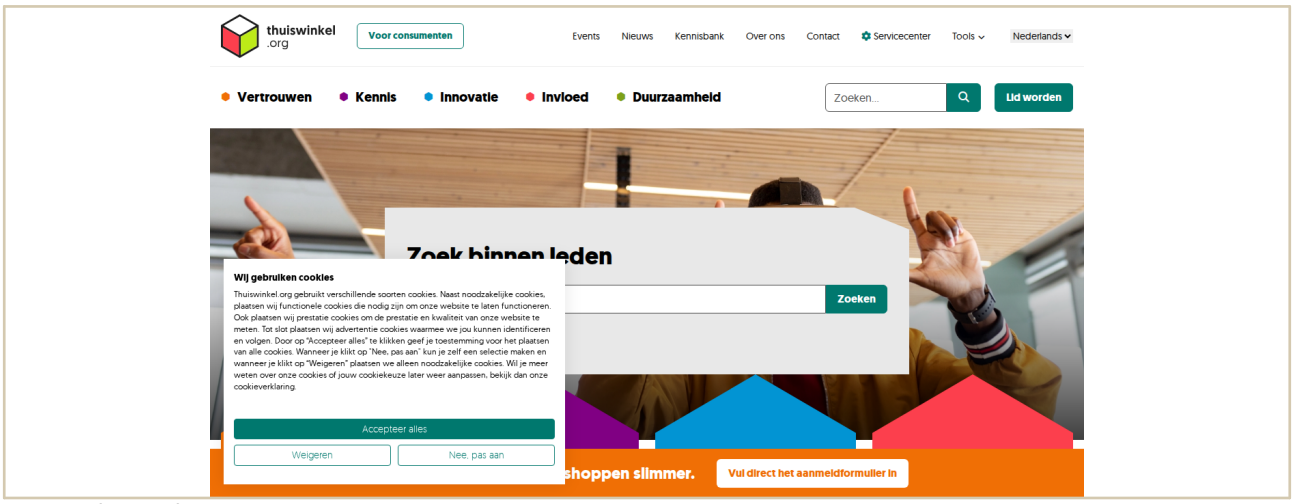
CookieChopper

Privacyscan — Verbeteradvies & Informatie

Website: **https://thuiswinkel.org/** · Datum: 07-04-2026 21:26



Screenshot zonder consent te geven.

3.8 Rapportcijfer — Zeer slecht

Persoonlijk bericht aan de website-eigenaar

Geachte Dames en Heren,

Op 07-04-2026 21:26 heb ik uw website https://thuiswinkel.org/ bezocht en een privacyscan uitgevoerd. De resultaten baren mij zorgen en ik deel ze graag met u.

Uw website scoort een 3,8 uit 10. Dat is een rode score. Dat betekent dat er serieuze problemen zijn met de manier waarop uw website omgaat met de privacy van bezoekers.

Ik zag dat uw website gegevens deelt met maar liefst vijf partijen, waaronder Google, Microsoft en Visual Website Optimizer. Dat zijn vijf zogenaamde hoog-risico trackers. Dat zijn kleine stukjes software die bijhouden wat u op een website doet, als een soort onzichtbare camera. Daar is op zichzelf niets mis mee, maar alleen als bezoekers daar eerst toestemming voor geven.

En precies dáár gaat het mis. Uw website heeft wel een cookiebanner, maar die werkt niet zoals het hoort. Als een bezoeker op "weigeren" klikt, blijven de trackers gewoon actief. Dat is alsof u iemand vraagt of hij koffie wil, hij zegt nee, maar u hem toch een kop inschenkt. Dit noemen we schijnveiligheid. De bezoeker denkt dat zijn keuze wordt gerespecteerd, maar dat is niet zo. Dat is in strijd met de wet.

Daarnaast heb ik op uw website geen Privacy Officer of Functionaris Gegevensbescherming kunnen vinden. Afhankelijk van de omvang van uw organisatie kan dit een wettelijke verplichting zijn. Het is in elk geval een belangrijk aandachtspunt.

Dit rapport is gemaakt door CookieChopper, een onafhankelijke privacyscanner zonder winstoogmerk. Ik nodig u van harte uit om de genoemde punten aan te pakken en daarna een nieuwe scan te doen via gosselaar.net/cookiechopper.

Hartelijke groeten,

CookieChopper

P.S. Dit is geen juridisch advies, maar een vriendelijke waarschuwing. De problemen die hier beschreven worden zijn wél echte wettelijke verplichtingen.

Prioriteit 0 — Uw cookiebanner werkt niet correct na weigeren

Vóór het klikken op "weigeren": **8 cookies**. Na het klikken op "weigeren": **9 cookies**.

KRITIEK: Er kwamen 1 cookies BIJ na het weigeren. In plaats van cookies te verwijderen, plaatst de website er meer.

De weigerfunctie van de cookiebanner biedt geen werkelijke controle over tracking. Controleer de CMP-configuratie en zorg dat alle niet-functionele cookies daadwerkelijk worden verwijderd wanneer een bezoeker weigert.

Netwerkverkeer-analyse — Wat doen deze trackers?

Op basis van het vastgelegde netwerkverkeer (HAR-bestand) zijn de volgende tracking-diensten geïdentificeerd. Per dienst wordt uitgelegd wat het doet, welke gegevens worden verstuurd, en wat u kunt doen om dit te verhelpen.

Google Tag Manager — Analytisch — risico: hoog

→ https://www.googletagmanager.com/gtm.js?id=GTM-5WN596

→ https://www.googletagmanager.com/gtag/js?id=G-7HYZB27N7H&cx=c&gtm=4e6460

Identificerende parameters: **GTM-5WN596, G-7HYZB27N7H, cid=2044263563.1775589898**

Google Analytics — Analytisch — risico: hoog

→ https://region1.google-analytics.com/g/collect?v=2&tid=G-7HYZB27N7H&...

Identificerende parameters: **tid=G-7HYZB27N7H, cid=2044263563.1775589898, gdid=dNjAwYj**

Visual Website Optimizer (VWO) — Tracking — risico: hoog

→ https://dev.visualwebsiteoptimizer.com/j.php?a=932848&u=...

→ https://dev.visualwebsiteoptimizer.com/dcdn/settings.js?a=932848&...

→ https://dev.visualwebsiteoptimizer.com/eu01/events/t?en=vwo_variationShown&a=932848&...

Identificerende parameters: **a=932848, v=f122f9da, _vwo_uuid=D0B14E69A96CA903D3611D6A4AD90AB05**

Cookies: _vwo_uuid_v2, _vwo_uuid, _vis_opt_exp_3_combi, _vis_opt_s, _vis_opt_test_cookie

Microsoft Clarity — Analytisch — risico: hoog

→ https://www.clarity.ms/tag/sge2pudn1p?ref=gtm

→ https://scripts.clarity.ms/0.8.59/clarity.js

→ https://k.clarity.ms/collect

Identificerende parameters: **sge2pudn1p**

CookieFirst — Functioneel — risico: middel

→ https://consent.cookiefirst.com/sites/thuiswinkel.org-52130183-d08f-4bcc-85f2-1a89ab68b807/consent.js

→ https://consent.cookiefirst.com/consentBanner.no-autoblock.js

→ `https://api.cookiefirst.com/prod/consent`

Identificerende parameters: **thuiswinkel.org-52130183-d08f-4bcc-85f2-1a89ab68b807**

Google Ads — Marketing — risico: hoog

→ `https://pagead2.googlesyndication.com/ccm/collect?frm=0&en=page_view&...`

Identificerende parameters: **did=dNjAwYj, gdid=dNjAwYj, tids=AW-1**

DiamondForms — Functioneel — risico: middel

→ `https://thuiswinkel.diamondforms.net/Diamant/Form?args=...`

→ `https://thuiswinkel.diamondforms.net/Diamant/JsonGetForm?encryptedIdentifier=...`

Identificerende parameters: **ASP.NET_SessionId**

Cookies: ASP.NET_SessionId

*De bronbestanden (HAR-bestand) van deze analyse zijn beschikbaar tot **07-05-2026** op verzoek via maurice@gosselaar.net.*

Uw pad naar een 8.0 — Verbeteradvies

Op basis van de scanresultaten heeft onze AI een gepersonaliseerd verbeterplan opgesteld. Een perfecte 10 is niet nodig — een **8.0** betekent dat uw website goed omgaat met de privacy van bezoekers. Hieronder vindt u concrete stappen om dat te bereiken.

Op basis van de scan zien wij verbetermogelijkheden. Hieronder vindt u concrete stappen.

Tip 1: Configureer uw CMP zodat scripts geblokkeerd worden

Uw cookiebanner is geïnstalleerd maar blokkeert tracking-scripts niet vóór consent. Configureer de blokkeerlijst in uw CMP zodat alle third-party scripts pas laden na toestemming.

Gemiddeld · Geschatte tijd: **1 uur**

Tip 2: Controleer uw Consent Mode configuratie

Google Consent Mode is gedetecteerd maar trackers laden alsnog. Controleer of alle consent-categorieën correct zijn geconfigureerd en test met de Tag Assistant.

Gemiddeld · Geschatte tijd: **1 uur**

Tip 3: Blokkeer third-party scripts vóór consent

Zorg dat scripts van derden (Hotjar, Clarity, Meta Pixel) pas laden nadat de bezoeker toestemming geeft via uw CMP.

Gemiddeld · Geschatte tijd: **1 uur**

Tip 4: Werk uw privacyverklaring bij

Vermeld alle cookies, hun doel, bewaartermijn en hoe bezoekers toestemming kunnen intrekken. Noem uw Functionaris Gegevensbescherming.

Makkelijk · Geschatte tijd: **1 uur**

Tip 5: Stel een Privacy Officer aan

Wijs een Functionaris Gegevensbescherming (FG) aan en vermeld deze op uw website met contactgegevens.

Makkelijk · Geschatte tijd: **30 min**

Tip 6: Test uw website regelmatig

Scan uw website periodiek met CookieChopper of vergelijkbare tools. Controleer ook handmatig via F12 > Application > Cookies.

Makkelijk · Geschatte tijd: **5 min**

Een 8.0 is haalbaar met relatief kleine aanpassingen. Uw bezoekers zullen het waarderen.

Wat zijn cookies en waarom zijn ze een probleem?

Cookies zijn kleine tekstbestanden die een website op uw computer, telefoon of tablet opslaat wanneer u de site bezoekt. Ze werden in 1994 uitgevonden als technische oplossing zodat websites een "geheugen" konden hebben tussen pagina's — denk aan een winkelwagen in een webshop. Sindsdien zijn cookies echter ook de motor geworden achter grootschalige online surveillance.

Drie soorten cookies

Functionele cookies

Noodzakelijk voor de werking van de website: inloggen, winkelwagen, taalvoorkeur. Mogen zonder toestemming geplaatst worden.

Analytische cookies

Meten hoe bezoekers de website gebruiken (bijv. Google Analytics). Vereisen toestemming tenzij volledig geanonimiseerd en privacy-vriendelijk geconfigureerd.

Tracking- & marketingcookies

Volgen uw gedrag over meerdere websites heen om gerichte advertenties te tonen. Denk aan: Meta Pixel, Google Ads, LinkedIn Insight Tag. Altijd toestemming vereist.

Waarom kunnen cookies schadelijk zijn?

Op zichzelf is een cookie een onschuldig tekstbestandje. Het gevaar zit in wat ermee gedaan wordt:

• **Profiel opbouwen:** Door tracking-cookies van derden (third-party cookies) wordt een schaduwprofiel van u opgebouwd: welke sites u bezoekt, wat u koopt, waar u zoekt — zonder dat u dat weet of daarvoor toestemming heeft gegeven.

• **Geen controle:** Veel websites plaatsen cookies vóór u toestemming geeft, in strijd met de AVG en de ePrivacy-richtlijn (Telecommunicatiewet in Nederland).

• **Prijsdiscriminatie:** Online winkels kunnen cookies gebruiken om uw eerdere bezoeken te herkennen en hogere prijzen te tonen.

• **Data-lekken:** Hoe meer partijen uw data verzamelen, hoe groter de kans dat het bij een datalek op straat belandt.

• **Manipulatie:** Gedetailleerde gedragsprofielen maken het mogelijk om gericht misleidende advertenties of desinformatie te tonen.

Wat zegt de wet?

In Nederland en de EU gelden strenge regels voor cookies. De **AVG** (Algemene Verordening Gegevensbescherming) en de **Telecommunicatiewet** (artikel 11.7a) schrijven voor dat:

• Niet-functionele cookies pas geplaatst mogen worden NA expliciete, geïnformeerde en vrije toestemming.

• Toestemming moet net zo makkelijk in te trekken zijn als te geven.

• "Doorgebruiken van de website" geldt NIET als toestemming.

• Pre-aangevinkte vakjes zijn verboden — de bezoeker moet actief kiezen.

• Een "cookie-wall" (geen toegang zonder accepteren) is in principe niet toegestaan.

Wat is een HAR-bestand?

Bij deze scan is een HAR-bestand (HTTP Archive) vastgelegd. Dit is een gestandaardiseerd bestandsformaat dat exact registreert welke netwerkverzoeken de browser heeft uitgevoerd, inclusief alle tracking-requests, cookies en parameters — met timestamps op de milliseconde. Het HAR-bestand is het digitale equivalent van een procesverbaal: het toont objectief en machineleesbaar wat de website doet.

U kunt een HAR-bestand openen in Chrome DevTools (F12 → Network → Import HAR) of via gratis online viewers. Het HAR-bestand van deze scan is 30 dagen beschikbaar op verzoek.

Dit is niet mijn website. Wat kan ik doen?

■■ Uiteindelijk kunt u een melding doen bij de autoriteit persoongsgegevens — een AP-melding is effectief maar heeft gevolgen

Een melding bij de Autoriteit Persoonsgegevens is een serieuze stap. De AP kan een onderzoek instellen en boetes opleggen. Dat is precies de bedoeling als een website de wet overtreedt — maar onderneem dit weloverwogen en met goed bewijs. Bijvoorbeeld als de Webmaster helemaal niet reageert of niets doet.

***Aanbevolen aanpak:** Probeer eerst direct contact op te nemen met de Privacy Officer (Functionaris voor Gegevensbescherming, FG) van de organisatie. Veel overtredingen zijn het gevolg van onwetendheid en worden snel opgelost als iemand het aankaart. Pas als dat niets oplevert, is een AP-melding de logische vervolgstap.*

Dit stappenplan leidt u door het volledige proces: van bewijs verzamelen, de Privacy Officer vinden, tot het indienen van een klacht bij de AP.

Fase 1 — Verzamel uw eigen bewijs

Dit rapport is indicatief. Voor een sterke klacht heeft u ook eigen bewijsmateriaal nodig.

Stap 1: Open de website in een incognitovenster

Gebruik een incognitovenster (Ctrl+Shift+N in Chrome/Edge, Ctrl+Shift+P in Firefox). Hierdoor zijn er geen bestaande cookies die het resultaat beïnvloeden. U start met een schone lei, precies zoals een nieuwe bezoeker.

Stap 2: Open de Ontwikkelaarstools (F12)

Druk op F12. Navigeer naar het tabblad "Application" (Chrome/Edge) of "Storage" (Firefox). Klik links op "Cookies" → de website-URL. U ziet nu alle cookies die VÓÓR toestemming zijn geplaatst. Maak een screenshot met datum en tijdstip zichtbaar in de taakbalk.

Stap 3: Controleer de Network-tab

Ga naar het tabblad "Network" en laad de pagina opnieuw (F5). Zoek naar verzoeken naar google-analytics.com, googletagmanager.com, facebook.com/tr of andere tracking-domeinen. Als die verschijnen vóór toestemming: dat is direct bewijs. Maak screenshots van deze verzoeken inclusief de request-headers.

Stap 4: Controleer LocalStorage

Nog steeds in het tabblad "Application": klik op "Local Storage" en "Session Storage". Staan hier tracking-sleutels (_ga, _fbp, hubspot, ajs_anonymous_id etc.) zonder dat u toestemming heeft gegeven? Dat is ook bewijs van een overtreding. Maak een screenshot.

Stap 5: Bewaar alles met tijdstempel

Sla alle screenshots op met de datum en het tijdstip zichtbaar. Noteer ook de exacte URL van de gescande pagina. Bewaar dit CookieChopper-rapport als aanvullende technische documentatie.

Fase 2 — Zoek de Privacy Officer (FG) en neem contact op

Stap 6 t/m 9 beschrijven hoe u de verantwoordelijke persoon vindt en aanspreekt.

Juridische context: wanneer is een FG verplicht?

Artikel 37 AVG verplicht de aanstelling van een Functionaris voor Gegevensbescherming (FG) voor: (1) overheidsinstanties en publieke organen, (2) organisaties die op grote schaal bijzondere persoonsgegevens verwerken, (3) organisaties die grootschalig gedrag van mensen volgen.

***Verplichte publicatie:** Artikel 37 lid 7 AVG verplicht dat de contactgegevens van de FG worden gepubliceerd. Als de website van een overheidsorganisatie (gemeente, ministerie, zorginstelling) géén FG-contactgegevens vermeldt in de privacyverklaring, is dat op zichzelf al een overtreding die u kunt melden bij de AP.*

Stap 6: Zoek de privacyverklaring van de website

Ga naar de website en zoek onderaan de pagina naar een link met "Privacybeleid", "Privacyverklaring" of "Privacy". Zoek daarin naar "Functionaris voor Gegevensbescherming", "FG", "DPO" of "Data Protection Officer". Staat daar een naam en e-mailadres? Noteer die. Staat die informatie er NIET? Voor overheidsorganisaties en grote bedrijven is dat een aparte overtreding — noteer dit ook.

Stap 7: Zoek de FG via LinkedIn of een AI-assistent

Is de FG niet vindbaar in de privacyverklaring? Probeer dan LinkedIn: zoek op de organisatienaam met de functietitel "Privacy Officer", "DPO" of "Functionaris Gegevensbescherming". U kunt ook een AI-assistent (zoals ChatGPT of Claude) vragen: "Wie is de Privacy Officer van [organisatienaam]?" — vaak levert dat bruikbare resultaten op basis van openbare bronnen. Kamer van Koophandel en het AVG-register (agentschaptelecom.nl) kunnen ook helpen.

Stap 8: Stuur een formele e-mail naar de Privacy Officer

Schrijf een korte, zakelijke e-mail. Vermeld: (1) de URL van de gescande pagina, (2) datum en tijdstip van uw onderzoek, (3) welke cookies/trackers u heeft aangetroffen vóór toestemming, (4) een verwijzing naar dit rapport als bijlage, (5) een verzoek om de situatie binnen 30 dagen te herstellen. Bewaar een kopie van deze e-mail — dit toont aan dat u eerst de interne weg heeft bewandeld.

Stap 9: Wacht op reactie (maximaal 30 dagen)

Een organisatie heeft redelijkerwijs 30 dagen om te reageren op een privacymelding. Reageert men niet, of is de overtreding na 30 dagen niet verholpen? Dan heeft u aantoonbaar geprobeerd het intern op te lossen. Dat versterkt uw positie bij een AP-klacht aanzienlijk.

Fase 3 — Dien een klacht in bij de Autoriteit Persoonsgegevens

Als direct contact niets heeft opgeleverd, is een AP-melding de volgende stap.

Stap 10: Dien uw klacht in bij de AP

Ga naar autoriteitpersoonsgegevens.nl en zoek "klacht indienen over cookies". U kunt de klacht indienen op uw eigen naam — de AP behandelt dit vertrouwelijk. Voeg het volgende toe als bijlage: (1) uw eigen screenshots met tijdstempel, (2) dit CookieChopper-rapport, (3) de e-mail die u naar de Privacy Officer heeft gestuurd en het eventuele antwoord (of bewijs van uitblijven van antwoord). Beschrijf in de klacht: welke website, welke cookies aangetroffen, wanneer, en wat u zelf al heeft ondernomen. Hoe concreter uw klacht, hoe groter de kans op actie.

Directe links Autoriteit Persoonsgegevens

```
Klacht indienen cookies: https://www.autoriteitpersoonsgegevens.nl/themas/internet-telefoon-tv-en-post/cookies/klacht-over-cookies

AVG-register FG's (agentschaptelecom.nl): https://autoriteitpersoonsgegevens.nl/themas/beveiliging/functionaris-voor-gegevensbescherming-fg

Algemene informatie cookies:
https://www.autoriteitpersoonsgegevens.nl/themas/internet-telefoon-tv-en-post/cookies
```

Stuur ons cookies in ruil voor uw Gratis rapport!

Vond je dit nuttig? Wij accepteren geen geld — maar koekjes zijn van harte welkom. Dit is een initiatief zonder winstoogmerk, dus een doos echte koekjes maakt onze dag al helemaal goed.

Even realistisch: elke scan kost ca. € 0,12 aan AI-tokens. Heel veel scans branden het budget snel op. Sponsoring in de vorm van koekjes helpt om dit initiatief levendig te houden.

Je kunt koekjes sturen naar:

CookieChopper
t.a.v. De cookie-detective Maurice
Amaliastraat 14
5971 JD Grubbenvorst
Nederland

Waarom CookieChopper? De naam komt voort uit Choppi, de hond van Jeroen. Honden mogen natuurlijk geen koekjes, maar wel hondenkoekjes. Je kunt overwegen bij de mensenkoekjes ook wat hondenkoekjes mee te sturen — we zorgen dat het bij Choppi terecht komt!

■ Dit is een privéadres. CookieChopper is een onafhankelijk initiatief zonder winstoogmerk.