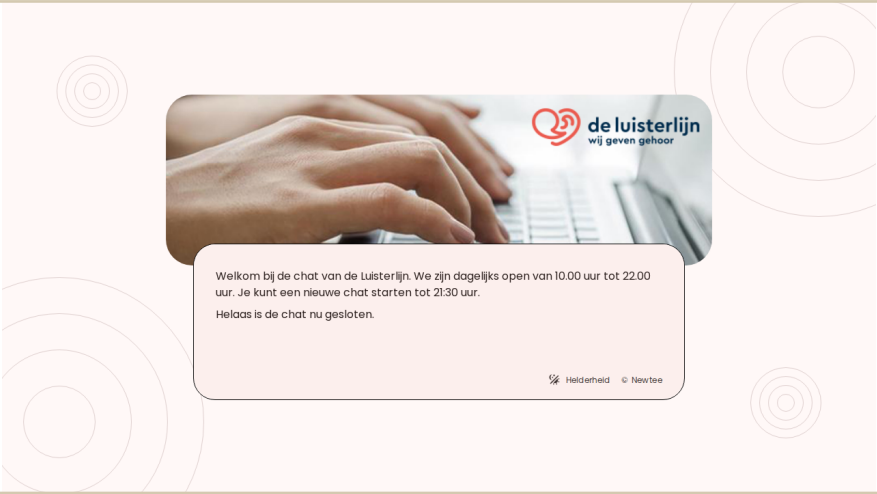
CookieChopper

Privacyscan — Verbeteradvies & Informatie

Website: **https://chat-client-luisterlijn.serviant.nl/** · Datum: 17-05-2026 23:11



Screenshot zonder consent te geven.

8.2 Rapportcijfer — Uitstekend

Persoonlijk bericht aan de website-eigenaar

Geachte Dames en Heren,

Op 17-05-2026 23:11 heb ik uw website https://chat-client-luisterlijn.serviant.nl/ bezocht en een privacyscan uitgevoerd. Ik deel graag de resultaten met u.

Het nieuws is goed. Uw website scoort een 8,2 op 10. Dat is een mooie score. Het betekent dat uw website op het gebied van privacy goed in elkaar zit. Er zijn geen hoog-risico trackers gevonden. Dat wil zeggen: er zijn geen verstopte volgsystemen die stiekem bijhouden wie uw bezoekers zijn of wat zij doen. Dat is precies zoals het hoort.

Toch zijn er twee punten die ik graag onder uw aandacht breng. Ten eerste heb ik geen cookiebanner aangetroffen op uw website. Omdat er ook geen trackers zijn gevonden, is dit op dit moment geen groot probleem. Maar mocht u in de toekomst iets toevoegen aan uw website — zoals een statistiekenprogramma of een ingebedde video — dan is een cookiebanner verplicht. Zorg er dan voor dat bezoekers écht kunnen kiezen.

Ten tweede heb ik geen Functionaris voor de Gegevensbescherming kunnen vinden op uw website. Dat is iemand die verantwoordelijk is voor privacy binnen uw organisatie. Het is verstandig om die persoon zichtbaar te vermelden, zodat bezoekers weten bij wie zij terechtkunnen met vragen of zorgen over hun gegevens.

Al met al doet u het prima. Met kleine aanpassingen kunt u de privacy van uw bezoekers nog beter waarborgen.

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

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 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.