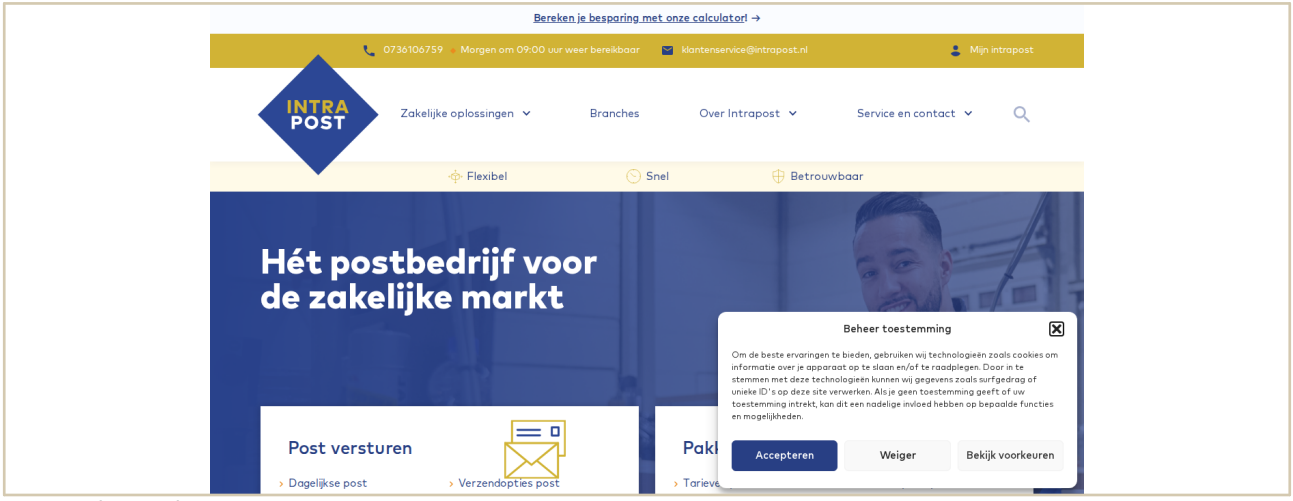
CookieChopper

Privacyscan — Verbeteradvies & Informatie

Website: **https://intrapost.nl/** · Datum: 12-04-2026 19:53



Screenshot zonder consent te geven.

5.2 Rapportcijfer — Onvoldoende

Persoonlijk bericht aan de website-eigenaar

Geachte Dames en Heren,

Op 12-04-2026 19:53 heb ik uw website https://intrapost.nl/ bezocht en een privacyscan uitgevoerd. Dit rapport is opgesteld door CookieChopper en legt uit wat ik heb aangetroffen.

Uw website scoort een 5.2 op 10. Dat is een oranje score. Niet alarmerend, maar er zijn duidelijke verbeterpunten waar u mee aan de slag moet. Een voldoende is het nog net niet.

Wat ik heb gezien: uw website deelt gegevens met Google, zonder dat bezoekers daar vooraf toestemming voor geven. Er is wel een cookiebanner aanwezig, maar die is generiek van aard. Dat betekent dat de banner er wel staat, maar waarschijnlijk niet goed is afgestemd op wat uw website werkelijk doet. Ik heb niet kunnen testen of het weigeren van cookies ook echt werkt. Dat is jammer, want juist dát is de kern van goede privacybescherming.

Er is één tracker gevonden met een hoog risico. Dat is de tracker van Google. Uw bezoekers weten mogelijk niet dat hun gegevens naar Google worden gestuurd, terwijl ze daar geen bewuste keuze voor hebben gemaakt. Dat is precies wat de AVG wil voorkomen.

Daarnaast heb ik op uw website geen Privacy Officer of Functionaris Gegevensbescherming kunnen vinden. Afhankelijk van uw organisatie kan dit verplicht zijn. Het is in ieder geval een duidelijk aandachtspunt.

Tot slot ontbreekt Consent Mode. Dit is een technische instelling waarmee Google-trackers pas echt actief worden nadat iemand toestemming geeft. Zonder dit werkt uw cookiebanner minder goed dan u misschien denkt.

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

Uw website scoort momenteel een 5.2 — er is duidelijk potentieel, maar ook een aantal concrete verbeterpunten die relatief snel aan te pakken zijn. Met de juiste stappen kunt u uw score naar een 8.0 brengen en uw bezoekers écht de privacy bieden waar ze recht op hebben.

Tip 1: Vervang generieke banner door erkende CMP

De huidige WordPress GDPR-plugin wordt niet herkend als een volwaardige Consent Management Platform (CMP). Vervang deze door een erkende oplossing zoals Cookiebot, Complianz of CookieYes, die aantoonbaar voldoen aan AVG-vereisten. Deze tools bieden ook een auditlog van verkregen toestemmingen, wat essentieel is bij een eventuele controle door de AP.

Gemiddeld · Geschatte tijd: **1 uur**

Tip 2: Blokkeer alle 4 trackers vóór consent

Op dit moment laden scripts en requests van 4 tracker-implementaties al vóór de bezoeker toestemming heeft gegeven. Configureer uw CMP zo dat alle tracking-scripts pas worden geactiveerd ná een expliciete 'Accepteer'-klik. In Complianz of Cookiebot gebeurt dit via de ingebouwde scriptblokkering; controleer of elke tracker correct is gecategoriseerd en geblokkeerd.

Gemiddeld · Geschatte tijd: **1 uur**

Tip 3: Implementeer Google Consent Mode v2

Google Consent Mode is niet gedetecteerd, terwijl Google-scripts wél aanwezig zijn — dit is een hoog-risico bevinding. Activeer Google Consent Mode v2 via uw Google Tag Manager-container door de consent-instellingen te koppelen aan uw CMP. Zo weet Google pas data te verwerken wanneer de bezoeker daadwerkelijk toestemming heeft gegeven.

Lastig · Geschatte tijd: **halve dag**

Tip 4: Herstel de hoog-risico Google-implementatie

De categorie 'Google (overig)' is aangemerkt als hoog-risico tracker-implementatie. Controleer in Google Tag Manager welke Google-tags actief zijn zonder consent-trigger en voeg voor elke tag een expliciete 'Consent Granted'-trigger toe. Verwijder of deactiveer tags die geen duidelijk doel hebben of waarvoor geen grondslag bestaat.

Gemiddeld · Geschatte tijd: **1 uur**

Tip 5: Stel een Privacy Officer aan en vermeld dit

Er is geen Privacy Officer (PO) of Functionaris voor Gegevensbescherming (FG) gevonden op uw website. Wijs intern iemand aan als verantwoordelijke voor privacy en vermeld diens naam of contactgegevens in uw privacyverklaring. Als uw organisatie verwerkingen uitvoert op grote schaal of met gevoelige gegevens, kan een FG zelfs wettelijk verplicht zijn.

Makkelijk · Geschatte tijd: **30 min**

Tip 6: Breid uw privacyverklaring volledig uit

De scan vond slechts 4 van de vereiste AVG-onderdelen in uw privacyverklaring. Voeg minimaal toe: de rechtsgrondslag per verwerking, bewaartermijnen, doorgifte naar derde landen (relevant bij Google), en de rechten van betrokkenen inclusief hoe deze uit te oefenen. Gebruik de checklist van de Autoriteit Persoonsgegevens (autoriteitpersoonsgegevens.nl) als leidraad.

Gemiddeld · Geschatte tijd: **halve dag**

Met deze zes stappen legt u een solide privacyfundament en brengt u uw website niet alleen naar een 8.0, maar geeft u uw bezoekers het vertrouwen dat ze verdienen.

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.