Voor de Autoriteit Persoonsgegevens

Vier opties die binnen het huidige mandaat en budget vallen:

- Een onderzoek opstarten naar misleidende claims onder AVG artikel 42 in keurmerken-marketing. Privacy Verified, Kiwa GDPR, Bureau Veritas TN BPG zijn alle drie te onderzoeken op de vraag of zij in marketing een wettelijk-erkende status suggereren die zij niet hebben.
- Een collectief handhavingstraject op cookies bij hulpverleningssites. Negen sites, AVG artikel 9 bijzondere persoonsgegevens, kwetsbare doelgroepen. Politiek minder controversieel dan handhaving op grote uitgevers, juridisch evenwaardige zaak, breed maatschappelijk draagvlak.
- Een actieve uitleg of bestendiging van de positie dat doorgifte naar US-cloud zonder aanvullende technische maatregelen onder Schrems II niet conform AVG is. Met expliciete benoeming van Microsoft Azure, AWS, Google Cloud.
- Een Woo-respons over Piwik PRO bij DPC, wat openbare DPIA's bestaan, welke aanbestedingen daaraan ten grondslag liggen.

10.2 Voor Tweede Kamerleden

Concrete vragen die nu gesteld kunnen worden, met directe wettelijke grondslag onder Reglement van Orde:

- Aan staatssecretaris Van Bruggen (D66, J&V): is er een plan om het AP-budget naar het door KPMG geadviseerde 66 miljoen euro te brengen? Zo nee, waarom niet, gegeven dat motie Hijink (Kamerstuk 27529-240) op 9 februari 2021 met een ruime Kamermeerderheid werd aangenomen?
- Aan minister Van Weel (VVD, J&V): de openbaarmaking via FTM en Woo van Marechaussee-Palantir contract sinds 2014 is in tegenspraak met uw eerdere antwoord aan de Kamer. Hoe verhoudt dit zich? Welke maatregelen?
- Aan staatssecretaris Van der Burg (VVD): is er sinds 27 maart 2026 een verschil ontstaan in uw inschatting van Cloud Act-blootstelling van DigiD via Solvinity? Hoe verhoudt zich uw besluit van 27 maart tot uw stilzwijgen daarover op 21 april in het Kamerdebat?
- Aan staatssecretaris Van Bruggen: een DPIA voor Piwik PRO bij DPC is sinds 13 jaar in gebruik op 600-800 rijksoverheidssites. Bestaat er een openbare DPIA? Bestaat er een Transfer Impact Assessment onder Schrems II? Bestaat er een aanbesteding waaruit blijkt dat Piwik PRO is geselecteerd?

10.3 Voor onderzoeksjournalistiek

Vijf concrete dossiers waarvan de bronnen volledig openbaar zijn en waaraan een onderzoeksredactie zelfstandig kan werken. Dit dossier brengt openbare bronnen samen, exclusief of geheim materiaal bevat het niet. Iedere journalist met internettoegang en een paar dagen tijd kan zelf naar de primaire bronnen toe.

- Het Privacy Verified moeder-dochter dossier. Bronnen openbaar via privacyverified.nl, ictrecht.nl, KvK-uittreksels, en het AP-register van goedgekeurde mechanismen. ICTRecht voert audits uit voor Privacy Verified-certificering. Privacy Verified geeft het certificaat af. Beide entiteiten behoren tot dezelfde groep. Drie ketens van Piwik PRO als partner-klant-leverancier.
- Het OPR-Google dossier. De deal van 14 april 2025 is feit, het bedrag en de redactionele afspraken zijn niet publiek. Een Woo-verzoek over OPR (als verband-onderdeel met publiekrechtelijke functie) of een onderzoek via NDP-jaarstukken kan licht op de inhoud werpen.
- Het EIB-financieringsdossier. 220 miljoen euro publiek geld, EIB-persberichten 28 januari 2022 en 19 december 2024. FTM-publicatie Mark Koster mei 2025 was de eerste investigation, kan worden uitgebreid met aanvullende Woo-verzoeken bij EIB en EU-Ombudsman.
- Het Solvinity-Kyndryl-DigiD dossier. 27 maart toestemming Van der Burg, 21 april dat besluit onvermeld in Kamerdebat, 6 mei kort geding-uitspraak. BTI-onderzoek loopt nog. Bronnen via Tweede Kamerstukken, AGConnect, iBestuur, Computable, Techzine. Vonnis-tekst volgt binnen twee weken na 6 mei 2026.
- Het Marechaussee-Palantir dossier. Volledig openbaar via FTM-publicatie van 25 april 2026. Woo-documenten zijn vrijgegeven, kunnen direct opgevraagd. NCTV-ambtenaar mailde op 24 juli 2025 het 'License and Service Agreement 2014.01.01 Netherlands Ministry of Security and Justice' intern door. Een onderzoeksjournalist kan zonder enige tussenkomst van Mick Beer naar de FTM-publicatie en de Woo-documenten toe.

Geen van deze vijf dossiers vereist toegang tot vertrouwelijk of niet-openbaar materiaal. Wat ontbreekt is niet bewijs, maar journalistieke capaciteit om de openbare bronnen samen te leggen tot een coherent beeld. Dit hoofddossier is een poging om die ene capaciteit-stap voor te zijn. De journalist neemt het over.

10.4 Civielrechtelijk model Xandr

De drie Xandr-vonnissen (5 december 2023, 7 juni 2024, 12 februari 2025, alle drie ECLI-nummers in hoofdstuk 4) bouwen civielrechtelijke jurisprudentie op tegen non-compliant cookies. Een burger met een advocaat in Rotterdam (mr. M.H.L. Hemmer is precedent-set) kan een vergelijkbare procedure starten tegen iedere Nederlandse uitgever. Maximum dwangsom 50.000 euro per gedaagde, niet symbolisch maar wel beperkt. De waarde zit in de jurisprudentie, niet in de directe sanctie.

10.5 Eerste Kamer-stem Digital Omnibus

De Eerste Kamer-behandeling van Digital Omnibus, naar verwachting tweede helft 2026 of begin 2027, is een politiek beslismoment. Het kabinet-Jetten heeft een minderheid (22 op 75 zetels: D66 9, VVD 9, CDA 4). Een meerderheid in de Eerste Kamer kan het kabinet dwingen tot een ander mandaat in Brussel.

11. Tijdlijn

Een chronologisch overzicht van de meest relevante data tussen 1987 en 10 mei 2026, met directe bron per gebeurtenis.

2003 Marjolein van der Linden start als vice-voorzitter NDP Nieuwsmedia.

Bron: ndpnieuwsmedia.nl

9 februari 2021 Tweede Kamer neemt motie Hijink (SP, ingediend 3 februari) aan met ruime Kamermeerderheid: AP-budget verhogen richting het KPMG-niveau. Demissionair minister Sander Dekker (VVD) weigert uitvoering.

Bron: tweedekamer.nl, Kamerstuk 27529-240

September 2021 Miljoenennota 2022 houdt AP-budget ongewijzigd.

Bron: rijksbegroting.nl

28 januari 2022 EIB verstrekt eerste tranche 100 miljoen euro aan DPG Media.

Bron: eib.org/en/press/news/2022/2022-029

Februari 2022 AP-boete DPG Media 525 duizend euro voor schending AVG art 12 (kopie identiteitsbewijs vragen).

Bron: autoriteitpersoonsgegevens.nl/actueel

2022 Microsoft koopt Xandr van AT&T. DPG begint met Microsoft Xandr als adserver voor Trusted Web.

Bron: news.microsoft.com

5 december 2023 Hof Amsterdam veroordeelt Microsoft Ireland (Xandr) voor cookies zonder toestemming.

Bron: uitspraken.rechtspraak.nl, ECLI:NL:GHAMS:2023:2971

Eind 2023 Piwik PRO Sp. z o.o. wordt overgenomen door Deense family office Kirk Kapital.

Bron: piwik.pro/about-us

Oktober 2023 AP keurt Brand Compliance BC 5701:2023 criteria goed. Eerste AP-goedgekeurd Nederlands keurmerk-criteria onder AVG art 42.

Bron: brand-compliance.com en autoriteitpersoonsgegevens.nl

Januari 2024 BNR-onderzoek: MIVD koopt commerciele locatiedata Datastream. 80 GB, ongeveer 50 procent van Nederlandse telefoons.

Bron: bnr.nl/podcast/cybercrime

Maart 2024 Hof van Justitie EU verklaart IAB Europe TCF onwettig in zaak C-604/22.

Bron: curia.europa.eu, C-604/22

7 juni 2024 Rechtbank Amsterdam veroordeelt Microsoft tweede keer.

Bron: uitspraken.rechtspraak.nl, ECLI:NL:RBAMS:2024:3331

April 2024 AP-boete Belastingdienst 3,7 miljoen euro voor FSV-zwarte lijst. Vestzak-broekzak betaling.

Bron: autoriteitpersoonsgegevens.nl/actueel

Oktober 2024 Atlas Privacy v Babel Street procesdossier publiek over Locate X. 8000 devices synagoge LA, abortuskliniek Alabama.

Bron: US District Court Eastern District Virginia

December 2024 EIB tweede tranche 120 miljoen euro aan DPG. Totaal 220 miljoen euro. Brand Compliance BC EU 5701:2024 door EDPB goedgekeurd voor hele EER.

Bron: eib.org/en/press en edpb.europa.eu

14 januari 2025 Marjolein van der Linden treedt aan als Eerste Kamerlid voor de VVD.

Bron: eerstekamer.nl/lid/marjolein_van_der_linden

12 februari 2025 Voorzieningenrechter Amsterdam veroordeelt Microsoft derde keer. R.o. 4.34: 'het willens en wetens niet nakomen van de wettelijke toestemmingsverplichting omdat nakoming het verdienmodel zou aantasten, is geen rechtens te beschermen belang.'

Bron: uitspraken.rechtspraak.nl, ECLI:NL:RBAMS:2025:885

14 april 2025 OPR sluit deal met Google over Extended News Previews. Bedrag en inhoud niet openbaar.

Bron: ftm.nl

Mei 2025 FTM (Mark Koster) publiceert onderzoek over de EIB-financiering van DPG. 50 miljoen euro EIB-financiering specifiek voor Trusted Web.

Bron: ftm.nl

3 juni 2025 Meta en Yandex stoppen met localhost-poorten praktijk na KU Leuven-publicatie. Geen sancties, geen publieke verantwoording.

Bron: usenix.org/conference/usenixsecurity26

Juli 2025 DPG neemt RTL Nederland over voor 1,1 miljard euro.

Bron: dpgmedia.nl

Augustus 2025 David van Weel (VVD, J&V) noemt het Marechaussee-Palantir-contract niet in antwoord op een directe Tweede Kamervraag.

Bron: tweedekamer.nl, Kamerstuk

24 september 2025 Raad van State definitieve uitspraak DPG: 262.500 euro. Boete Februari 2022 verlaagd van 525.000 euro.

Bron: uitspraken.rechtspraak.nl, ECLI:NL:RVS:2025:4562

1 december 2025 Marjolein van der Linden in dienst van DPG Media (formele indiensttreding pas 1 mei 2026, registerwijziging pas april 2026).

Bron: eerstekamer.nl/lid/marjolein_van_der_linden

December 2025 SDM-brandbrief van 22 mediabedrijven aan informateur Buma. SDM 14,27 procent aandeelhouder DPG Media.

Bron: sdm.nl en villamedia.nl

Eind 2025 Solvinity en Kyndryl maken aandeelhoudersovereenkomst over overname Solvinity. ACM-goedkeuring.

Bron: acm.nl

30 januari 2026 Coalitieakkoord 'Aan de slag' (D66, VVD, CDA) honoreert SDM-wensen vrijwel volledig.

Bron: kabinetsformatie2025.nl

23 februari 2026 Kabinet-Jetten beedigd. Premier Rob Jetten (D66), J&V David van Weel (VVD), staatssecretaris J&V Claudia van Bruggen (D66, AP-portefeuille), staatssecretaris Koninkrijksrelaties en Slagvaardige Overheid Eric van der Burg (VVD).

Bron: rijksoverheid.nl

Maart 2026 Mick Beer publiceert Medium-artikelen over cookie-onderzoek NU.nl, Volkskrant, Telegraaf. AP-melding 7cb0-9871 ingediend 24-25 maart.

Bron: medium.com/@mickbeer

17 maart 2026 Nixon Digital onderzoek: 60+ procent Nederlandse gemeentewebsites delen data met Google voor toestemming.

Bron: nixon.digital

27 maart 2026 Eric van der Burg (VVD) geeft toestemming voor Solvinity-DigiD verlenging twee jaar.

Bron: tweedekamer.nl

8 april 2026 Staatssecretaris Van Bruggen non-paper Brussel met zorgen over Digital Omnibus.

Bron: rijksoverheid.nl

21 april 2026 Kamerdebat: Eric van der Burg laat zijn besluit van 27 maart onvermeld.

Bron: tweedekamer.nl

25 april 2026 FTM publiceert via Woo: ministerie van Justitie en Veiligheid had een Palantir-contract uit 2014 voor passagiersgegevens-analyse door de Marechaussee (gebruik 2009-2015). Minister Van Weel noemde dit contract niet bij Kamervragen in augustus 2025; het Woo-besluit dateert van medio april 2026, Van Weel informeerde de Kamer op 20 april.

Bron: ftm.nl

April 2026 Eerste Kamer functieregister-wijziging Van der Linden, vier maanden na feitelijke aanvang DPG-rol, na vragen GeenStijl.

Bron: eerstekamer.nl en geenstijl.nl

1 mei 2026 Marjolein van der Linden formeel manager public affairs DPG Media.

Bron: dpgmedia.nl

2 mei 2026 forensisch dossier 100 sites. 110 kritieke, 252 ernstige bevindingen.

Bron: mickbeer.com

3 mei 2026 Publicatie 100 NL sites forensisch dossier.

Bron: mickbeer.com

5 mei 2026 Kort geding ingesteld door drie burgers tegen Solvinity-verlenging. Advocaat mr. R. Sharaf (Adelmeijer Hoyng Maastricht).

Bron: agconnect.nl

6 mei 2026 Haagse rechter wijst kort geding af. Solvinity-contract verlengd. Pieter van Oordt (CPO Logius) ontslagen.

Bron: ibestuur.nl en computable.nl

7 mei 2026 Antoni Bar (ex-Piwik PRO Product Manager Wroclaw) bevestigt op LinkedIn: geen Piwik PRO Polen-cloud, alleen Azure of Elastx (Zweden).

Bron: linkedin.com/in/antonibar

9-10 mei 2026 104 sites burgerrapport plus 106 sites privacy-onderzoek. Scan-output gehashed via SHA256 plus OpenTimestamps op Bitcoin (zie Bijlage B).

Bron: mijnoverheid.us

10 mei 2026 Creatiedatum van dit hoofddossier (publicatie volgt).

Bron: mickbeer.com, mijnoverheid.us

12. Bronnen per claim

Iedere claim in dit dossier is voorzien van een primaire openbare bron. Hieronder de complete bronnenlijst per hoofdstuk, met directe URL waar mogelijk. Toegang vereist geen abonnement, geen bibliotheek, geen autorisatie. Alles staat open.

13.1 Hoofdstuk 3 (technische bewijslast)

- Forensisch dossier 100 NL sites door Mick Beer, 3 mei 2026 — https://mickbeer.com
- Burgerrapport 104 sites, BeforeYouMick scanner v3.7, 9-10 mei 2026 — https://mijnoverheid.us
- Het Privacy Onderzoek 106 organisaties, BeforeYouMick scanner v3.7-3.8, 10 mei 2026
- Mick Beer Medium artikelen cookie-onderzoek, maart 2026 — https://medium.com/@mickbeer
- AP-melding 7cb0-9871 (24-25 maart 2026), referentie via Autoriteit Persoonsgegevens
- BeforeYouMick scanner-output (privé op Hetzner): SHA256 + OpenTimestamps in Bijlage A

13.2 Hoofdstuk 4 (de commerciele tracking-cirkel)

- DPG Media jaarcijfers 2024-2025 — https://www.marketingreport.nl en https://www.marketingtribune.nl
- EIB persbericht 28 januari 2022 over 100 miljoen euro DPG-lening — https://www.eib.org/en/press/news/2022/2022-029
- EIB persbericht 19 december 2024 over 120 miljoen euro DPG-lening — https://www.eib.org/en/press/news
- FTM Mark Koster, mei 2025, EIB-DPG en Trusted Web 50 miljoen — https://www.ftm.nl
- Big Brother Award 2024, expert-prijs DPG Trusted Web — https://bigbrotherawards.nl/winnaars-2024
- Hof Amsterdam 5 december 2023, Xandr — https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHAMS:2023:2971
- Rb Amsterdam 7 juni 2024, Xandr — https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2024:3331
- Rb Amsterdam vzr 12 februari 2025, Xandr — https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2025:885
- Raad van State 24 september 2025, DPG — https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RVS:2025:4562

13.3 Hoofdstuk 5 (parallelle architectuur)

- AP-boete Belastingdienst 7 december 2021 — https://www.autoriteitpersoonsgegevens.nl/actueel/boete-belastingdienst-voor-zwarte-lijst-fsv
- AP-boete Belastingdienst FSV 12 april 2022 — https://www.autoriteitpersoonsgegevens.nl/actueel
- BNR onderzoek MIVD-Datastream januari 2024 — https://www.bnr.nl/podcast/cybercrime
- FTM publicatie Marechaussee-Palantir, 25 april 2026 — https://www.ftm.nl
- Rb Den Haag 5 februari 2020, SyRI — https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBDHA:2020:865
- Nixon Digital onderzoek gemeentewebsites Google Analytics, 17 maart 2026 — https://nixon.digital
- Atlas Privacy v Babel Street, US District Court Eastern District Virginia, oktober 2024

13.4 Hoofdstuk 6 (toezicht-vacuum)

- KPMG-onderzoek capaciteit AP, 2020, aangeboden aan de Tweede Kamer via Kamerbrief 25268/32761 nr. 192 — https://www.tweedekamer.nl
- Motie Hijink, Kamerstuk 27529-240, aangenomen 9 februari 2021 — https://www.tweedekamer.nl/kamerstukken/moties
- Brief Sander Dekker over weigering uitvoering motie, april 2021 — https://www.tweedekamer.nl
- Miljoenennota 2022, AP-budget hoofdstuk J&V — https://www.rijksbegroting.nl
- AP jaarverslag 2024, cookie-handhavingsbudget — https://www.autoriteitpersoonsgegevens.nl/jaarverslag
- AG Connect, citaat Michiel van Nispen (SP) over motie-blokkade — https://www.agconnect.nl
- Aleid Wolfsen quote 'lachwekkende achterstanden' Trouw-interview — https://www.trouw.nl

13.5 Hoofdstuk 7 (keurmerken-stelsel)

- Status accreditatie AVG-certificering Nederland — https://www.rva.nl/nieuws/avg-certificatie
- AP over AVG-certificering — https://www.autoriteitpersoonsgegevens.nl/themas/basisregels-avg/avg-in-de-praktijk/avg-certificaat
- Brand Compliance BC 5701:2023 schema — https://www.brand-compliance.com
- Brand Compliance BC EU 5701:2024, EDPB-goedkeuring — https://edpb.europa.eu
- Privacy Verified register — https://privacyverified.nl/deelnemers
- ICTRecht — https://www.ictrecht.nl
- NEN 7510:2024 norm — https://www.nen.nl/nen-7510

- ISO/IEC 27701:2025 — https://www.iso.org/standard/85819.html
- NOREA Privacy Audit Proof — https://www.norea.nl
- Justitia: Kiwa-certificaat is geen AVG-certificaat — https://www.justitia.nl

13.6 Hoofdstuk 8 (Cloud Act blootstelling)

- Piwik PRO blog over public/private/self-hosted — https://piwik.pro/blog/public-cloud-private-cloud-self-hosted
- Piwik PRO glossary cloud-hosting — https://piwik.pro/glossary/cloud-hosting
- Piwik PRO privacy en security — https://piwik.pro/privacy-security
- Piwik PRO LinkedIn-pagina — https://www.linkedin.com/company/piwik-pro
- LinkedIn-comment Antoni Bar (ex-Piwik PRO Product Manager), 7 mei 2026
- ICTRecht over Cloud Act — https://www.ictrecht.nl/blog/mag-de-amerikaanse-overheid-persoonsgegevens-vorderen-bij-eu-bedrijven-onder-de-cloud-act
- ICT Magazine, 13 januari 2026 — https://www.ictmagazine.nl/blogs/de-juridische-spagaat-van-cloudopslag
- Kiteworks over EU-soevereiniteit — https://www.kiteworks.com/nl/avg-naleving/europese-ondernemingen-microsoft-365-soevereiniteit
- Arnoud Engelfriet over Cloud Act — https://blog.iusmentis.com
- Techzine: Microsoft Cloud for Sovereignty wassen neus, Atea-CEO Sønsteby, 16 december 2023 — https://www.techzine.nl
- Zivver, juni 2025 — https://www.zivver.com/nl/blog/de-echte-risicos-van-de-amerikaanse-cloud
- AG Connect: burgers naar rechter DigiD-Solvinity-Kyndryl, mei 2026 — https://www.agconnect.nl
- iBestuur: rechter besluit Solvinity verlenging, 6 mei 2026 — https://www.ibestuur.nl
- Computable: Nederlandse Staat verlengt met Solvinity, 6 mei 2026 — https://www.computable.nl
- Techzine: kort geding eist stop verlenging DigiD, mei 2026 — https://www.techzine.nl

13.7 Internationale context

- ICCL-rapport 2022 (Johnny Ryan) RTB als grootste datalek — https://www.iccl.ie/digital-data/iccl-report-on-the-rtb-system
- KU Leuven USENIX Security 2026, Vlummens en Girish, Meta-Yandex localhost-poorten — https://www.usenix.org/conference/usenixsecurity26
- HvJ EU C-604/22, IAB Europe TCF onwettig, maart 2024 — https://curia.europa.eu
- BNR Pols en Moonen, Datastream Frederikkazerne, januari 2024 — https://www.bnr.nl
- Secura over Datastream — https://www.secura.com

13.8 Hoofdstuk 9 (politieke lobbylaag)

- Eerste Kamer register nevenfuncties Marjolein van der Linden — https://www.eerstekamer.nl/lid/marjolein_van_der_linden
- DPG Media persbericht aanstelling Van der Linden, 1 december 2025 — https://dpgmedia.nl
- Stichting Democratie en Media — https://www.sdm.nl
- Brandbrief 22 mediabedrijven aan informateur Buma, december 2025 — https://www.villamedia.nl
- Coalitieakkoord 'Aan de slag', kabinet-Jetten, 30 januari 2026 — https://www.kabinetsformatie2025.nl
- Beediging kabinet-Jetten, 23 februari 2026 — https://www.rijksoverheid.nl
- Eerste Kamer zetelverdeling per 10 mei 2026 — https://www.eerstekamer.nl/zetelverdeling
- FTM publicatie OPR-Google deal — https://www.ftm.nl
- Big Brother Award 2023 Dilan Yesilgoz — https://bigbrotherawards.nl/winnaars-2023
- GeenStijl-vragen over Van der Linden meldingstermijn — https://www.geenstijl.nl

13.9 Hoofdstuk 10 en 12 (hefbomen en tijdlijn)

- Tweede Kamer kamerstukken digitalisering — https://www.tweedekamer.nl/kamerstukken
- AP-website klachten en handhaving — https://www.autoriteitpersoonsgegevens.nl
- EDPB en EDPS gepubliceerde non-papers — https://edpb.europa.eu
- Bits of Freedom — https://www.bitsoffreedom.nl
- Privacy First — https://privacyfirst.nl
- EDRi (European Digital Rights) — https://edri.org

13.10 Bijlage A (cryptografische integriteit)

- OpenTimestamps protocol en CLI — https://opentimestamps.org
- OpenTimestamps client (Python) — https://github.com/opentimestamps/opentimestamps-client
- Bitcoin-blockchain explorer — https://mempool.space
- Calendar a.pool.opentimestamps.org — https://a.pool.opentimestamps.org
- Calendar Eternity Wall — https://btc.calendar.eternitywall.com
- Calendar Catallaxy — https://btc.calendar.catallaxy.com

A. Bijlage A · cryptografische integriteit van scan-data

De rauwe scan-output (104 canonieke site-JSONs uit BeforeYouMick scanner v3.7 en v3.8, gemeten op 9 en 10 mei 2026) is gehashed met SHA256 en getekend via OpenTimestamps. Dat geeft drie bewijslijnen tegelijkertijd:

- De SHA256-hash bewijst dat de scan-output sinds het moment van vastlegging niet is gewijzigd.
- De OpenTimestamps-handtekening (die uiteindelijk in het Bitcoin-blockchain wordt opgenomen) bewijst dat de hash bestond op een specifiek tijdstip en niet later is gefabriceerd.
- De combinatie maakt dat een bevinding in dit dossier niet alleen reproduceerbaar is, maar ook achteraf falsifieerbaar als iemand zou beweren dat de scan-data gemanipuleerd is na publicatie.

A.1 Status per 10 mei 2026

Stempelmoment: 10 mei 2026 om 18:44 UTC. Alle 104 SHA256-hashes zijn op dat moment ingediend bij vier publieke OpenTimestamps-kalenders: a.pool.opentimestamps.org, b.pool.opentimestamps.org, eternitywall.com en btc.calendar.catallaxy.com.

Op creatiedatum van dit dossier is per individuele hash sprake van calendar-attestation maar nog niet van Bitcoin block-attestation. Dat is verwacht gedrag: kalenders bundelen hashes en publiceren een Merkle-wortel naar de Bitcoin-blockchain. Block-attestation volgt typisch binnen enkele uren tot een etmaal na het stempelmoment. Een ots verify <bestand>.ots toont op 10 mei 2026 om 19:00 UTC nog 'Pending confirmation in Bitcoin blockchain'. Dit verandert in 'Success! Bitcoin block <nummer> attests existence as of <ts>' zodra het block-anker beschikbaar is.

De volgende handeling op of rond 11 mei 2026: ots upgrade <bestand>.ots draait per zijbestand en haalt de Bitcoin block-attestation op. Daarna is de proof zelfstandig verifieerbaar zonder vertrouwen in welke kalender of welke partij dan ook.

A.2 Verdeling over scan-batches

De 104 sites zijn gemeten in drie achtereenvolgende scan-batches:

- Batch A: runs/2026-05-09_forensisch_v3.7/ (39 sites, gemeten 9 mei 2026 vanaf 23:42 CEST)
- Batch B: runs/2026-05-10_remaining_v3.8/ (41 sites, gemeten 10 mei 2026 vanaf 00:39 CEST)
- Batch C: runs/2026-05-09_forensisch_v3.7_v2/ (24 sites, herhaalmeting 9 mei 2026 voor sites met onvolledige eerste meting)

A.3 Verificatie-instructies

Iedere lezer kan de integriteit zelfstandig verifieren met de open-source OpenTimestamps CLI:

```
# integriteit (hash moet matchen onderstaande tabel):
sha256sum <pad-naar-json>
# tijdsanker (vraagt Bitcoin-blockchain confirmatie):
ots verify <pad-naar-json>.ots
```

Een succesvolle verificatie ziet er ongeveer zo uit (na Bitcoin-confirmatie):

> *Got 1 attestation(s) from https://btc.calendar.catallaxy.com — Success! Bitcoin block <nr> attests existence as of <ts> UTC.*

A.4 Volledige tabel: 104 SHA256-hashes met OpenTimestamps-status

Onderstaande tabel bevat per site de getrunceerde SHA256-hash (eerste 16 plus laatste 8 hex-karakters van de 64-karakter hash) en de scan-batch (A, B of C). De volledige hashes staan in sha256.txt, beschikbaar op verzoek of via mijnoverheid.us. Volgorde: alfabetisch op site-naam.

Site	SHA256 (eerste 16 ... laatste 8)	Batch
113.nl	ab4ffe91a233e37c…6be2e4f0	C
50plus.nl	6c359b2ce6456b49…fc326793	B
accenture.com	3a028dccaf1e35f4…0c2dbbd3	A
ad.nl	42839bc93461bb70…a1545df7	B
afas.nl	2f32313df3242064…f2d07922	A
aivd.nl	e83da63a79dbf073…bd855de7	B
atos.net	a133a29444d1493b…85654a20	A
autoriteitpersoonsgegevens.nl	a71ea61091d8be4d…c000ac89	A
bbb.nl	829452a0a455ebb0…f1dab56e	B
belastingdienst.nl	74420863895f6518…b788b25d	B
bitsoffreedom.nl	6339ceac85fb3c49…fc6c2856	B
bnr.nl	aeb3e0e0ca4ae8c7…42cf7dc4	C
brand-compliance.com	4070d446746307df…33953ac7	A
capgemini.com	72835d58b880dafb…b574a7c5	A
cbs.nl	bef5f5c5b07c7796…55876fa3	B
cda.nl	619575bb4e0250f4…2fcfb1b2	B
centric.eu	8e1a067595ddda33…81a1c774	A
centrumseksueelgeweld.nl	f53b69e79c28e218…6113d749	C
chipsoft.nl	9dbe25bd938a0c9c…19195b9c	A
christenunie.nl	253f260163cb5353…2b9d011f	B
considerati.com	e6362180a92ded41…a11fe9f3	B
ctivd.nl	41ecc60dc9dd5564…d7eb2c8a	B
d66.nl	69c68a8d2c1fc6a6…5f9a3e44	B
decorrespondent.nl	b80865d723eb28c5…5a1af134	C
denk.nl	726f8a1e10d9247d…760f1835	B
digid.nl	5192c87f36c677f5…a55176a1	A
dnv.com	6b70cd77e03646e3…8b359233	A
dpgmedia.nl	54070c4d4e68d566…d0b60015	B

Site	SHA256 (eerste 16 ... laatste 8)	Batch
duo.nl	`3dfd76e0a5ca4e0c…63777cd2`	C
exact.com	`7748cfcda7709b14…fa681da6`	A
examenblad.nl	`16f1d12c1d126e90…92a31e50`	C
ftm.nl	`3974391669fdc9fd…dfa428c9`	C
fvd.nl	`3e12c408db211430…42cdbba0`	B
groenlinkspvda.nl	`e3b4a5828e345b9f…bd3bec00`	B
huisvanklokkenluiders.nl	`b41d1d3a134fadbe…f8471049`	B
humanitas.nl	`c1bdc658b49617de…a178c259`	C
ictrecht.nl	`b0f4db357d8d5a00…21321386`	A
ictu.nl	`344e98934efd1117…b3627a61`	A
iddin.nl	`ed148ceacca06396…a41ecc1e`	A
itslearning.com	`aaa92ae5612e6228…e22efedf`	C
itsme.nl	`aae3157c0f9a3e07…8fc4ffd1`	A
ja21.nl	`42ef6780c10177fe…61f0afd0`	B
juridischloket.nl	`2729a59c14cd130c…cf6c9bdc`	C
kennisnet.nl	`cc15cbfb238d0236…d369f1df`	C
kindertelefoon.nl	`bbf9f094f14e2f2c…2fec5412`	C
kiwa.com	`cf348fe24ad171a1…b863dc69`	A
klokkenluiders.nl	`73def3b22974dad6…fa37aba6`	C
kpn.com	`4e1b4eea49745b11…330935ec`	A
kvk.nl	`ab94fbc05c2e920b…3e89029f`	A
kyndryl.nl	`78c211f7f047f2eb…bb89affd`	A
logius.nl	`b8be959d61f6cd7d…b09c467c`	A
magister.nl	`1dec94f3eff67357…0eecd593`	C
mendix.com	`dc2f68c150c00705…0a764454`	A
mijnoverheid.nl	`779fe416e8693125…896e2758`	A
mijnschoolinfo.nl	`ffde94032f3e34b1…fbb04399`	C
mindkorrelatie.nl	`aec44f55116118ce…d4f5fb5d`	C
moedersvoormoeders.nl	`7b1f33b175dad1ab…70758413`	C
nbip.nl	`70240fc88b8cb9f1…439f1435`	A
ncsc.nl	`c23b5a68d84d0ac0…569ca7fb`	B
ndpnieuwsmedia.nl	`1e6175688da5ee22…0d85b124`	B
nederlandictenoverheid.nl	`79c8e569243f786c…552264b6`	A
nictiz.nl	`88bba924a501852b…3ef2680c`	A
nos.nl	`2769f8f7df637a77…e6bf1e90`	B
nrc.nl	`29cc799086c64888…cd8973fc`	B
nsc.nu	`a744b84249364132…e6109fc0`	B
nu.nl	`3e168f87c5a057ee…09c3711a`	B
odc-noord.nl	`d58e1c1797fee6c8…28febbeb`	A
odido.nl	`76dfcff6700769d2…6e327888`	A
om.nl	`59a7a3f3cb755e32…3e0d6913`	B
partijvoordedieren.nl	`9ea0276b11537338…0ad96603`	B
pinkroccade.nl	`c65f53b9d12b1917…10e4ab02`	A
politie.nl	`d2213c82b890b4d3…7259924b`	B
privacycompany.eu	`c5d275e287477a61…51e7d05e`	A
privacyfirst.nl	`3ebdbac06f5e7d43…baa21b21`	B
privacyverified.nl	`5845ca59ce4b661c…81a46a8e`	B
publeaks.nl	`f11fee76f5a75623…701e5214`	C
pvv.nl	`fb26eee5e2ce5df3…e289c246`	B
quanza.net	`22877973c058c616…5d71ab7b`	A
rdw.nl	`6543ab8187b9fefe…75380dbe`	A
rechtspraak.nl	`4f4cd94b70fa614b…8ba50694`	B
rijksoverheid.nl	`b2a45e46a64b136a…86e17163`	B

Site	SHA256 (eerste 16 ... laatste 8)	Batch
schuldhulpmaatje.nl	`ca001b6d1fa19898…62478a36`	C
sgp.nl	`d6391482cf4325e4…0a2112c0`	B
signicat.com	`95a1f12dda190bd1…8c91e5dc`	A
slachtofferhulp.nl	`7fa6c8757872d2da…cc47fa7b`	C
soaaids.nl	`53f321e694d79dcf…66ee95a3`	B
somtoday.nl	`380a97bd3f59be91…75ebdb92`	C
sp.nl	`78928023a03acf5f…e7e70b3d`	B
ster.nl	`fc3a653b0fbc6a0f…c9bea690`	B
studielink.nl	`960ab98f96ebf749…d1b64c02`	C
surf.nl	`8e13ccf70f125379…4a17f03b`	A
svb.nl	`31f6cd18d8a75463…ed9a8e92`	A
topicus.nl	`fc9de6c50cb1d6f2…133196bf`	A
trouw.nl	`a4efed14380720e9…8416242c`	B
tuv-nederland.nl	`de0af9dfa3c56000…a8a9bdc9`	B
tüv-nederland.nl	`7f0a49f4632ece72…82b1ef4a`	A
uwv.nl	`c12c972749838080…d85e5962`	A
vecozo.nl	`b71045bbf7481bff…cbf19e22`	A
veiligthuis.nl	`432c6de45f4d8fa3…f0675d06`	C
vk.nl	`ae4d5bb2df03c4d7…d6391d96`	C
volkskrant.nl	`c30c0c3159dba632…fb3aaa93`	B
volt.nl	`073e63372a697566…8edd8ccc`	B
vvd.nl	`b7f1a496ea888b64…5c8d5186`	B
yivi.app	`467ed222e1e9f532…bf18615a`	A

Totaal: 104 bestanden gehashed, 104 OpenTimestamps proofs aanwezig op 10 mei 2026 om 18:44 UTC. Bitcoin block-attestation volgt typisch binnen 24 uur na stempeltijd.

A.5 Wat dit niet doet

De hashing en timestamping bewijzen alleen integriteit en ouderdom van de scan-output. Zij bewijzen niet dat de scan correct is uitgevoerd, dat de scanner correct functioneert, of dat de bevindingen juridisch standhouden. Dat blijft inhoudelijk onderzoek. Wel garandeert de tijdsanker dat geen enkel bestand na 10 mei 2026 is aangepast en als oudere staat van scan-output kan worden gepresenteerd, en dat geen enkel bestand achteraf is gefabriceerd.

> *Praktisch: een onderzoeker, journalist of toezichthouder die later twijfelt aan de scan-data hoeft* de auteur *niet te vertrouwen. Een sha256sum op de geleverde JSON, een ots verify op de bijbehorende .ots, en een Bitcoin-blockchain-lookup geven samen een onafhankelijk integriteitsbewijs dat losstaat van iedere uitgevende partij.*

Einde dossier