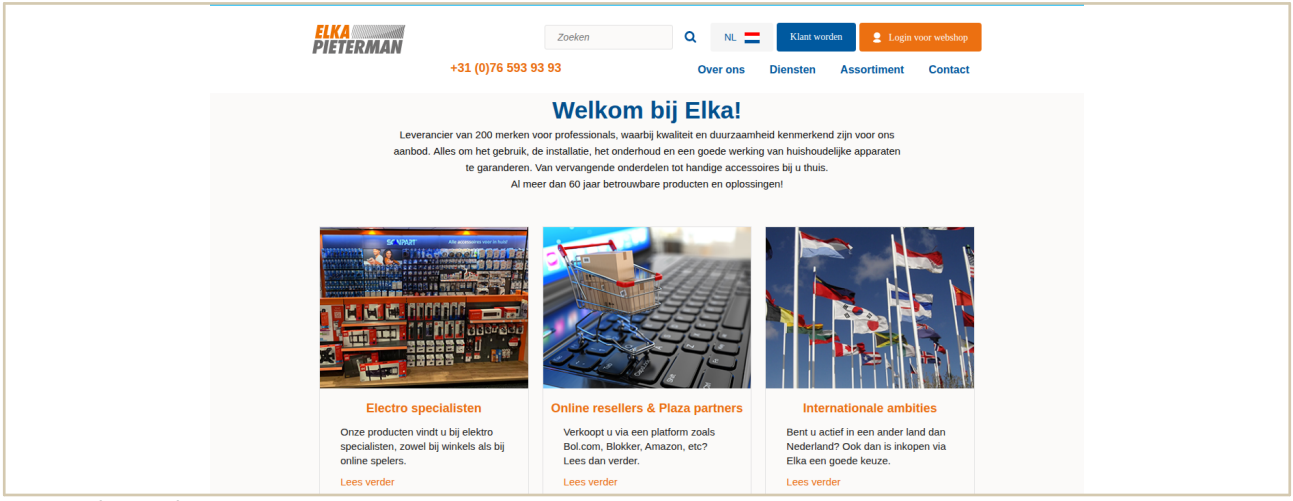
CookieChopper

Privacyscan — Verbeteradvies & Informatie

Website: **https://elka.nl/** · Datum: 25-04-2026 20:24



Screenshot zonder consent te geven.

4.5 Rapportcijfer — Onvoldoende

Persoonlijk bericht aan de website-eigenaar

Geachte Dames en Heren,

Op 25-04-2026 om 20:24 heb ik uw website https://elka.nl/ bezocht en een privacyscan uitgevoerd. Ik deel de resultaten graag met u, omdat ik denk dat u hier iets mee wilt doen.

Uw website scoort een 4,5 uit 10. Dat is een rode score. Het betekent dat er op dit moment dingen gebeuren op uw website die niet in orde zijn volgens de privacywet, de AVG.

Het grootste probleem is dit: uw website stuurt gegevens van bezoekers door naar Google, via Google Analytics en Google Tag Manager. Dat gebeurt op het moment dat iemand uw website bezoekt. Maar er verschijnt geen cookiebanner. Er wordt dus niet eerst aan de bezoeker gevraagd of die dat goed vindt. Dat is te vergelijken met iemand fotograferen zonder dat je het vraagt of zelfs maar vertelt. Dat mag niet zomaar. Dit is het meest dringende punt om op te lossen.

Beide gevonden trackers vallen in de categorie hoog risico. Dat wil zeggen dat ze gevoelige informatie kunnen verzamelen en doorgeven aan grote techbedrijven. Zolang er geen toestemming wordt gevraagd, is dat wettelijk gezien niet toegestaan.

Er is ook geen zogeheten Consent Mode actief. Dat is een technische instelling waarmee je Google kunt vertellen dat een bezoeker geen toestemming heeft gegeven. Ook dat ontbreekt nu.

Er is één duidelijk positief punt. U heeft een privacy officer aangesteld, bereikbaar via privacy@elka.nl. Dat is goed geregeld en laat zien dat u privacy serieus neemt. Des te meer reden om ook de technische kant op orde te brengen.

Dit rapport is gemaakt met CookieChopper, een onafhankelijke privacyscanner zonder winstoogmerk. Heeft u verbeteringen doorgevoerd? Doe dan een nieuwe scan via gosselaar.net/cookiechopper en kijk of uw score omhoog gaat.

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.

■ Geen cookiebanner aanwezig

Er is geen cookiebanner gedetecteerd, terwijl de website wél tracking-cookies en/of tracking-scripts plaatst. Bezoekers hebben geen enkele mogelijkheid om cookies te weigeren of hun toestemming te geven. Dit is op zichzelf al een overtreding wanneer er tracking-cookies worden geplaatst.

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-5G4DP8C

Identificerende parameters: **id=GTM-5G4DP8C**

Google Analytics — Analytisch — risico: hoog

→ https://www.google-analytics.com/analytics.js

→ https://www.google-analytics.com/j/collect?v=1&_v=j102&a=570846531&t=pageview&_s=1&dl=https%3A%2F%2F...

→ https://www.google-analytics.com/j/collect?v=1&_v=j102&a=2097829666&t=pageview&_s=1&dl=https%3A%2F%2...

Identificerende parameters: **cid=992126674.1777141434, tid=UA-97813403-1, _gid=2067735400.1777141434, _u=YEBAAEABAAAAACAAI~**

Cookies: _ga=GA1.2.992126674.1777141434, _gid=GA1.2.2067735400.1777141434, _gat_UA-97813403-1

LeadInfo — Tracking — risico: hoog

→ https://cdn.leadinfo.net/ping.js

→ https://collector.leadinfo.net/config/LI-601178E6703A7/

→ https://api.leadinfo.com/v1/identify/LI-601178E6703A7

Identificerende parameters: **LI-601178E6703A7**

Left5lock — Marketing — risico: middel

→ https://secure.left5lock.com/js/204251.js

Identificerende parameters: **204251**

Netivity Forms — Functioneel — risico: laag

→ https://forms.netivity.nl/api/js/netivity-forms.js

*De bronbestanden (HAR-bestand) van deze analyse zijn beschikbaar tot **25-05-2026** 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.

Uw website scoort momenteel een 4.5 en heeft op een aantal kritieke punten directe aandacht nodig — maar het goede nieuws is dat u met gerichte stappen snel naar een 8.0 kunt groeien. De grootste winst zit in het correct inrichten van consent en het stoppen van tracking vóór toestemming.

Tip 1: Installeer een erkende CMP-cookiebanner

Er is momenteel geen cookiebanner gevonden terwijl er wel tracking-cookies worden geplaatst — dit is een directe AVG-overtreding. Installeer een erkend Consent Management Platform (CMP) zoals Cookiebot, CookieYes of Usercentrics. Deze tools bieden kant-en-klare banners die voldoen aan de AVG en integreren eenvoudig via een script of plug-in.

Gemiddeld · Geschatte tijd: **1 uur**

Tip 2: Stop tracking vóór toestemming is gegeven

Op dit moment worden tracking-cookies geplaatst voordat een bezoeker toestemming heeft gegeven, wat niet is toegestaan onder de AVG. Zorg ervoor dat Google Analytics en Google Tag Manager pas worden geladen nádat de gebruiker actief akkoord heeft gegaan. Dit regelt u via de blokkeer-instelling in uw CMP in combinatie met tag-firing-regels in Google Tag Manager.

Gemiddeld · Geschatte tijd: **1 uur**

Tip 3: Activeer Google Consent Mode v2

Google Consent Mode is niet gedetecteerd, terwijl Google-scripts wel actief zijn op de website. Implementeer Google Consent Mode v2 via Google Tag Manager door de juiste consent-signalen (ad_storage, analytics_storage, etc.) te koppelen aan uw CMP. Dit zorgt ervoor dat Google-tools respectvol omgaan met de keuze van de bezoeker én het is verplicht voor gebruik van Google Ads-conversies.

Lastig · Geschatte tijd: **halve dag**

Tip 4: Beperk hoog-risico trackers tot het minimum

Van de 4 gedetecteerde tracker-implementaties zijn er 2 aangemerkt als hoog-risico (Google Analytics en Google Tag Manager). Controleer in Google Tag Manager welke tags en triggers actief zijn en verwijder alle tags die niet strikt noodzakelijk zijn voor de werking van de site. Minder actieve trackers betekent minder risico én een betere privacyscore.

Gemiddeld · Geschatte tijd: **1 uur**

Tip 5: Voeg een volledige AVG-verklaring toe aan de privacypagina

De scan heeft een beperkte AVG-verklaring gevonden met slechts 4 onderdelen, terwijl de AVG meer informatievereisten stelt. Breid de privacyverklaring uit met in ieder geval: de rechtsgronden voor verwerking, bewaartermijnen per categorie persoonsgegevens, de rechten van betrokkenen (inzage, correctie, verwijdering) en of gegevens worden doorgegeven buiten de EU. Gebruik de modelverklaring van de Autoriteit Persoonsgegevens als basis.

Gemiddeld · Geschatte tijd: **halve dag**

Tip 6: Test en documenteer de consent-flow regelmatig

Eenmalig instellen is niet voldoende — scripts en plug-ins kunnen consent-instellingen onbedoeld overschrijven na een update. Plan maandelijks een korte controle met een tool zoals CookieChopper of de browserextensie 'Cookie AutoDelete' om te verifiëren dat er geen cookies worden geplaatst vóór toestemming. Leg de uitkomsten kort vast zodat u kunt aantonen dat u actief toezicht houdt, wat ook relevant is voor uw verantwoordingsplicht.

Makkelijk · Geschatte tijd: **30 min**

Met deze zes stappen legt u een solide privacyfundament dat uw bezoekers vertrouwen geeft én uw organisatie beschermt — zet vandaag nog de eerste stap!

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
```

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.