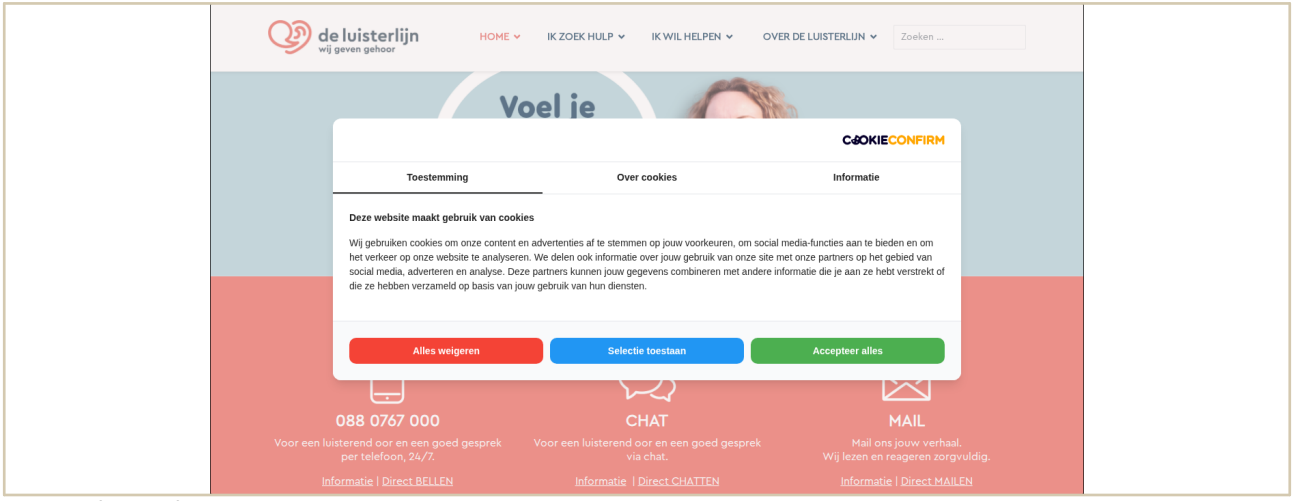
CookieChopper

Privacyscan — Verbeteradvies & Informatie

Website: **https://deluisterlijn.nl/** · Datum: 18-05-2026 18:11



Screenshot zonder consent te geven.

5.2 Rapportcijfer — Onvoldoende

Persoonlijk bericht aan de website-eigenaar

Geachte Dames en Heren,

Op 18-05-2026 18:11 heb ik uw website https://deluisterlijn.nl/ bezocht en een privacyscan uitgevoerd. Ik deel de resultaten graag met u, zodat u kunt zien hoe uw website er op dit moment voor staat.

Uw website scoort een 5.2 op 10. Dat is een oranje score. Het betekent dat het niet slecht is, maar dat er zeker ruimte is voor verbetering. Er zijn een paar dingen die aandacht verdienen.

Ik zag dat uw website gegevens deelt met Google, zonder dat mij eerst gevraagd werd of ik dat goed vind. Dit gebeurde al voordat ik ergens op had geklikt. Dat mag eigenlijk niet. Er is wel een cookiebanner aanwezig, maar daarin ontbreekt iets belangrijks: de mogelijkheid om cookies te weigeren is niet getest. Ook mist uw website Consent Mode. Dat is een technische instelling waarmee u Google pas gegevens laat verzamelen nadat een bezoeker daarmee instemt. Zonder die instelling loopt u een risico.

Er is één tracker gevonden die als hoog risico is aangemerkt. Dat is de tracker van Google.

Wat goed is: ik heb op uw website een Privacy Officer gevonden. Dat is de persoon die verantwoordelijk is voor de omgang met persoonsgegevens. Die is te bereiken via privacy@deluisterlijn.nl. Dat is een duidelijk positief punt en laat zien dat u privacy serieus neemt.

Met een paar gerichte aanpassingen kunt u uw score aanzienlijk verbeteren en voldoen aan de wettelijke regels rondom privacy.

Dit rapport is gemaakt met CookieChopper, een onafhankelijke privacyscanner zonder winstoogmerk. Heeft u de verbeteringen doorgevoerd? Doe dan gerust een nieuwe scan 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.

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: Installeer een erkende cookiebanner (CMP)

Gebruik een erkende CMP zoals Cookiebot, CookieYes of Klaro. Deze blokkeren automatisch tracking-scripts tot de bezoeker toestemming geeft.

Makkelijk · Geschatte tijd: **30 min**

Tip 2: Implementeer Google Consent Mode v2

Voeg gtag('consent','default',{ad_storage:'denied',analytics_storage:'denied'}) toe vóór uw GA/GTM code. Zo laden Google-scripts cookieloos tot consent.

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: Controleer cookie-instellingen na updates

Na elke website-update of plugin-update kunnen cookie-instellingen terugvallen naar standaardwaarden. Controleer na elke update of uw CMP nog correct werkt.

Makkelijk · Geschatte tijd: **5 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.

Browser-fingerprinting: tracking zonder cookies

Steeds meer bedrijven gebruiken **browser-fingerprinting** als alternatief voor cookies. Bij fingerprinting wordt een unieke "vingerafdruk" van uw browser gemaakt door allerlei technische kenmerken te combineren — zonder dat er een bestand op uw computer wordt gezet.

Techniek	Hoe het werkt
Canvas fingerprinting	Onzichtbaar tekenen op een HTML5-canvas levert een unieke afbeelding op per apparaat/GPU-combinatie.
Audio fingerprinting	Verwerking van een geluidssignaal via AudioContext levert unieke variaties op per hardware.
Lettertype-detectie	Door te meten welke fonts op uw systeem geïnstalleerd staan, wordt een profiel opgebouwd.
WebGL fingerprinting	De GPU-renderer, extensies en shader-precisie leveren een unieke combinatie op.
Schermresolutie & kleurdiepte	Combinatie van schermgrootte, pixelratio en kleurdiepte helpt bij identificatie.
Plugin & MIME-detectie	Welke browser-plugins en MIME-types beschikbaar zijn verschilt per installatie.

Het gevaar van fingerprinting is dat het **onzichtbaar** is en **niet te blokkeren** door simpelweg cookies te weigeren. U kunt cookies verwijderen, maar u kunt uw browsereigenschappen niet veranderen. Onder de AVG wordt fingerprinting als persoonsgegevensverwerking beschouwd en is dus ook toestemming vereist.

Andere trackingtechnieken

Naast cookies en fingerprinting bestaan er nog meer methoden om u online te volgen:

LocalStorage & SessionStorage

Trackers slaan identificatiegegevens op in de browseropslag in plaats van cookies. Dit omzeilt cookie-blokkers maar valt juridisch onder dezelfde regels.

URL-decoratie (link tracking)

Parameters als fbclid=, gclid= en utm_source= worden aan URL's toegevoegd om uw klikgedrag over sites heen te volgen, zelfs als cookies geblokkeerd zijn.

Tracking-pixels (beacons)

Onzichtbare afbeeldingen van 1x1 pixel (bijv. Meta Pixel, LinkedIn Insight Tag) die bij laden een verzoek naar een tracking-server sturen met uw gegevens.

CNAME-cloaking

Third-party trackers worden verstopt als first-party door een DNS-alias (CNAME-record) in te stellen. Dit omzeilt adblockers die third-party domeinen blokkeren.

Server-side tracking

Steeds meer bedrijven verplaatsen tracking naar hun eigen server. Uw gegevens worden dan server-to-server doorgestuurd naar Google, Meta etc. — onzichtbaar voor uw browser en adblockers.

Juridische conclusie

Al deze technieken — cookies, fingerprinting, tracking-pixels, localStorage, CNAME-cloaking en server-side tracking — vallen onder de AVG als ze worden gebruikt om personen te identificeren of profielen op te bouwen. Het maakt juridisch niet uit of het een cookie, fingerprint of pixel is: **toestemming is vereist voor niet-functionele verwerking van persoonsgegevens.**

Hoe kunt u uzelf beschermen?

• **Gebruik een adblocker:** Extensies als uBlock Origin blokkeren veel tracking-scripts en cookies van derden.

• **Gebruik een privacy-browser:** Firefox met strenge tracking-protectie, Brave of DuckDuckGo bieden betere standaardbescherming.

• **Weiger altijd niet-noodzakelijke cookies:** Klik bij cookiebanners altijd op "Weigeren" of "Alleen noodzakelijk".

• **Gebruik regelmatig incognito-modus:** In een incognitovenster worden cookies verwijderd zodra u het venster sluit.

• **Installeer Privacy Badger:** Deze extensie van de EFF leert automatisch welke trackers u volgen en blokkeert ze.

• **Verwijder URL-parameters:** Extensies als ClearURLs verwijderen automatisch tracking-parameters uit URL's.

• **Controleer websites met CookieChopper:** Scan websites die u bezoekt en meld overtredingen via de Autoriteit Persoonsgegevens.

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
```

Dit rapport is gratis. Helpt u het zo te houden?

CookieChopper is een onafhankelijk initiatief zonder winstoogmerk. Geen advertenties, geen abonnementen, geen dataverkoop. Elke scan kost ons tussen de € 0,50 en € 1,00 aan AI-tokens, server-tijd en netwerkverkeer. Dit initiatief draait volledig op eigen middelen.

Wilt u een vrijwillige bijdrage doen?

Elke bijdrage — groot of klein — helpt direct om de servers draaiend te houden en meer websites gratis te kunnen scannen. Er is geen BTW-factuur nodig: het is een vrijwillige gift aan een persoonlijk initiatief.

Betaalverzoek via bunq

`https://bunq.me/mgosselaar`

Kies zelf een bedrag. Elke euro telt.

Liever iets tastbaars?

We jagen digitale cookies op, maar houden van de eetbare variant. Een doos stroopwafels, speculaas of bastogne is ook heel welkom. Hondenkoekjes gaan naar Choppi.

CookieChopper / t.a.v. Maurice Gosselaar

Amaliastraat 14, 5971 JD Grubbenvorst

Contact: maurice@gosselaar.net • https://gosselaar.net/cookiechopper/

Hartelijk dank voor uw steun. Samen maken we het internet een stukje veiliger.