HACKEDEMIA

Dossier 113.nl

Privacy-onderzoek op de website van Stichting 113 Zelfmoordpreventie

Dit dossier documenteert de bevindingen van een onafhankelijk privacy-onderzoek op de website van Stichting 113 Zelfmoordpreventie (113.nl). Het bevat de eerste meting van 9 mei 2026, de herhalingsmeting van 11 mei 2026 na de publieke respons van 113, de juridische context, en het verloop van de constructive disclosure.

Alle bevindingen zijn cryptografisch verifieerbaar via SHA-256 en de oorspronkelijke scan-output is verankerd via OpenTimestamps op de Bitcoin-blockchain. Raw scan-data is op 12 mei 2026 met 113 gedeeld voor onafhankelijke verificatie.

Onderzoeker	Mick Beer, maatschappelijk hacker
Organisatie	Hackedemia (hackedemia.nl)
Domein	113.nl
Subject	Stichting 113 Zelfmoordpreventie
Dossier-klasse	ORANJE
Eerste meting	9 mei 2026, 23:49 UTC · scanner v3.7
Herhalingsmeting	11 mei 2026, 20:15 · scanner v3.8
LinkedIn-publicatie	9 mei 2026 (post 1/9)
Respons 113	binnen enkele uren publiek
Microsoft Clarity	verwijderd (bevestigd 11 mei)
Overige bevindingen	6 ernstig, ongewijzigd
Documentversie	1.0 · 12 mei 2026

Wat overkomt een bezoeker op 113.nl

Hieronder schematisch de dataflow van een gemiddeld bezoek aan 113.nl. Het beeld toont in één oogopslag wat een bezoeker overkomt en waar diens data terechtkomt: vóór de cookiebanner is geklikt, bij een klik op "weigeren", en bij een klik op "toestaan".

Alle elementen in het diagram zijn direct uit de scan-output van 9 mei 2026 afgeleid. De status van Microsoft Clarity (rood gemarkeerd) reflecteert de re-scan van 11 mei 2026: Stichting 113 heeft Clarity tussen 9 en 11 mei verwijderd, alle andere bevindingen zijn ongewijzigd.

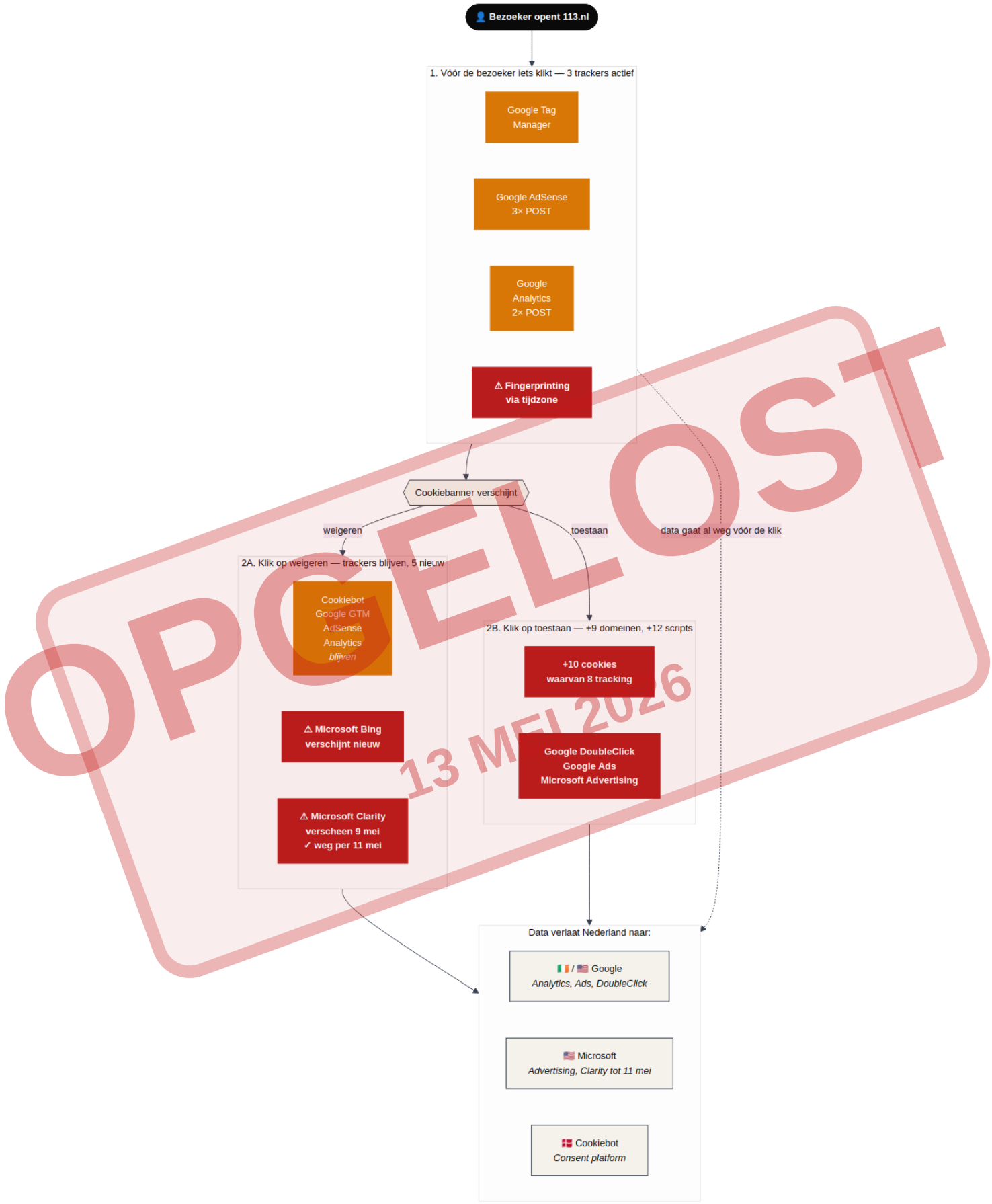
Hoe het diagram te lezen

Oranje blokken: trackers die actief zijn zonder dat de bezoeker daartoe geldige toestemming heeft gegeven. Functioneel oké of gangbaar, maar onder Tw artikel 11.7a en de AVG niet zonder consent toegestaan.

Rode blokken: bevindingen die in het rapport als ernstig worden gemarkeerd — ofwel omdat er actief data wordt verzonden, ofwel omdat een tracker verschijnt ná een uitdrukkelijke weiger-klik.

Beige blokken: de bestemming van de data. Onder de bestemming is steeds aangegeven welke diensten van die partij worden ingezet.

Stippellijn: data die het systeem al verlaat vóórdat de bezoeker iets heeft kunnen klikken. Dat is het kernpunt van bevinding 2 in het rapport.



***Oranje**: tracker actief zonder geldige toestemming. **Rood**: ernstig ten opzichte van AVG, of nieuw toegevoegd na een weiger-klik. **Beige**: bestemming van de data. De getallen (3 trackers vóór klik, 5 POST-requests, 5 nieuwe domeinen na weigeren, +12 scripts na toestaan) zijn direct uit de scan-output.*

1. Samenvatting

ERNSTIG OPGELOST	6 ERNSTIG OPENSTAAND	2 AANDACHTSPUNTEN

Op 9 mei 2026 werd op 113.nl een meting uitgevoerd in drie modi: zonder klik op de cookiebanner (NOOP), na klik op "alles weigeren" (REFUSE), en na klik op "alles toestaan" (ACCEPT). De meting legde acht bevindingen vast, waarvan zes als ernstig zijn geclassificeerd en twee als aandachtspunt. Daarnaast verscheen Microsoft Clarity (screen-recording) na een weiger-klik, hetgeen op een suïcidepreventielijn als een bijzonder zwaar punt wordt aangemerkt vanwege de bescherming die de AVG kent voor gezondheidsgegevens.

Op 9 mei werd een LinkedIn-publicatie gedaan over deze bevinding op 113.nl. Stichting 113 Zelfmoordpreventie heeft binnen enkele uren publiek gereageerd, een intern onderzoek gestart, externe deskundigen ingeschakeld, en Microsoft Clarity van de website verwijderd. Een herhalingsmeting op 11 mei 2026 bevestigt dat Clarity uit de scan-output is verdwenen.

De zes overige ernstige bevindingen zijn op 11 mei ongewijzigd t.o.v. 9 mei. Stichting 113 Zelfmoordpreventie heeft aangekondigd dat hun onderzoek doorloopt. De raw scan-data van beide metingen is op 12 mei 2026 met 113 gedeeld voor onafhankelijke verificatie. Een tweede onderzoekscyclus is voorzien rond 9 juni 2026 om verdere verbetering aantoonbaar te maken.

> **Stichting 113 Zelfmoordpreventie als constructief sector-voorbeeld.** De snelheid en transparantie van de respons is van uitzonderlijk niveau in de Nederlandse hulpverleningssector. Geen advocatenbrief, geen ontkenning; wel publiek erkennen, intern onderzoek, externe deskundigen inschakelen, en feitelijke verwijdering van de meest aansprekende bevinding. Het rapport-voorwoord van Hackedemia stelt dat geen van de onderzochte organisaties moedwillig veroorzaker is van het gedocumenteerde patroon. Stichting 113 bevestigt deze stelling door snel en constructief te handelen.

2. Identificatie

Domein	113.nl
Organisatie	Stichting 113 Zelfmoordpreventie
Doelgroep	Mensen met suïcidale gedachten · mensen die zich zorgen maken om een ander · nabestaanden van suïcide
Klasse in dossier	ORANJE
Scan-datum (UTC)	2026-05-09T23:49:41 (eerste meting) · 2026-05-11T20:15:55 (herhalingsmeting)
Scanner-versie	v3.7 (eerste meting) · v3.8 (herhalingsmeting) · modi: noop, refuse, accept
Sanity-check	Compleet voor beide metingen
Raw scan-bestand	`runs/2026-05-09_forensisch_v3.7_v2/113.nl_20260509_234941.json`
SHA-256 scan-JSON	`ab4ffe91a233e37c30604581da789e2db735788e682019c91449aa506be2e4f0`
OpenTimestamps-proof	Aanwezig voor eerste meting (`…234941.json.ots`) · Bitcoin-blockchain
HAR-archief	`113.nl_har_20260509_234933.har` (eerste meting) · `113.nl_har_20260511.har` (herhaling)

SHA-256 raw scan-data leveringspakket (12 mei 2026):

```
cf3f2dcc06c0e4f65e04835817287a6e89ff153e1254eaad503dc5b97d44f6b1
```

Bestand: `113-rawdata-20260511.zip` · 88 KB · 10 bestanden in manifest · Geleverd aan Stichting 113 Zelfmoordpreventie op 12 mei 2026 voor onafhankelijke verificatie via SHA-256 en OpenTimestamps.

3. Functionele context en AVG-raakvlak

De website 113.nl is de digitale voordeur van Stichting 113 Zelfmoordpreventie. Bezoekers van de site zoeken contact in een context die direct raakt aan hun geestelijke gezondheid: suïcidale gedachten, zorgen om een naaste, of het verwerken van het verlies van een dierbare door zelfdoding.

AVG-specifieke aandachtspunten

- **Artikel 9 lid 1 — bijzondere persoonsgegevens (gezondheid):** Suïcidaliteit is een gegeven over de geestelijke gezondheid van de betrokkene. Het laden van de hulppagina of het openen van het chat- of bel-menu is op zichzelf al een afgeleid bijzonder persoonsgegeven.
- **Artikel 35 — DPIA-plicht:** De verwerking is hoog-risico vanwege de aard van de bijzondere persoonsgegevens en de kwetsbare doelgroep. Een Data Protection Impact Assessment is wettelijk vereist voordat dergelijke verwerkingen worden gestart.
- **Artikel 8 — minderjarigen:** Hoewel niet primaire doelgroep, kunnen minderjarige bezoekers (onder de zestien) de site bereiken. Voor hen geldt aanvullende bescherming en de eis van ouderlijke toestemming bij verwerking op grond van toestemming.

Wat is op 113.nl functioneel waarneembaar

Functioneel element	Aanwezigheid en context
Session-recording (screen replay)	Niet gedetecteerd vóór consent. Verscheen wel ná klik op "weigeren" door verkeerd geconfigureerde Consent API (Microsoft Clarity). **Verwijderd per 11 mei 2026.**
Heatmaps / behavior-tracking	Geen losse heatmap-tool (Crazy Egg, Decibel) gedetecteerd. Heatmap-functionaliteit binnen GA4/GTM is niet apart gemeten.
Formulier-tracking	Google Tag Manager kan form-submit-triggers en veldwaarden doorgeven aan GA4 en Google Ads. De gtm.js bevat endpoints `…/pagead/form-data` en `…/ccm/form-data` (Google's formulier-data-uploadkanaal). Activatie op dit domein: nog te verifieren in productie.
Fingerprinting-indicatoren	Tijdzone-uitlezing aanwezig in code van `www.googletagmanager.com` . Geen losse commerciële fingerprint-dienst (FingerprintJS).
Marketing pixels	Vóór consent: `pagead2.googlesyndication.com` (Google Ads / DoubleClick). Ná "alles toestaan" bovendien: Google Ads server-side, Google Ads / DoubleClick, Microsoft Advertising (UET).
Analytics + tag managers	Vóór consent: Google Tag Manager + Google Analytics 4. Acht tracker-identifiers in scripts: `siteId 58479` , `GTM-5N44BF4` , `GTM-MQ7B2P5` , `G A4 G-NSYB6F1YZJ` , `GA4 G-9LJGQ20WLQ` , `UA-10657158-3` , `AW-793289595` , `AW-938136512` .
Foutmonitoring / performance	Geen externe error- of performance-monitoring (Sentry, New Relic, Datadog, Azure App Insights) gedetecteerd.
Externe chat- of supportwidgets	Geen externe widget-infrastructuur van een derde gedetecteerd.

4. Methodologie

Scanopzet

De website 113.nl is gescand in drie afzonderlijke consent-modi, met telkens een schone browser-context (geen cookies, geen storage, geen voorafgaande sessie):

- **NOOP**: bezoek aan 113.nl zonder enige interactie met de cookiebanner. Doel: wat laadt by-default, voor de bezoeker zelfs maar een klik heeft kunnen geven.
- **REFUSE**: bezoek aan 113.nl en klik op "alles weigeren" (Cookiebot-knop `#CybotCookiebotDialogBodyButtonDecline`). Doel: wat blijft of begint te laden ná een actieve weigering.
- **ACCEPT**: bezoek aan 113.nl en klik op "alles toestaan". Doel: wat laadt bij volle toestemming, als referentiemodus.

Per modus zijn vastgelegd: alle externe netwerk-requests (URL, methode, status, body), alle gezette cookies (naam, domein, levensduur, secure-vlag, httpOnly-vlag, SameSite), de DOM-staat, scripts die in het document zijn ingeladen, en geconstateerde fingerprinting-indicatoren zoals tijdzone-uitlezing en canvas-rendering.

Technische uitvoering

Engine	Playwright 1.59.1 op Chromium
User-Agent	Chrome/130.0.0.0
Viewport	1280 × 720 pixels
Tijdzone	Europe/Amsterdam
Taal	nl-NL
Wachtcriterium	networkidle (alle requests afgerond)
Sandbox-modus	Ingeschakeld; scriptuitvoering toegestaan

Verificatie

Voor elke meting is een SHA-256 hash gegenereerd over alle uitvoer-bestanden (JSON, HAR, cookie-store, samenvattingsrapport). Voor de eerste meting van 9 mei 2026 is daarnaast een OpenTimestamps-stempel aangevraagd, waarmee het bestaan van de gemeten data per die datum verifieerbaar wordt op de Bitcoin-blockchain. Het raw-data leveringspakket dat op 12 mei 2026 met Stichting 113 Zelfmoordpreventie is gedeeld, bevat een MANIFEST.sha256 plus de oorspronkelijke .ots-bestanden.

Beperkingen van het onderzoek

Dit onderzoek meet wat een willekeurige bezoeker op het moment van scannen op 113.nl zou ervaren in de browser. Het meet géén achterliggende verwerkingen op de servers van Stichting 113 of van derde-partijen, geen interne dataretentie-instellingen, en geen verwerkingsovereenkomsten. De juridische beoordeling van de bevindingen is voorbehouden aan rechter, toezichthouder en juridisch specialisten. Hackedemia documenteert wat gemeten is en koppelt het aan het geldende wettelijke kader.

5. Bevindingen — overzicht

De acht bevindingen van 9 mei 2026, met huidige status na de herhalingsmeting van 11 mei 2026. Zes zijn als ernstig geclassificeerd, twee als aandachtspunt. Een ernstige bevinding (Microsoft Clarity-screenrecording na weiger-klik) is door 113 verwijderd voordat de herhalingsmeting werd uitgevoerd.

Nr.	Bevinding	Ernst	Status 11 mei	Wetsartikel / norm
1	Microsoft Clarity (screen-recording) actief ná klik op weigeren door verkeerd geconfigureerde Consent API	ERNSTIG	✓ Verwijderd	AVG 6, 7(3), 9 · Tw 11.7a
2	Google Tag Manager, Google AdSense en Google Analytics geladen vóór enige consent	ERNSTIG	Ongewijzigd	Tw 11.7a · AVG 6, 28
3	Vijf bekende trackers blijven actief ná klik op weigeren (Cookiebot, GTM, AdSense, Analytics)	ERNSTIG	Ongewijzigd	Tw 11.7a · AVG 7(3)
4	Eén tracker-script (`gtm.js?id=GTM-MQ7B2P5`) blijft geladen ná weigeren	ERNSTIG	Ongewijzigd	Tw 11.7a
5	Vijf POST-requests naar third-parties met body (3× Google AdSense, 2× Google Analytics)	ERNSTIG	Ongewijzigd	AVG 6, 9, 28
6	Vijf tracker-bestanden bevatten fingerprinting-indicatoren (tijdzone-uitlezing)	ERNSTIG	Ongewijzigd	AVG 9 (mogelijk), 13 · EDPB GL 02/2023
7	Obfuscatie-patroon (`atob + eval/Function`) in tracker-bestand bemoeilijkt controle	ERNSTIG	Ongewijzigd	AVG 5(1)(a)
L1	Referrer-Policy ingesteld op `no-referrer-when-downgrade` — mogelijke URL-lekkage	LET OP	Ongewijzigd	AVG 32 (beveiliging)
L2	Acht unieke tracker-identifiers in scriptinhoud — verifieer registratie in AVG-register / privacyverklaring	LET OP	Ongewijzigd	AVG 30 · Fashion ID (HvJ-EU 2019)

Totaaltelling 9 mei 2026 en 11 mei 2026: 0 kritiek · 6 ernstig (ongewijzigd) · 2 let-op. Bevinding 1 (Microsoft Clarity) is per 11 mei verwijderd.

6. Per-modus vergelijking (9 mei 2026)

De drie consent-modi laten zien wat de werkelijke uitwerking is van de cookiebanner op 113.nl. Een bezoeker die op "weigeren" klikt, komt in een ander beeld terecht dan een bezoeker die niets klikt — niet doordat trackers verdwijnen, maar doordat er bij blijven en nieuwe verschijnen.

NOOP — bezoek zonder klik

- Cookies: 2 totaal · 0 als tracking-cookie geclassificeerd
- Geladen tracker-scripts: 5
- Third-party domeinen actief: 5
- Cookiebanner zichtbaar bij paginalaad: **nee** (CMP in DOM: CookiePro/OneTrust + Cookiebot)

Cookies geplaatst vóór consent

Naam	Domein	Levensduur	Secure	SameSite	Tracking?
`gtm_pageview_count`	www.113.nl	sessie	nee	Lax	nee
`gtm_active_time`	www.113.nl	sessie	nee	Lax	nee

POST-requests met body (actieve dataverzending)

Endpoint	Method	Body	Tracker
`pagead2.googlesyndication.com/ccm/collect`	POST	0 B (beacon)	Google AdSense
`pagead2.googlesyndication.com/ccm/collect`	POST	0 B (beacon)	Google AdSense
`pagead2.googlesyndication.com/ccm/collect`	POST	0 B (beacon)	Google AdSense
`region1.google-analytics.com/g/collect`	POST	0 B (beacon)	Google Analytics
`region1.google-analytics.com/g/collect`	POST	227 B (text/plain)	Google Analytics

REFUSE — na klik op "alles weigeren"

- Cookiebanner zichtbaar bij paginalaad: **nee**
- Weiger-actie uitgevoerd op: `#CybotCookiebotDialogBodyButtonDecline`
- Tracking-cookies ná weigeren: 0
- Tracker-scripts ná weigeren: 1 blijft geladen (`gtm.js?id=GTM-MQ7B2P5`)
- Bekende trackers vóór weigeren: 3 — ná weigeren: 10 (5 blijvend, 5 nieuw verschenen)

Trackers die blijven bestaan ná weigeren

- `consent.cookiebot.com`
- `consentcdn.cookiebot.com`
- `googletagmanager.com`
- `pagead2.googlesyndication.com`
- `region1.google-analytics.com`

Trackers die nieuw verschijnen ná weigeren (9 mei)

- `bat.bing.com` (Microsoft Advertising)
- `bat.bing.net` (Microsoft Advertising)
- `clarity.ms` (Microsoft Clarity — screen-recording) → verwijderd per 11 mei
- `i.clarity.ms` (Microsoft Clarity) → verwijderd per 11 mei
- `scripts.clarity.ms` (Microsoft Clarity) → verwijderd per 11 mei

> **Conclusie REFUSE-modus.** De weiger-klik op 113.nl is in zijn werking cosmetisch. Na klik op "alles weigeren" blijven nul tracking-cookies bestaan, maar er blijft één tracker-script geladen en vijf bekende tracker-domeinen blijven actief. Bovendien verschijnen vijf nieuwe tracker-domeinen ná de weiger-klik — waaronder Microsoft Clarity (screen-recording) in de oorspronkelijke meting van 9 mei. Er verdwijnt feitelijk niets, en er komen trackers bij. Dit raakt direct AVG artikel 7 lid 3, dat verlangt dat intrekken van toestemming even eenvoudig is als het geven ervan.

ACCEPT — na klik op "alles toestaan"

In ACCEPT-modus is sprake van een kwantitatieve explosie ten opzichte van NOOP. Toegevoegd worden tien cookies (waarvan acht als tracking-cookie te classificeren), negen extra tracker-domeinen, en twaalf extra tracker-scripts.

Nieuw verschenen tracker-domeinen in ACCEPT-modus

- `bat.bing.com` (Microsoft Advertising)
- `clarity.ms` (Microsoft Clarity) → verwijderd per 11 mei
- `i.clarity.ms` · `scripts.clarity.ms` → verwijderd per 11 mei
- `google.com` · `google.nl` (search-/advertising-infrastructuur)
- `googleads.g.doubleclick.net` (DoubleClick / Google Ads)
- `region1.analytics.google.com` (Google Analytics)
- `stats.g.doubleclick.net` (DoubleClick)

7. Bevindingen — gedetailleerd

Hieronder de bevindingen op volgorde van ernst, met onderbouwing per bevinding, plus het wettelijke kader. Bevinding 1 (Microsoft Clarity) is per 11 mei 2026 door Stichting 113 Zelfmoordpreventie verwijderd. Bevindingen 2 t/m 7 zijn op het moment van schrijven (12 mei 2026) ongewijzigd.

1. Microsoft Clarity (screen-recording) actief ná klik op weigeren

ERNSTIG ✓ Verwijderd per 11 mei 2026 · AVG 6 · 7(3) · 9 · Tw 11.7a

Microsoft Clarity is een session-replay-tool die muisbewegingen, kliks, scrollgedrag en in veel gevallen formulier-invoer kan registreren — vóórdat het formulier wordt verzonden. In de oorspronkelijke meting van 9 mei 2026 is geconstateerd dat na klik op "alles weigeren" de drie Clarity-domeinen (`clarity.ms` , `i.clarity.ms` , `scripts.clarity.ms`) alsnog werden geladen. Deze configuratie is in strijd met Tw artikel 11.7a en AVG artikel 7 lid 3.

De directe oorzaak is een verkeerd geconfigureerde Consent API: het consent-event werd getriggerd door elke knop in de cookiebanner, niet enkel door de accept-knop, waardoor een weiger-klik dezelfde uitkomst opleverde als een accept-klik. Bij een bezoeker op een suïcidepreventielijn is dit bijzonder ernstig vanwege de aard van de bijzondere persoonsgegevens (AVG artikel 9).

Op 11 mei 2026 is in een herhalingsmeting bevestigd dat Microsoft Clarity is verwijderd: de Clarity-domeinen verschijnen niet meer in de scan-output. Bevinding opgelost.

OPGELOST 13 MEI 2026

2. Google Tag Manager, AdSense en Analytics geladen vóór enige consent

ERNSTIG · Tw 11.7a · AVG 6, 28

In NOOP-modus — een bezoek zonder enige interactie met de cookiebanner — zijn drie externe trackers actief vóór toestemming: `googletagmanager.com` , `pagead2.googlesyndication.com` (Google AdSense) en `region1.google-analytics.com` (Google Analytics).

Telecommunicatiewet artikel 11.7a vereist sinds 2009 dat voor het plaatsen van zulke trackers eerst toestemming is gegeven. Nederlandse rechters hebben dit patroon — tracking-zonder-geldige-toestemming bij commerciële adtech-praktijken — in een reeks kort gedingen tussen 2023 en 2025 onrechtmatig geoordeeld. De Autoriteit Persoonsgegevens heeft in april 2025 vijftig organisaties gewaarschuwd over deze configuratie, met dreiging van handhaving binnen drie maanden.

3. Tracking blijft actief ná klik op weigeren

ERNSTIG · Tw 11.7a · AVG 7(3)

Ná klik op "alles weigeren" blijven vijf bekende tracker-domeinen actief op 113.nl: `consent.cookiebot.com`, `consentcdn.cookiebot.com`, `googletagmanager.com`, `pagead2.googlesyndication.com` en `region1.google-analytics.com`. Bovendien verschijnen er trackers nieuw, waaronder in de oorspronkelijke meting Microsoft Clarity.

AVG artikel 7 lid 3 stelt: "Het intrekken van de toestemming is even eenvoudig als het geven ervan." Wanneer een weiger-klik niet leidt tot het uitschakelen van tracking, is van een rechtsgeldige intrekking geen sprake.

4. Tracker-script `gtm.js` blijft geladen ná weigeren

ERNSTIG · Tw 11.7a

Het script `gtm.js?id=GTM-MQ7B2P5` wordt na klik op "alles weigeren" niet uitgeschakeld of opnieuw geladen, en blijft als geladen script in het document aanwezig. Hiermee kan via de Google Tag Manager nog steeds gedrag worden gemeten zonder dat de wettelijk vereiste toestemming voorhanden is.

5. Vijf POST-requests met body naar third-parties

ERNSTIG · AVG 6, 9, 28

Tijdens een bezoek aan 113.nl worden vijf POST-requests naar externe partijen verstuurd: drie naar `pagead2.googlesyndication.com` (Google AdSense) en twee naar `region1.google-analytics.com` (Google Analytics). Daarvan bevatten vier een leeg beacon-frame en één een body van 227 bytes (`text/plain`). Dit is geen passieve telling maar actieve dataverzending.

In de context van een bezoek aan een suïcidepreventielijn raakt deze verwerking mogelijk aan AVG artikel 9 (bijzondere persoonsgegevens). De juridische kwalificatie is voorbehouden aan rechter en toezichthouder.

6. Fingerprinting-indicator (tijdzone-uitlezing) in Google Tag Manager-bestanden

ERNSTIG · AVG 9 (mogelijk), 13 · EDPB Guidelines 02/2023

In vijf gedownloade tracker-bestanden van `www.googletagmanager.com` is tijdzone-uitlezing geconstateerd. Tijdzone-detectie is een bekend ingrediënt voor browser-fingerprinting: het stelt de aanbieder in staat een bezoeker te identificeren zonder gebruik te maken van expliciete cookies.

De European Data Protection Board (EDPB) heeft in Guidelines 02/2023 over de technische reikwijdte van artikel 5(3) ePrivacy-richtlijn vastgesteld dat fingerprinting onder dezelfde toestemmingsregels valt als cookies. Voorafgaande toestemming is vereist.

7. Obfuscatie-patroon in tracker-bestand

ERNSTIG · AVG 5(1)(a) — transparantie

In een bestand op `www.googletagmanager.com` is een combinatie van `atob` (base64-decodering) en `eval` / `Function` (dynamische code-uitvoering) aangetroffen. Deze combinatie is een bekend obfuscatie-patroon: code wordt uit base64-strings opgebouwd en pas op het moment van uitvoeren door de browser samengesteld, waardoor statische controle wordt bemoeilijkt.

AVG artikel 5 lid 1 onderdeel a vereist dat verwerking van persoonsgegevens "transparant" plaatsvindt. Code die zich tegen inzicht verzet, staat op gespannen voet met dat beginsel. De aanwezigheid is geen direct bewijs van kwade intentie, wel een signaal dat aanvullende controle vraagt.

Aandachtspunten

Code	Aandachtspunt	Wetsartikel / actie
L1	Referrer-Policy ingesteld op `no-referrer-when-downgrade`. Dit kan ertoe leiden dat URL-data (mogelijk inclusief query-parameters) met externe partijen wordt gedeeld.	AVG 32 (beveiliging) · advies: `same-origin` of `strict-origin-when-cross-origin`
L2	Acht unieke tracker-identifiers in scriptinhoud aangetroffen: `siteId 58479`, `GTM-5N44BF4`, `GTM-MQ7B2P5`, `GA4 G-NSYB6F1YZJ`, `GA4 G-9LJGQ20WLQ`, `UA-10657158-3`, `AW-793289595`, `AW-938136512`.	AVG 30 — verifieer registratie · Fashion ID (HvJ-EU C-40/17, 2019) — joint controllership

8. Juridische context

Geraakte wettelijke normen

Bepaling	Relevantie voor 113.nl
AVG art. 9 lid 1 (gezondheidsgegevens)	Suïcidaliteit is een gegeven over de geestelijke gezondheid. Het enkel bezoeken van de hulppagina kan reeds een afgeleid bijzonder persoonsgegeven opleveren. Verhoogde beschermingsgraad.
AVG art. 35 (DPIA-plicht)	De combinatie van bijzondere persoonsgegevens en een kwetsbare doelgroep maakt deze verwerking hoog-risico. Een DPIA is wettelijk vereist.
AVG art. 8 (minderjarigen)	Niet de primaire doelgroep, maar minderjarige bezoekers (onder de 16) kunnen de site bereiken. Voor hen geldt ouderlijke toestemming als grondslag voor tracking.
AVG art. 6 (rechtsgrond)	Geen geldige rechtsgrond voor tracking vóór of zonder toestemming. Gerechtvaardigd belang geldt niet voor marketing- of profileringscookies, zoals herhaaldelijk bevestigd in jurisprudentie.
AVG art. 7 lid 3 (intrekken)	"Het intrekken van de toestemming is even eenvoudig als het geven ervan." Bij 113.nl is intrekken niet alleen niet-werkend — het is actief contrair: er verschijnen trackers ná de weiger-klik.
AVG art. 13/30 (transparantie)	Verifieer of de acht tracker-identifiers expliciet in de privacyverklaring én in het verwerkingsregister staan vermeld.
AVG art. 26/28 (joint controllership / verwerker)	Fashion ID (HvJ-EU C-40/17, 2019) bepaalt dat een site-eigenaar die een derde via tracking laat meelezen, samen met die derde verantwoordelijk wordt onder de AVG voor de fase van verzameling en doorgifte. Bij 113.nl is dit van toepassing op meerdere derde-partijen.
Tw art. 11.7a (toestemming voor cookies)	Overtreding: bekende trackers laden vóór toestemming; geen banner zichtbaar bij paginalaad.

Jurisprudentie en richtsnoeren

De Nederlandse en Europese jurisprudentie op het gebied van tracking-cookies, joint controllership en toestemming geeft een consistent beeld. Hieronder de meest relevante uitspraken en richtsnoeren voor de bevindingen op 113.nl.

Bron	Kerngedachte voor 113.nl-bevindingen
Fashion ID HvJ-EU, C-40/17, 29 juli 2019	Joint controllership: een site-eigenaar die een derde via tracking laat meelezen, is samen met die derde verantwoordelijk in de zin van de AVG voor de fase van verzameling en doorgifte. Direct toepasbaar op 113.nl's verhouding tot Google en Microsoft.
Nederlandse adtech-jurisprudentie Hof en Rechtbank Amsterdam, 2023–2025	In een reeks kort gedingen tegen adtech-bedrijven (waaronder Criteo en Microsoft/LinkedIn/Xandr) hebben Nederlandse rechters geoordeeld dat het plaatsen van tracking-cookies zonder geldige voorafgaande toestemming onrechtmatig is, en dat ook de derde partij (niet alleen de site-eigenaar) verwerkingsverantwoordelijk is op grond van AVG artikel 26.
EDPB Guidelines 02/2023 European Data Protection Board, eind 2023	Fingerprinting-technieken — waaronder tijdzone-uitlezing — vallen onder dezelfde toestemmingsregels als cookies, op grond van artikel 5(3) ePrivacy-richtlijn. Voorafgaande toestemming is vereist.
AP cookie-handhavingsactie Autoriteit Persoonsgegevens, april 2025	Vijftig Nederlandse organisaties zijn formeel gewaarschuwd voor misleidende cookiebanners en het zonder geldige toestemming plaatsen van tracking-cookies. Drie maanden voor compliance, daarna handhaving en mogelijke boetes. De AP heeft per 2025 extra budget gekregen voor toezicht op tracking-technologie.
AP guidance op cookiewalls Autoriteit Persoonsgegevens, sinds 2019	De AP heeft sinds 2019 aangegeven dat cookiewalls — waarbij toegang tot een website afhankelijk wordt gemaakt van toestemming — niet voldoen aan het vrij-gegeven-toestemming-vereiste van de AVG.

Specifieke ECLI-nummers van relevante kort gedingen en aanvullende richtsnoeren zijn op verzoek beschikbaar bij Hackedemia. Voor toepassing op een individuele zaak wordt juridisch advies aanbevolen.

9. Verloop constructive disclosure

Hackedemia volgt voor dit onderzoek de werkwijze van constructive disclosure: bevindingen worden contact gezocht met de betrokken organisatie, ruimte voor reactie wordt geboden, publieke documentatie wordt voorzien van update-mogelijkheden, en raw scan-data is voor de betrokken organisatie verifieerbaar beschikbaar.

Het tijdsverloop met Stichting 113 Zelfmoordpreventie illustreert hoe deze werkwijze in de praktijk functioneert wanneer een organisatie constructief reageert.

9 mei 2026 23:49 UTC	Eerste scan op 113.nl uitgevoerd. Scanner v3.7, drie modi. Acht bevindingen vastgelegd. SHA-256 hash gegenereerd. OpenTimestamps-stempel aangevraagd voor verankering op de Bitcoin-blockchain.
9 mei 2026	LinkedIn-publicatie post 1/9 over Microsoft Clarity-bevinding op 113.nl. Cryptografische hash en methodologie publiek toegankelijk gemaakt op hackedemia.nl.
10 mei 2026 binnen enkele uren	Stichting 113 Zelfmoordpreventie reageert publiek onder de LinkedIn-post. Strekking van de reactie: dank voor het onder de aandacht brengen, intern onderzoek direct gestart, het betreffende onderdeel (Microsoft Clarity) is verwijderd, onderzoek naar werking en mogelijke impact loopt. 113 onderstreept dat privacy en zorgvuldigheid voorop staan.
11 mei 2026 20:15 UTC	Herhalingsmeting (re-scan) uitgevoerd op 113.nl met scanner v3.8. Bevestigd: Microsoft Clarity-domeinen (`clarity.ms` , `i.clarity.ms` , `scripts.clarity.ms`) komen in de scan-output van 11 mei niet meer voor. De zes overige ernstige bevindingen en twee aandachtspunten zijn ongewijzigd t.o.v. 9 mei.
11 mei 2026	Update geplaatst bovenaan de oorspronkelijke LinkedIn-post: "✓ 113 heeft Microsoft Clarity (screen-recording) verwijderd, re-scan vandaag bevestigt. Zes overige ernstige bevindingen onveranderd t.o.v. 9 mei; 113 heeft aangekondigd dat het onderzoek doorloopt."
12 mei 2026	Mail van Stichting 113 Zelfmoordpreventie ontvangen, waarin gevraagd wordt om de volledige raw scan-data inclusief technische onderbouwing voor onafhankelijke verificatie door externe deskundigen.
12 mei 2026	Raw-data leveringspakket samengesteld: scan-output 9 mei en 11 mei, HAR-bestanden, OpenTimestamps-bewijs, dossier, SHA-256 manifest, verificatie-instructies. Pakket cryptografisch verzegeld met hoofd-SHA-256 `cf3f2dcc06c0e4f65e04835817287a6e89ff153e1254eaad503dc5b97d44f6b1` en aan Stichting 113 Zelfmoordpreventie geleverd.
9 juni 2026 gepland	Tweede onderzoekscyclus voorzien om eventuele verdere verbeteringen aantoonbaar te maken voor publicatie in een vervolg-rapport.

10. Aanbevelingen aan Stichting 113 Zelfmoordpreventie

De aanbevelingen hieronder zijn opgesteld in de geest van constructive disclosure: zij bieden een concreet pad voor verdere verbetering, gebouwd op de bevindingen van de onderhavige meting en op de norm zoals die in jurisprudentie en richtsnoeren is vastgelegd.

1. **Implementeer een werkende Consent Management Platform-configuratie** waarin tracking pas wordt geactiveerd ná expliciete toestemming. De Google Tag Manager, AdSense en Analytics-instellingen kunnen worden voorzien van een consent-mode 2-implementatie die deze norm wel afdwingt. Technisch oplosbaar binnen dagen, niet maanden.
2. **Voer (of update) een Data Protection Impact Assessment (DPIA)** conform AVG artikel 35 voor de online aanwezigheid van 113.nl, waarin de noodzaak van elk afzonderlijk tracker-element wordt afgewogen tegen de aard van de bijzondere persoonsgegevens van de doelgroep.
3. **Schoon de tracker-stack op** tot wat echt noodzakelijk is voor de primaire hulpfunctie. Veel van de aanwezige trackers zijn georiënteerd op fondsenwerving en marketing. Een minimale technische voetafdruk is bij hulpverlening aan kwetsbare doelgroepen wenselijk vanuit het beginsel van data-minimalisatie (AVG artikel 5 lid 1c).
4. **Laat een onafhankelijke audit uitvoeren** door een partij die niet in een commerciële relatie staat met de leveranciers van de gebruikte tracking-tools. Dit voorkomt schijn van belangenverstrengeling.
5. **Werk de privacyverklaring bij** met expliciete vermelding van alle acht aangetroffen tracker-identifiers. Verifieer of alle doelen, ontvangers en bewaartermijnen voldoende specifiek zijn beschreven (AVG artikel 13).
6. **Onderzoek joint controllership-verhoudingen** met Google, Microsoft en eventuele andere derde-partijen op grond van Fashion ID (HvJ-EU C-40/17, 2019). Beoordeel of bestaande verwerkersovereenkomsten passend zijn voor deze gezamenlijke verantwoordelijkheid.

11. Bijlagen

Bijlage A — Verificatiehashes

SHA-256 van het raw scan-bestand 9 mei 2026:

```
ab4ffe91a233e37c30604581da789e2db735788e682019c91449aa506be2e4f0
```

SHA-256 van het raw-data leveringspakket (ZIP, 12 mei 2026):

```
cf3f2dcc06c0e4f65e04835817287a6e89ff153e1254eaad503dc5b97d44f6b1
```

OpenTimestamps: Aanwezig voor het 9 mei scan-bestand (`113.nl_20260509_234941.json.ots`). Verifieerbaar via opentimestamps.org of via lokale CLI (`ots verify`).

Bijlage B — Bronbestanden

Bestand	Inhoud
`runs/2026-05-09_forensisch_v3.7_v2/113.nl_20260509_234941.json`	Volledige scan-output 9 mei (cookies, scripts, third-parties per modus)
`113.nl_20260509_234941.json.ots`	OpenTimestamps-bewijs van scan-output 9 mei
`113.nl_har_20260509_234933.har`	HAR-archief 9 mei — volledig netwerk-verkeer per modus
`runs/2026-05-11_113-recheck_v3.8/113.nl_20260511_201555.json`	Scan-output herhalingsmeting 11 mei
`113.nl_har_20260511.har`	HAR-archief 11 mei
`share/113-rawdata-20260511.zip`	Volledig leveringspakket, gedeeld met Stichting 113 op 12 mei 2026

Bijlage C — Definities

Term	Definitie
Consent API	Software-interface die door een cookiebanner-leverancier wordt geleverd om toestemming-keuzes van bezoekers door te geven aan tracking-tools.
CMP	Consent Management Platform. Software die de toestemmingsdialoog op een website verzorgt en de keuzes vastlegt en doorgeeft aan downstream-tools.
Fingerprinting	Techniek om een bezoeker te identificeren op basis van een combinatie van technische browser-eigenschappen, zonder gebruik van cookies. Tijdzone, schermresolutie, taal-instellingen en fonts zijn ingrediënten.
Obfuscatie	Techniek om broncode minder leesbaar te maken. `atob` + `eval` -combinaties zijn een bekend patroon waarbij code uit base64-strings dynamisch wordt opgebouwd op het moment van uitvoeren.
HAR	HTTP Archive. JSON-formaat dat al het netwerk-verkeer tijdens een browser-sessie vastlegt — URL's, headers, bodies, timings. Te openen in browser-DevTools.
OpenTimestamps	Open standaard voor het cryptografisch verankeren van een bestand op de Bitcoin-blockchain, zodanig dat het bestaan van het bestand op een bepaalde datum onomstotelijk kan worden aangetoond.
Constructive disclosure	Werkwijze waarbij privacy-bevindingen worden gedeeld met de betrokken organisatie, ruimte voor reactie wordt geboden, raw data publiek verifieerbaar is, en eventuele herstelacties worden gedocumenteerd in vervolgmetingen.

Bijlage D — Over Hackedemia

Hackedemia is een onafhankelijk privacy-onderzoeksprogramma onder leiding van Mick Beer, maatschappelijk hacker. Het programma documenteert sectorbrede patronen in Nederlandse digitale infrastructuur, met als publiek doel laten zien wat er onder de motorkap van Nederlandse websites werkelijk gebeurt. Alle bevindingen zijn cryptografisch verifieerbaar via SHA-256 en, waar mogelijk, OpenTimestamps op de Bitcoin-blockchain.

Het werk staat publiek op **hackedemia.nl** en op **mijnoverheid.us**. Hackedemia is niet-commercieel: geen subsidies, geen sponsoring, geen commercieel verdienmodel. Onderzoek wordt naast regulier werk in eigen tijd uitgevoerd.

Het 113.nl-onderzoek maakt deel uit van een sectorbreed onderzoek naar negen Nederlandse hulpverleningssites, waarvan het volledige rapport in mei 2026 op hackedemia.nl beschikbaar komt.