PRIVACYONDERZOEK

DigiD.nl & Logius

Tracking, gegevensverwerkingen en privacygebreken bij de nationale authenticatievoorziening

17 april 2026 · Versie 2.0 · Publiek rapport

Samenvatting

Dit rapport beschrijft een onafhankelijk technisch privacyonderzoek naar digid.nl en de bijbehorende dienstverlening van Logius (onderdeel Ministerie van Binnenlandse Zaken). Het onderzoek is uitgevoerd op 17 april 2026 via browseranalyse in een schone private-browsersessie, HAR-bestandsanalyse en broncode-inspectie.

De bevindingen zijn verdeeld in drie clusters:

- Cluster A — Website-tracking: op digid.nl worden trackingcookies gezet en externe scripts geladen zónder dat de gebruiker toestemming heeft gegeven. Dit is aantoonbaar in strijd met de Telecommunicatiewet.
- Cluster B — Solvinity: de infrastructuurbeheerder van DigiD (Solvinity) is niet vermeld als verwerker in de officiële privacydocumentatie, terwijl DigiD zelf erkent dat Solvinity persoonsgegevens verwerkt. Bij een overname door het Amerikaanse Kyndryl geldt de CLOUD Act.
- Cluster C — Documentaire gebreken: DigiD heeft van 2018 tot minimaal 2023 gefunctioneerd zonder een geldige AVG-conforme DPIA. De beloofde nieuwe DPIA is niet aangetroffen in het Rijksoverheid AVG-register.

Elk hoofdstuk sluit af met een eerlijkheidsoordeel: wat is technisch bewezen, wat is aannemelijk maar niet bevestigd, en wat is uitdrukkelijk niet bewezen.

Ernst	Bevinding	Juridische grondslag
🔴 KRITIEK	Matomo trackingcookies gezet vóór toestemming — op homepage, inlogpagina, MFA-stap en dashboard	Telecommunicatiewet art. 11.7a
🔴 KRITIEK	DPIA ontbreekt: vijf jaar zonder geldige AVG DPIA (2018–2023)	AVG art. 35
🔴 KRITIEK	Solvinity erkend als verwerker door DigiD zelf, maar niet vermeld in privacyverklaring of DPIA	AVG art. 13, 28, 30
🟠 ERNSTIG	KCM Survey (commerciële derde partij) geladen op activatiepagina zonder consent	AVG art. 28 + Tw 11.7a

🟠 ERNSTIG	Service Integrator heeft toegang tot ALLE persoonsgegevens — identiteit niet publiek	AVG art. 13/14
🟠 ERNSTIG	2017 PIA-claim over Piwik-anonimiteit aantoonbaar onjuist gebleken in 2026	AVG art. 5(1)(a)
🟡 MATIG	Verwerkingslocatie-claim 'enkel Nederland' dekt niet de volledige verwerkerskéten	AVG art. 44–49
🟡 MATIG	MCC (Belastingdienst) als verwerker van DigiD app-logs: niet vermeld in privacyverklaring	AVG art. 13

Inhoudsopgave

Onderzoeksmethode en onderzochte domeinen

Methode

Het onderzoek is uitgevoerd op 17 april 2026. Elke sessie begon met een schoon Firefox-profiel in private-browsermodus — geen cookies, geen cache, geen opgeslagen data. Zo wordt de situatie nagebootst van een gewone burger die digid.nl voor het eerst bezoekt.

Gebruikte technieken:

- Firefox DevTools: Network-tab voor alle HTTP-verzoeken, Storage Inspector voor cookies en lokale opslag, Debugger voor JavaScript-broncode
- HAR-export: volledige logging van alle requests, responses, cookies en parameters tijdens de inlogflow
- Broncode-inspectie: directe analyse van JavaScript-bestanden via view-source:
- HTML-broncode analyse van de officiële Logius privacydocumentatie

Onderzochte domeinen

Onderzochte URL	Type	Tijdstip
www.digid.nl	Publieke homepage	17 apr 2026 — 01:37
digid.nl/inloggen	Inlogpagina (vóór authenticatie)	17 apr 2026 — 01:39
digid.nl/sms_controleren	MFA-stap: SMS-verificatie	17 apr 2026 — 01:58
digid.nl/aanvragen-en-activeren/code-ontvangen	DigiD-activatiepagina	17 apr 2026 — 01:43
mijn.digid.nl/home	Persoonlijk dashboard (na inloggen)	17 apr 2026
logius.nl/.../gegevensverwerkingen-digid	Officiële verwerkingsdocumentatie	17 apr 2026 — 01:45
digid.nl/solvinity	Solvinity FAQ-pagina	17 apr 2026
digid.nl/over-digid/privacy	Privacyverklaring DigiD	17 apr 2026

DEEL I

Website-tracking en cookies

Wat digid.nl doet vóórdat u iets heeft aangeklikt

Bevinding 1 — Matomo trackingcookies zonder toestemming

KRITIEK

Bij het laden van digid.nl worden trackingcookies gezet die een persistent bezoekersprofiel aanmaken — vóór enige interactie of toestemming van de gebruiker.

Wat is aangetoond

Bij eerste bezoek aan www.digid.nl — schone browser, niets aangeklikt — worden direct twee Matomo-cookies aangemaakt:

Cookie	Waarde	Levensduur	Functie
_pk_id.28.d667	4eaf2372832... (unieke hash)	13 maanden	Persistent bezoekersprofiel over sessies
_pk_ses.28.d667	1	~30 minuten	Sessietracking

Op de inlogpagina verstuurt Matomo een trackingpixel naar statistiek.digid.nl. Uit HAR-analyse zijn de volgende parameters aantoonbaar:

Parameter	Waarde	Betekenis voor de gebruiker
_id	ed711fb7c7671aab	Uw unieke bezoeker-ID — consistent over alle sessies
_idts	1776383659	Tijdstip van uw allereerste bezoek (opgeslagen)
url	https://digid.nl/inloggen	Exact bijgehouden: u was op de inlogpagina
action_name	DigiD: Inloggen | Keuze	Paginanaam én context van uw bezoek
res	1920x1080	Uw schermresolutie
pdf / qt / fla / java	1 / 0 / 0 / 0	Profiel van uw browser-plugins
h / m / s	1 / 54 / 19	Exact tijdstip van dit bezoek: 01:54:19

Broncode: geen toestemmingscontrole aanwezig

Het JavaScript-bestand analytics-[hash].js bevat:

```
_paq.push(["trackPageView"]);    // direct uitgevoerd, geen consent-check _paq.push(["enableLinkTracking"]); // ook klik-gedrag wordt geregistreerd
```

Er is geen if-statement, geen cookiebanner-integratie, geen opt-in mechanisme. trackPageView() wordt direct bij het laden van elke pagina uitgevoerd.

Nuancering: statistiek.digid.nl is first-party

Statistiek.digid.nl is een subdomein van digid.nl, wat sterk duidt op self-hosting door Logius. Data gaat dus waarschijnlijk niet naar een extern commercieel bedrijf. Dit is een positief punt.

Dit verandert echter niets aan de wettelijke verplichting: de Telecommunicatiewet art. 11.7a vereist ondubbelzinnige toestemming vóór het plaatsen van cookies die niet strikt noodzakelijk zijn, ongeacht wie de ontvanger is.

De analytische-cookies-uitzondering van de AP geldt NIET voor _pk_id: die uitzondering vereist dat er geen persistent cross-session identifier wordt aangemaakt. _pk_id heeft een levensduur van 13 maanden en koppelt alle bezoeken van één browser aan hetzelfde profiel.

Tegenstrijdigheid met de eigen privacyverklaring

De privacyverklaring van DigiD (sectie 5) belooft over Piwik/Matomo:

> *"Daarvoor wordt gebruik gemaakt van een cookie met een anoniem visitor-id — niet herleidbaar tot een persoon."*

De HAR-analyse bewijst technisch het tegendeel: _pk_id bevat een unieke hash, een timestamp van het eerste bezoek en een bezoekteller. In combinatie met tijdstip, URL-sequentie en browserfingerprint is dit een traceerbaar profiel over meerdere sessies.

Dezelfde tegenstrijdigheid staat letterlijk in de 2017 PIA, waar wordt toegezegd dat de Piwik-implementatie 'niet herleidbaar zal zijn naar een persoon'. Die belofte is nooit gerealiseerd en de PIA is nooit bijgewerkt.

Bevinding 2 — Tracking door de volledige authenticatieketen

KRITIEK Matomo volgt de gebruiker van de eerste pagina tot na het inloggen. Eén persistent ID koppelt alle stappen aan hetzelfde profiel.

Stap	Onderzochte URL	Matomo actief	Bewijs
1. Homepage	www.digid.nl	Ja	Storage Inspector: _pk_id en _pk_ses gezet bij laden
2. Inlogpagina	digid.nl/inloggen	Ja	HAR: trackingpixel verstuurd met persistent ID + tijdstip
3. MFA-stap	digid.nl/sms_controleren	Ja	Debugger: analytics.js + piwik.js geladen
4. Persoonlijk dashboard	mijn.digid.nl/home	Ja	Network-tab: matomo.js + piwik.js aanwezig
5. Activatiepagina	digid.nl/aanvragen-en-activeren/...	Ja (×2)	Network-tab: Matomo beacon twee keer verstuurd

Wat dit betekent: via de persistente _pk_id cookie registreert Matomo dat één bezoeker de homepage bezocht, vervolgens de inlogpagina, MFA voltooide en het dashboard bekeek — allemaal gekoppeld aan hetzelfde bezoekersprofiel.

Eerlijkheidsoordeel: hoewel Matomo actief is op mijn.digid.nl (het dashboard waar het BSN zichtbaar is), is NIET aangetoond dat het BSN zelf naar Matomo wordt verstuurd. De trackingpixel-parameters bevatten geen BSN. Matomo registreert gedragspatronen, niet de inhoud van de pagina.

Bevinding 3 — KCM Survey: externe commerciële partij op gevoelige pagina

ERNSTIG Op de DigiD-activatiepagina worden scripts geladen van een commercieel Nederlands klanttevredenheidsbedrijf, zonder dat de gebruiker hierover is geïnformeerd of toestemming heeft gegeven.

Op digid.nl/aanvragen-en-activeren/code-ontvangen worden de volgende externe domeinen gecontacteerd:

Domein	Geladen	Functie
api.kcmg.nl	SystemTranslations, locales	Survey-API: configureert en initieert de vragenlijst
v.kcmg.nl	CSS, fonts (Radnika-Medium.otf)	Survey-stijlen en lettertypes
viewer.kcmg.nl	kcm-survey.js	Survey-engine JavaScript
viewerapi.kcmg.nl	StartSurvey (POST)	Verstuurt data bij initialisatie survey

KCM Group BV is een Nederlands commercieel bedrijf dat klanttevredenheidsonderzoek aanbiedt (NPS, CES). De functionaliteit is een 'Heeft deze informatie u geholpen?'-widget onderaan de pagina. De intentie is begrijpelijk — kwaliteitsverbetering — maar de implementatie roept vragen op:

- KCM staat niet vermeld in de privacyverklaring of gegevensverwerkingsdocumentatie van Logius.
- Een extern JavaScript-bestand van een commerciële partij laadt op een pagina waar iemand bezig is de enige universele Nederlandse authenticatiemethode te activeren.
- De Content-Security-Policy van v.kcmg.nl staat verbindingen toe naar player.vimeo.com, www.youtube.com en Azure CDN — dit zijn potentiële extra tracking-vectoren.
- AVG art. 28 vereist een verwerkersovereenkomst met KCM als zij persoonsgegevens verwerken. Of die overeenkomst bestaat is niet publiek verifiëbaar.

Bevinding 4 — Sentry foutmonitor in de authenticatieflow

> **MATIG** Een foutmonitoring-dienst verstuurt technische data tijdens het inlogproces. Sentry is gehost op een overheidsdomein, wat externe risico's beperkt — maar transparantie ontbreekt.

Op meerdere DigiD-pagina's worden POST-requests verstuurd naar sentry.dtnr.nl:

- Endpoint: POST https://sentry.dtnr.nl/api/27/envelope/
- Client: sentry.javascript.nextjs/10.42.0
- Verstuurt foutinformatie, transactie-data en URL-patronen

Nuancering: dtnr.nl is geregistreerd voor de Nederlandse Rijksoverheid. Sentry is waarschijnlijk een self-hosted instantie — geen doorgifte aan Sentry Inc. (Amerikaans bedrijf) aangetoond. Dit beperkt het risico aanzienlijk ten opzichte van de eerste analyse.

Wat blijft: Sentry staat niet vermeld als verwerker in de Logius-documentatie. Of PII-scrubbing is geconfigureerd (zodat geen gebruikersdata in error-logs terechtkomt) is niet verifiëbaar zonder toegang tot de configuratie.

DEEL II

Solvinity, infrastructuur en CLOUD Act

Wie beheert de kern van DigiD — en staat dat ergens beschreven?

Bevinding 5 — Solvinity is AVG-verwerker: vier bewijsbronnen

KRITIEK

DigiD erkent zelf in eigen bewoordingen dat Solvinity persoonsgegevens verwerkt. Desondanks staat Solvinity nergens vermeld als verwerker in de officiële privacydocumentatie.

Bewijs 1 — DigiD's eigen FAQ (digid.nl/solvinity)

De FAQ bevat letterlijk de sectie:

> *"Welke persoonsgegevens worden verwerkt door Solvinity?"*

Met als antwoord:

> *"Solvinity ontvangt het IP-adres en e-mailadressen van mensen met een DigiD-account. Solvinity verwerkt deze gegevens alleen om DigiD goed te laten werken."*

De AVG-definitie van een verwerker (art. 4 lid 8) is: een partij die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. DigiD heeft dit met eigen woorden bevestigd.

Bewijs 2 — Solvinity ontbreekt in de privacyverklaring (AVG art. 13)

Privacyverklaring sectie 6 noemt als ontvangers van persoonsgegevens: helpdesk-partijen, een survey-partij en opsporingsdiensten. Solvinity staat er NIET in — terwijl de FAQ bevestigt dat Solvinity IP-adressen en e-mailadressen ontvangt.

Dit is een directe schending van AVG art. 13(1)(e): betrokkenen moeten worden geïnformeerd over alle ontvangers van hun persoonsgegevens.

Bewijs 3 — Solvinity ontbreekt in het officiële Omgevingsmodel DigiD

Het Omgevingsmodel DigiD (Figuur 1 in de Logius gegevensverwerkingsdocumentatie) vermeldt 11 partijen. Solvinity — de partij die het centrale infrastructuurplatform beheert waarover alle authenticatieverkeer loopt — ontbreekt volledig in dit diagram.

Bewijs 4 — Intern Logius-onderzoek (NOS/Volkskrant, 16 april 2026)

Uit een intern Logius-onderzoek dat op 16 april 2026 via NOS naar buiten kwam, bleek dat Solvinity technische toegang heeft tot de persoonlijke gegevens die zichtbaar zijn in MijnOverheid — naam, geboortedatum, adres, inkomen en meer. Dit gaat aanzienlijk verder dan alleen IP-adressen.

Pieter van Oordt, de privacy-adviseur van Logius, trad bewust naar buiten omdat er intern niet naar hem geluisterd werd:

> *"Ik kan het niet simpeler zeggen: de VS kunnen DigiD voor langere tijd uitzetten en geheime informatieverzoeken uitvaardigen."*

Van Oordt kon niet spreken met de staatssecretaris van Binnenlandse Zaken. Het DigiD-contract met Solvinity loopt in 2028 af.

AVG-kwalificatie en gevolgen

- AVG art. 28: een schriftelijke verwerkersovereenkomst is verplicht. Of die bestaat is niet publiek verifiëbaar, maar Solvinity ontbreekt in alle gepubliceerde documentatie.
- AVG art. 13(1)(e): schending. Solvinity ontbreekt als ontvanger in de privacyverklaring.
- AVG art. 30: het verwerkingsregister is incompleet doordat Solvinity ontbreekt.
- AVG art. 44–49: bij overname door Kyndryl (Amerikaans bedrijf, beursgenoteerd) geldt de CLOUD Act. Die geeft de VS het recht om data op te eisen, ook als die data in Nederland staat.
- BTI-toetsing (Bureau Toetsing Investeringen) beoordeelt de overname economisch — dit is géén AVG-toets.

Bevinding 6 — Architectuurclaim vs. werkelijkheid

ERNSTIG

DigiD presenteert Solvinity als passieve hardware-leverancier. Het eigen architectuurdiagram toont een ander beeld: Solvinity centraal in alle authenticatieflows.

DigiD stelt op digid.nl/solvinity:

> *"Solvinity levert het platform waar DigiD op draait. Dit platform draait in een overheidsdatacentrum. Dit maakt Solvinity een leverancier van DigiD, niet eigenaar."*

Het eigen architectuurdiagram op dezelfde pagina toont echter een centrale oranje box 'Infrastructuur platform beheerd door Solvinity' die centraal staat in zowel de aanvraagflow als de inlogflow. Alle authenticatieverkeer van alle Nederlanders loopt er langs.

Wat DigiD claimt	Feitelijke situatie (bewezen of aannemelijk)
"Solvinity is leverancier, niet eigenaar"	Eigen diagram: centrale infrastructuurrol in alle auth-flows
"Platform in overheidsdatacentrum"	Beheer (en daarmee toegang) ligt bij Solvinity, niet bij Logius
"Solvinity verwerkt alleen IP + e-mail"	Intern onderzoek (NOS): Solvinity heeft toegang tot alle MijnOverheid-data
"Niet doorgegeven buiten EU"	Bij Kyndryl-overname geldt CLOUD Act — VS kan data opeisen
"DigiD voldoet aan strenge privacyeisen"	Tracking zonder consent, DPIA ontbreekt, verwerkers niet gedocumenteerd

Eerlijkheidsoordeel: de juridische kwalificatie 'verwerker versus leverancier' is een interpretatie die zonder contractinzage niet sluitend te bewijzen is. Wat wél sluitend is bewezen: DigiD erkent zelf dat Solvinity persoonsgegevens 'verwerkt', en Solvinity ontbreekt desondanks in de volledige privacydocumentatie.

DEEL III

Gebrekkige verwerkingsdocumentatie

Wat de officiële documenten zeggen, weglaten en tegenspreken

Bevinding 7 — Anonieme verwerkers met brede toegang tot persoonsgegevens

ERNSTIG Eén anonieme externe partij heeft toegang tot álle persoonsgegevens die DigiD verwerkt. De identiteit van meerdere sleutelpartijen is publiek niet verifiëbaar.

De officiële gegevensverwerkingsdocumentatie van Logius vermeldt de volgende partijen:

Partij	Toegang tot	Naam publiek?	Opmerking
Leverancier applicatie-diensten (Service Integrator)	ALLE GEGEVENS	Nee	Eén partij — alles; bronnen 2015 noemen Capgemini
Leverancier infrastructuur-diensten (1)	IP-adres, e-mailadres	Nee	Vermoedelijk Solvinity
Leverancier infrastructuur-diensten (2)	IP-adres, e-mailadres	Nee	Tweede infra-partij; identiteit onbekend
MCC (Belastingdienst)	Technische logging, pushnotificaties	Ja (MCC)	Overheidsorgaan als verwerker DigiD-app
Dictu (MinEZK)	Contactformulier	Ja (Dictu)	Cross-ministeriële verwerking
Leverancier SIEM/SOC	Auditlogging	Nee	Beveiligingsmonitoring door onbekende partij
Leverancier helpdesk (2x)	BSN, contactgegevens	Nee	Eerstelijns support; 2017-bron noemt Webhelp
Solvinity	IP, e-mail + MijnOverheid-data	NIET VERMELD	Erkend als verwerker in FAQ, ontbreekt hier

De Service Integrator: één partij met toegang tot alles

De meest vergaande vermelding in de documentatie is: 'Leverancier applicatie-diensten — Persoonsgegevens: Alle gegevens.' Eén anonieme contractor heeft toegang tot het complete DigiD-gegevensbereik: BSN, naam, adres, e-mail, telefoonnummer, inloghistorie en identiteitsdocumentgegevens van 17 miljoen Nederlanders.

Nuancering: het niet-publiceren van leveranciersnamen kan een legitieme veiligheidsmaatregel zijn. Maar AVG art. 13/14 vereist dat betrokkenen worden geïnformeerd over categorieën van ontvangers. 'Leverancier applicatie-diensten' is te generiek om aan die verplichting te voldoen.

MCC (Belastingdienst) als verwerker van DigiD-logs

Het Mobile Competence Center van de Belastingdienst bouwt en beheert de DigiD-app en heeft daarvoor toegang tot technische logging en pushnotificaties. Dit is op zichzelf niet onrechtmatig — er kunnen strikte functiescheidingen gelden. Maar de Belastingdienst is ook de grootste afnemer van DigiD-authenticaties. Dat dezelfde organisatie zowel de authenticatietool als de doeldienst beheert is een architecturekeuze die transparantie verdient. Dit staat niet vermeld in de privacyverklaring.

Bevinding 8 — DPIA-status: 8 jaar AVG, geen conforme DPIA gepubliceerd

KRITIEK

DigiD heeft van 2018 tot minimaal 2023 gefunctioneerd zonder een geldige AVG-conforme DPIA. De beloofde nieuwe DPIA is niet aangetroffen in het AVG-register van de Rijksoverheid.

Periode	Situatie	AVG-compliant?
Dec 2017	Twee PIAs gepubliceerd — onder de Wbp, vóór AVG	Nee: Wbp-PIA ≠ AVG DPIA
Mei 2018	AVG treedt in werking — DPIA verplicht voor hoog risico	Geen DPIA uitgevoerd
2018–2023	Eigen erkenning: 'PIA's gaven voldoende inzicht'	Vijf jaar structurele schending
2023	Besluit tot nieuwe DPIA bij invoering WDO	In voorbereiding
17 april 2026	DPIA beloofd in AVG-register	Niet aangetroffen

Waarom vijf jaar zonder DPIA een kritieke schending is

AVG art. 35(1) verplicht een DPIA voor verwerkingen die waarschijnlijk een hoog risico inhouden. DigiD verwerkt het BSN van 17+ miljoen Nederlanders in een centrale authenticatiedienst voor de gehele overheid. De AP heeft in haar verplichte DPIA-lijst overheidsauthenticatiesystemen expliciet opgenomen.

Logius erkent dit zelf in het document: 'Na invoering van de AVG, in 2018, is er niet direct een nieuwe DPIA uitgevoerd, omdat de eerder uitgevoerde PIA's voldoende inzicht gaven.' Dat is een onderschatting van de AVG-vereisten.

De 2017 PIAs zijn geen geldige AVG DPIA

De twee gepubliceerde PIAs (DigiD Substantieel en DigiD Hoog, Mazars, 21 december 2017) zijn opgesteld onder de Wbp, vijf maanden vóór de AVG. Ze gebruiken Wbp-terminologie en de NOREA PIA-methodiek. Een Wbp-PIA is geen AVG DPIA: format, diepgang, consultatieverplichting (FG en eventueel AP) en beoordelingscriteria zijn wezenlijk anders.

De 2017 PIA-claim over Piwik is aantoonbaar onjuist gebleken

De 2017 PIA stelt expliciet over de Piwik-implementatie op de website:

> *"De gegevens zullen niet te herleiden zijn naar een persoon."*

In 2026 bewijst onze HAR-analyse technisch het tegendeel: _pk_id is een persistent cross-session identifier met een timestamp van het eerste bezoek. De PIA-belofte is nooit gerealiseerd. De PIA is nooit bijgewerkt om de feitelijke implementatie te weerspiegelen.

Dit illustreert structureel het probleem: privacydocumentatie wordt opgesteld als momentopname en vervolgens niet actueel gehouden, terwijl de werkelijke technische implementatie doorontwikkelt.

Bevinding 9 — Tegenstrijdigheden in officiële documentatie

ERNSTIG Op meerdere punten spreken de officiële DigiD-documenten zichzelf of de technische realiteit tegen.

Document	Wat het stelt	Tegenstrijdigheid (aangetoond)
Privacyverklaring §5	'Anoniem visitor-id, niet herleidbaar'	HAR: persistent ID + timestamp + browserfingerprint
Privacyverklaring §6	Solvinity niet als ontvanger vermeld	FAQ digid.nl: Solvinity 'verwerkt IP en e-mail'
Privacyverklaring §7	'Beheerd door Logius, niet buiten EU'	Solvinity beheert infra; Kyndryl-overname → CLOUD Act
Omgevingsmodel DPIA	11 partijen in diagram	Solvinity (centrale infra) ontbreekt volledig
digid.nl/solvinity	'Solvinity is leverancier, niet eigenaar'	Intern onderzoek: Solvinity heeft toegang tot MijnOverheid-data
digid.nl/solvinity	'DigiD voldoet aan strenge privacyeisen'	Tracking zonder consent, ontbrekende DPIA, anonieme verwerkers
digid.nl/solvinity	'DigiD is niet verplicht'	Vereist voor belasting, zorg, DUO, gemeenten, woning

DEEL IV

Juridische analyse

Welke wettelijke verplichtingen zijn geschonden en hoe ernstig

Juridische analyse

Telecommunicatiewet art. 11.7a — Cookiewet

Dit is de sterkste en meest direct aantoonbare schending. Art. 11.7a Tw vereist ondubbelzinnige toestemming vóór het plaatsen van cookies die niet strikt noodzakelijk zijn voor de gevraagde dienst.

- _pk_id (13 maanden, persistent ID): niet functioneel noodzakelijk voor authenticatie
- _pk_ses: niet functioneel noodzakelijk
- Beide worden gezet bij eerste bezoek, vóór enige interactie of toestemming
- Er is geen cookiebanner of consent-mechanisme aanwezig

De analytische-cookies-uitzondering van de AP is NIET van toepassing: die vereist dat er geen persistent cross-sessie-ID wordt aangemaakt. _pk_id maakt dat wel.

AVG art. 35 — DPIA-verplichting

DigiD verwerkt het BSN van 17+ miljoen Nederlanders in een centrale overheidsdienst. Dit valt categorisch onder 'hoog risico'. Van mei 2018 tot minimaal 2023 ontbrak een geldige AVG DPIA. Dit is een structurele, langdurige schending van AVG art. 35.

AVG art. 13(1)(e) — Informatieplicht over ontvangers

Solvinity, Matomo, Sentry en KCM zijn niet vermeld als ontvangers in de privacyverklaring. Betrokkenen zijn daarmee niet geïnformeerd over wie hun gegevens verwerkt.

AVG art. 28 — Verwerkersovereenkomsten

Voor elke verwerker is een schriftelijke verwerkersovereenkomst verplicht. Of overeenkomsten bestaan voor Solvinity, Sentry en KCM is publiek niet verifiëbaar. De afwezigheid uit alle gepubliceerde documentatie is een significant transparantiegebrek.

AVG art. 30 — Verwerkingsregister

Het verwerkingsregister (gegevensverwerkingsdocumentatie) is incompleet: Solvinity, Matomo, Sentry en KCM ontbreken als verwerkingspartijen.

AVG art. 5(1)(a) — Transparantiebeginsel

De combinatie van onjuiste claims in privacyverklaring en PIA, ontbrekende vermelding van verwerkers, en het uitblijven van een conforme DPIA vormt een structureel transparantiegebrek.

Wat dit onderzoek NIET bewijst

Bewering	Status	Toelichting
DigiD stuurt BSN naar Matomo	Niet aangetoond	HAR: trackingpixel bevat geen BSN
Sentry is extern commercieel risico	Genuanceerd	sentry.dtnr.nl is overheidsdomein; risico eerder beperkt
Matomo is een externe partij	Onjuist gebleken	statistiek.digid.nl is first-party subdomein
Session cookies zijn onbeveiligd	Niet bevestigd	HAR is onbetrouwbaar voor cookie-flags; vereist header-inspectie
DigiD schendt bewust de AVG	Niet aangetoond	Geen bewijs van opzet; kan implementatiefout zijn
Solvinity heeft een verwerkersovereenkomst	Onbekend	Bestaat mogelijk intern; publiek niet verifiëbaar

DEEL V

Conclusies en aanbevelingen

Wat gevraagd wordt van Logius, de toezichthouder en de politiek

Conclusies

DigiD heeft twee structurele privacyproblemen die naast elkaar bestaan en beide aandacht verdienen:

1. Technische implementatie: tracking zonder toestemming

De implementatie van Matomo op digid.nl — inclusief de inlogpagina en de volledige authenticatieketen — is technisch aantoonbaar in strijd met de Telecommunicatiewet. Dit is het concrete, direct bewijsbare probleem dat de AP direct kan beoordelen.

2. Documentair: onvolledige en verouderde privacydocumentatie

De gegevensverwerkingsdocumentatie vermeldt sleutelverwerkers niet, de privacyverklaring bevat aantoonbaar onjuiste claims, en de DPIA is vijf jaar lang uitgebleven. Dit is een structureel governance-probleem dat los staat van de technische tracking-kwestie.

Beide problemen zijn reeds decennia-oud of recent ontstaan — maar het feit dat ze op 17 april 2026, bijna negen jaar na de invoering van de AVG, aantoonbaar zijn, is verontrustend voor een dienst die de identiteitsinfrastructuur van Nederland vormt.

Aanbevelingen

Aan Logius / DigiD

- Implementeer direct een consent-mechanisme voor Matomo. Overweeg Matomo in privacy-vriendelijke modus te configureren (geen persistent ID, IP-anonimisering, geen cross-session tracking) zodat de analytische-cookies-uitzondering van toepassing is.
- Voeg Solvinity, Sentry en KCM expliciet toe aan de privacyverklaring als ontvangers en aan het verwerkingsregister als verwerkers.
- Publiceer de beloofde nieuwe AVG-conforme DPIA in het AVG-register van de Rijksoverheid.
- Verifiëeer en publiceer verwerkersovereenkomsten met alle partijen in de verwerkingsketen, inclusief Solvinity.
- Update de privacyverklaring om de feitelijke Matomo-implementatie correct te beschrijven.
- Voer een directe HTTP-header-inspectie uit op de _session_id cookie om te verifiëren of HttpOnly en Secure flags correct zijn ingesteld.

Aan de Autoriteit Persoonsgegevens

- Onderzoek of de huidige Matomo-implementatie (persistent ID, geen consent) voldoet aan de analytische-cookies-uitzondering of een andere grondslag vereist.
- Vraag Logius om aantoonbaarheid van verwerkersovereenkomsten met Solvinity, Sentry en KCM.
- Beoordeel of het vijf jaar ontbreken van een AVG DPIA een handhavingsplichtige situatie is.

Aan de Tweede Kamer

- Stel vragen over de Solvinity/Kyndryl-overname en de CLOUD Act-implicaties.
- Vraag om een onafhankelijke audit van de DigiD-privacyimplementatie, inclusief alle actieve tracking-tools.
- Overweeg wetgeving die eist dat privacy-documentatie voor kritieke nationale authenticatiediensten actief wordt bijgehouden en gepubliceerd.

Bronnen en bewijsmateriaal

Verzameld bewijsmateriaal

Bestand	Type	Inhoud
cookies_beforeconsent_.png	Screenshot	Storage Inspector www.digid.nl: _pk_id en _pk_ses bij eerste bezoek
matomo_.png	Screenshot	Network-tab: statistiek.digid.nl/matomo.js en beacon-request
digid_n-inloggen.png	Screenshot	Inlogpagina network-tab: trackingpixel request zichtbaar
digid_inloggen_cookies_noconsent.png	Screenshot	Cookie-overzicht inlogpagina incl. Matomo cookies
mfa_digid_assets.png	Screenshot	Debugger MFA-pagina: analytics.js + piwik.js geladen
mijn_digid.png	Screenshot	mijn.digid.nl dashboard: matomo.js + piwik.js in network-tab
trackpageview_.png	Screenshot	Broncode analytics.js: trackPageView() zonder consent-check
non-digid-domeinen-nonconsent.png	Screenshot	Activatiepagina: kcmg.nl, sentry.dtnr.nl en statistiek zichtbaar
solvinity.png	Screenshot	DigiD architectuurdiagram + FAQ-tekst 'verwerkt door Solvinity'
1776385714817_image.png	Screenshot	DigiD FAQ: 'Welke persoonsgegevens worden verwerkt door Solvinity?'
1776385927621_image.png	Screenshot	Omgevingsmodel DigiD: Solvinity ontbreekt in het diagram
digid-inloggen.har	HAR-bestand	Volledige inlogflow: 20 requests, Matomo pixel parameters
Privacy___DigiD.html	HTML-broncode	Privacyverklaring digid.nl incl. tegenstrijdige claims
Logius___Gegevensverwerkingen_DigiD.html	HTML-broncode	Officiële verwerkingsdocumentatie + Sentry DSN in broncode
PIA DigiD Hoog (Mazars, 21 dec 2017)	PDF	Pre-AVG PIA; Piwik-claim aantoonbaar onjuist in 2026
Autorisatiebesluit BRP voor DigiD (18 juli 2024)	Staatscourant	Formele BRP-autorisatie; bevestigt verwerkingsbereik
NOS-artikel 16 apr 2026	Nieuwsbron	Intern onderzoek: Solvinity kan bij MijnOverheid-data
preloaderroronfirstlaunch.png	Screenshot	Network-tab 63 requests homepage + console errors
logius_cookies_wo_cons.png	Screenshot	Logius.nl: pk_id, pk_ses, stg_* cookies zonder consent

Relevante wet- en regelgeving

- Telecommunicatiewet art. 11.7a (cookiewet Nederland)
- AVG art. 5, 13, 28, 30, 35 (Verordening (EU) 2016/679)
- AP-richtsnoeren analytische cookies (2023)
- Wet Digitale Overheid (WDO) 2023

Externe verificatie

- dtnr.nl: 'geregistreerd voor de Nederlandse Rijksoverheid' — bevestigt overheidshosting Sentry
- KCM Group BV / kcmsurvey.eu — bevestigt commerciële derde-partij status
- NOS.nl, 16 april 2026: Solvinity/Kyndryl CLOUD Act-risico via intern Logius-onderzoek

Dit rapport is opgesteld op 17 april 2026 op basis van eigen technisch onderzoek door Mick Beer (mickbeer.com). Bevindingen zijn voorzien van een eerlijkheidsoordeel. Technisch bewijs is beschikbaar op verzoek.