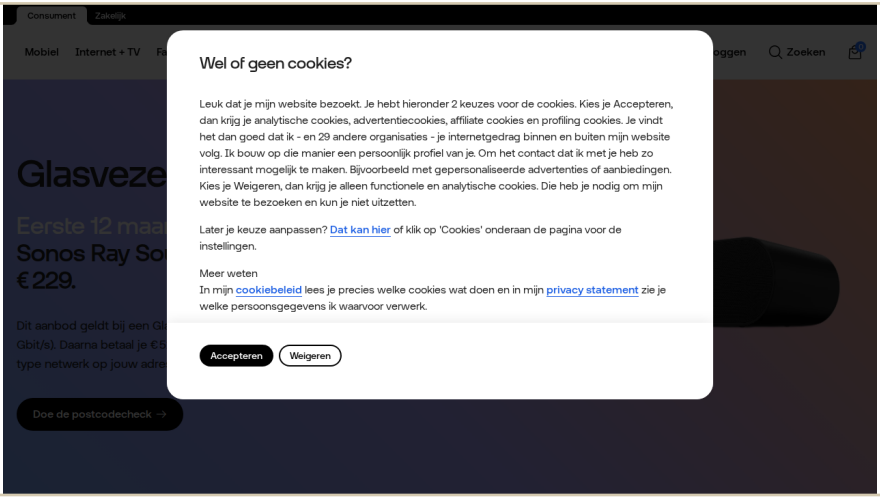
CookieChopper

Privacyscan — Verbeteradvies & Informatie

Website: **https://odido.nl/** · Datum: 25-04-2026 20:30



Screenshot zonder consent te geven.

3.0 **Rapportcijfer — Zeer slecht**

Persoonlijk bericht aan de website-eigenaar

Geachte Dames en Heren,

Op 25-04-2026 20:30 heb ik uw website https://odido.nl/ bezocht en een privacyscan uitgevoerd. De resultaten baren mij zorgen en ik deel ze graag met u.

Uw website scoort een 3.0 op een schaal van 10. Dat is rood. Dit betekent dat er serieuze problemen zijn die aandacht vragen. Concreet zag ik dat uw website gegevens doorstuurt naar vier verschillende partijen: Google Analytics, Google, Siteimprove en Google Tag Manager. Dit zijn zogenaamde trackers. Ze houden bij wat bezoekers doen op uw site.

U heeft wel een cookiebanner, dat is goed. Maar er is een groot probleem: als iemand op "weigeren" klikt, blijven de trackers gewoon actief. Dat voelt voor de bezoeker alsof hij een keuze heeft, maar in werkelijkheid verandert er niets. Dit noemen we schijnveiligheid. Een bezoeker denkt dat hij beschermd is, maar dat is hij niet. Dit is niet toegestaan volgens de wet.

Ik zag ook dat Consent Mode slechts gedeeltelijk is ingesteld. Dit is de technische instelling die ervoor zorgt dat trackers pas starten ná toestemming. Dat werkt nu dus nog niet helemaal goed.

Er is ook goed nieuws. U heeft een aangewezen privacyfunctionaris, ook wel Data Protection Officer genoemd. Die is vermeld op uw privacypagina en bereikbaar via dpo@odido.nl. Dat is een positief punt en laat zien dat u privacy serieus neemt.

De volgende stap is om de technische kant op orde te brengen, zodat "weigeren" ook echt weigeren betekent.

Dit rapport is gemaakt door CookieChopper, een onafhankelijke privacyscanner zonder winstoogmerk. Na het doorvoeren van verbeteringen nodigen wij u uit 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": **9 cookies**. Na het klikken op "weigeren": **17 cookies**.

KRITIEK: Er kwamen 8 cookies BIJ na het weigeren. In plaats van cookies te verwijderen, plaatst de website er meer.

2 hoog-risico tracker(s) bleven actief na weigeren: **_ga, _ga_2DEMN3VQTY**.

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-PX48MK3

→ https://www.googletagmanager.com/gtag/js?id=G-2DEMN3VQTY&cx=c&gtm=4e64m2

→ https://www.googletagmanager.com/a?id=G-2DEMN3VQTY&v=3&t=t&pid=765153603&gtm=45je64n0h2v874560465za20gzb...

Identificerende parameters: **cid=1898596117.1777141721, ecid=2027673163, pid=765153603, sid=3432366327307529**

Cookies: _ga=GA1.1.1898596117.1777141721, _ga_2DEMN3VQTY=GS2.1.s1777141721

Google Analytics via GA4 — Analytisch — risico: hoog

→ https://www.odido.nl/elmyra/g/collect?v=2&tid=G-2DEMN3VQTY&gtm=45je64m2v874560465z89122565658za20gzb9122565658zd...

Identificerende parameters: **tid=G-2DEMN3VQTY, cid=1898596117.1777141721, ecid=2027673163, _p=1777141720394**

Cookies: _ga_2DEMN3VQTY=GS2.1.s1777141721$o1$g0$t1777141721$j60$l0$h202767, _ga=GA1.1.1898596117.1777141721

Siteimprove Analytics — Analytisch — risico: middel

→ https://siteimproveanalytics.com/js/siteanalyze_6004843.js

→ https://6004843.global.siteimproveanalytics.io/image.aspx?url=https%3A%2F%2Fwww.odido.nl%2F&title=Odido%3A%20je%20pr...

Identificerende parameters: **accountid=6004843, luid=7db8e84a-fb3c-aae0-2bdd-ed897bb73070, prev=240a61cd-c633-2703-bf86-53d96cd417a5**

Cookies: nmstat=240a61cd-c633-2703-bf86-53d96cd417a5

Google Ads Conversion Tracking — Marketing — risico: hoog

→ https://pagead2.googlesyndication.com/ccm/collect?rcb=12&frm=0&ae=g&en=page_view&dl=https%3A%2F%2Fwww.od...

Identificerende parameters: **rnd=613454632.1777141721, rcb=12**

CIWSS — Marketing — risico: hoog

→ https://ciwss.com/index.php?94a08da1fecbb6e8b46990538c7b50b2=www.odido.nl&ad5f82e879a9c5d6b5b442eb37e50551=0a987f39d...

Identificerende parameters: **94a08da1fecbb6e8b46990538c7b50b2=www.odido.nl, ad5f82e879a9c5d6b5b442eb37e50551=0a987f39d2722610004ddb52b57a22f1**

Elastic APM RUM — Functioneel — risico: middel

→ https://unpkg.com/@elastic/apm-rum/dist/bundles/elastic-apm-rum.umd.min.js

→ https://unpkg.com/@elastic/apm-rum@5.17.4/dist/bundles/elastic-apm-rum.umd.min.js

→ https://da26b69ba06d492da337b32ae28a29b1.apm.eu-central-1.aws.cloud.es.io/intake/v2/rum/events

Identificerende parameters: **event_tracking_via_apm_endpoint**

Mopinion — Analytisch — risico: middel

→ https://deploy.mopinion.com/js/pastease.js

→ https://deploy.mopinion.com/config/OuUpMtNbySqQ1tBKQBWTfMAtUFMRJ4Bo1G5Z6SDj

→ https://deploy.mopinion.com/config/PBD9pwARRSOs27VujqMSjXQhIo8chuTBKuDizcFJ

Identificerende parameters: **config_id=OuUpMtNbySqQ1tBKQBWTfMAtUFMRJ4Bo1G5Z6SDj, config_id=PBD9pwARRSOs27VujqMSjXQhIo8chuTBKuDizcFJ**

Visual Website Optimizer — Tracking — risico: hoog

→ https://dev.visualwebsiteoptimizer.com/j.php?a=741212&u=https%3A%2F%2Fwww.odido.nl%2F&f=1&r=0.07931492062997...

→ https://dev.visualwebsiteoptimizer.com/cdn/web/djIkdGU6Ny4wOmFzeW5jJWdxdWVyeQ==/tag-71b55da48a4a43c893cee9eb8e65122ebr.j...

→ https://dev.visualwebsiteoptimizer.com/dcdn/settings.js?a=741212&settings_type=4&ts=1777117316&dt=desktop&am...;

Identificerende parameters: **a=741212, u=https://www.odido.nl/, r=0.07931492062997403**

Salesforce Live Agent — Functioneel — risico: middel

→ https://d.la1-c2-ar3.salesforceliveagent.com/content/g/js/61.0/deployment.js

Identificerende parameters: **X-Salesforce-CHAT_token**

Cookies: X-Salesforce-CHAT=!71+oWm0751N0YVTzzFXKgnYEZqwda8dqPJQQ5+jUFiRlyQI0mWCopk0DU9+ma

Awin Tracking — Marketing — risico: middel

→ `tracking_via_AwinChannelCookie`

Identificerende parameters: **AwinChannelCookie=direct, ServerAwinChannelCookie=direct**

Cookies: AwinChannelCookie=direct, ServerAwinChannelCookie=direct

*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 3.0 — er is duidelijk werk aan de winkel, maar het goede nieuws is dat de basis voor een sterke privacyaanpak al aanwezig is. Met een aantal gerichte verbeteringen brengt u uw score naar een 8.0 en laat u zien dat u de privacy van uw bezoekers serieus neemt.

Tip 1: Stop cookies plaatsen vóór consent

Op dit moment worden tracking-cookies geplaatst nog voordat een bezoeker toestemming heeft gegeven — dit is een directe overtreding van de AVG. Blokkeer alle niet-essentiële scripts en cookies volledig totdat een actieve keuze is gemaakt via uw cookiebanner. Dit is de meest urgente aanpassing en heeft de grootste impact op uw score.

Lastig · Geschatte tijd: **halve dag**

Tip 2: Installeer een erkende CMP-oplossing

Er is momenteel geen gecertificeerde Consent Management Platform (CMP) gevonden, terwijl uw cookiebanner niet geverifieerd functioneert. Implementeer een erkende CMP zoals Cookiebot, CookieYes of Usercentrics — deze tools zorgen automatisch voor correcte consent-registratie en blokkering van scripts. Kies bij voorkeur een CMP die IAB TCF-gecertificeerd is voor maximale compliance.

Gemiddeld · Geschatte tijd: **1 uur**

Tip 3: Verwijder cookies die bijkomen na weigeren

Bij het weigeren van cookies werden er extra cookies geplaatst, wat een ernstige overtreding is en uw Cookiebanner-score zwaar heeft gedrukt (-3.0). Controleer via Google Tag Manager welke tags en triggers actief blijven na een 'weigeren'-keuze en zorg dat deze volledig geblokkeerd worden. Test dit na implementatie met een browserinspectietool of via CookieChopper.

Gemiddeld · Geschatte tijd: **1 uur**

Tip 4: Rond Google Consent Mode v2 volledig af

Er is een gedeeltelijke implementatie van Consent Mode gedetecteerd (npa=1/gcs), maar de volledige Consent Mode v2 ontbreekt nog. Voeg in Google Tag Manager de parameters 'ad_storage', 'analytics_storage', 'ad_user_data' en 'ad_personalization' toe met een correcte standaardwaarde van 'denied'. Koppel dit vervolgens aan de consentstatussen uit uw CMP zodat de signalering volledig en correct werkt.

Gemiddeld · Geschatte tijd: **1 uur**

Tip 5: Beperk en documenteer de 4 hoog-risico trackers

Er zijn 8 tracker-implementaties gevonden, waarvan 4 als hoog-risico zijn aangemerkt: Google Analytics, Google (overig), Siteimprove en Google Tag Manager. Beoordeel per tracker of deze strikt noodzakelijk is en leg in uw privacyverklaring expliciet vast welke trackers worden gebruikt, met welk doel en op welke rechtsgrond. Verwijder trackers die niet langer actief worden gebruikt om het risicoprofiel te verlagen.

Gemiddeld · Geschatte tijd: **halve dag**

Tip 6: Voer een cookie-audit uit en actualiseer cookielijst

Zorg dat alle geplaatste cookies — inclusief die van Siteimprove en Google-diensten — volledig gedocumenteerd zijn in een actuele cookielijst op uw website. Gebruik een tool zoals Cookiebot Scanner of de auditfunctie van uw CMP om automatisch alle cookies te inventariseren en te categoriseren. Een transparante en actuele cookielijst verhoogt zowel uw AVG-compliance als het vertrouwen van uw bezoekers.

Makkelijk · Geschatte tijd: **30 min**

Met deze zes stappen legt u een solide privacyfundament en brengt u uw website naar de 8.0 die uw bezoekers verdienen — succes!

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.