

PRIVACY COMPLIANCE

Cookie Scanner Extension: Activation & First-Audit Guide

Install the free GetCookies Chrome extension in 4 minutes
and run a complete GDPR cookie audit of any site in 10

- ✓ Print-optimized
- ✓ Expert-curated
- ✓ Actionable tips

Cookie Scanner Extension: Activation & First-Audit Guide

Install the free GetCookies Chrome extension in 4 minutes and run a complete GDPR cookie audit of any site in 10

Cookie Scanner Extension: Activation & First-Audit Guide

Install the free GetCookies Chrome extension in 4 minutes and run a complete GDPR cookie audit of any site in 10

This guide walks you from a downloaded ZIP to a finished compliance audit. The Cookie Scanner is a Manifest V3 Chrome/Edge/Brave extension that lists every cookie on the current site, auto-categorizes them as **Necessary, Analytics, Marketing, or Other**, and flags the consent problems regulators actually fine for. Works on any site — yours or a competitor's.

Tested on Chrome 120+, Edge 120+, Brave, and Arc. ~3 MB, no account required, scans run entirely on your machine.

Part 1 — Install (4 minutes)

1. **Unzip** `cookie-scanner-extension.zip`. You'll get a folder containing `manifest.json`, `popup.html`, `popup.js`, `background.js`, and an `icons/` folder. Keep this folder somewhere permanent — deleting it removes the extension.
2. Open your browser and go to `chrome://extensions/` (Edge: `edge://extensions/`, Brave: `brave://extensions/`).
3. Toggle **Developer mode** ON (top-right corner).
4. Click **Load unpacked** and select the unzipped folder (the one that *contains* `manifest.json`, not the ZIP).
5. The "Cookie Scanner – GDPR Compliance Checker" tile appears. Click the **puzzle-piece icon** in your toolbar and **pin** it so it's always one click away.

You should now see the cookie icon in your toolbar. That's it.

Permissions it asks for (and why)

Permission	Why it's needed
<code>cookies</code>	Read the cookies set on the page you're auditing
<code>activeTab</code>	Know which site you're currently on
<code>storage</code>	Remember your last scan locally (nothing is uploaded)
<code><all_urls></code>	Let you scan any website, not just one

Part 2 — Run Your First Audit (10 minutes)

Do this in an **incognito window** so previous browsing doesn't pollute the results.

1. Open a new **incognito** window (Cmd/Ctrl+Shift+N). Enable the extension for incognito if prompted (Details → "Allow in Incognito").
2. Navigate to the site you want to audit. **Do not click the cookie banner yet.**
3. Click the **Cookie Scanner** icon. It lists every cookie with its name, domain, category, and expiry.
4. Note the **pre-consent count** — these are the cookies set *before* the visitor agreed to anything.
5. Now click **"Reject All"** on the site's banner, refresh, and scan again. Compare the counts.

What "good" looks like

- **Before consent:** only Necessary cookies (session, CSRF, the consent cookie itself).
- **After Reject All:** Analytics and Marketing cookies are gone.
- **After refresh:** the banner does **not** reappear (the choice was stored).

If Analytics or Marketing cookies appear *before* consent, that's the #1 most-fined violation in the EU.

Part 3 — Reading the Results (cheat sheet)

Category	Examples	Allowed before consent?
Necessary	<code>session_id</code> , <code>XSRF-TOKEN</code> , <code>cookie_consent</code>	✅ Yes
Analytics	<code>_ga</code> , <code>_gid</code> , <code>_ga_*</code> , Plausible, Hotjar, Mixpanel	❌ No — needs opt-in
Marketing	<code>_fbp</code> , <code>_fbclid</code> , <code>fr</code> , <code>IDE</code> , <code>test_cookie</code> , TikTok	❌ No — needs opt-in
Other / Unknown	Anything uncategorized	⚠️ Investigate — uncategorized often means an undisclosed tracker

Red flags the scanner surfaces:

- Analytics/Marketing cookies present at the pre-consent scan
 - More cookies live than your cookie policy discloses
 - Third-party cookies with long expiries (>13 months violates several guidelines)
 - "Other/Unknown" cookies you can't explain — these need a vendor and a purpose
-

Part 4 — 5-Point Pass/Fail Audit Worksheet

Run this on every site and tick the boxes. Three or more fails = urgent remediation.

- ☐ **Pre-consent test:** Only Necessary cookies present before any banner click

- ☐ **Reject-All test:** Non-essential cookies removed after clicking Reject All
- ☐ **Persistence test:** Choice remembered on refresh (banner doesn't reappear)
- ☐ **Disclosure test:** Every cookie the scanner finds is named in the cookie policy
- ☐ **Expiry test:** No non-essential cookie lives longer than 13 months

Record the date, URL, pre-consent count, and post-reject count so you can prove improvement over time.

Troubleshooting

Symptom	Fix
Extension won't load	You selected the ZIP or a parent folder. Re-select the folder that directly contains <code>manifest.json</code> .
"Manifest version 2 is deprecated" or load error	Make sure you unzipped the latest build — this is Manifest V3.
No cookies show	Refresh the tab, then reopen the popup. The scanner reads the active tab on open.
Doesn't work in incognito	<code>chrome://extensions/</code> → Cookie Scanner → Details → enable "Allow in Incognito".
Changed files but nothing updates	Click the reload icon on the extension tile in <code>chrome://extensions/</code> .
Icon missing from toolbar	Click the puzzle-piece icon and pin it.

Part 5 — From Audit to Fixed

The scanner tells you *what's* wrong. Fixing it means blocking non-essential tags until consent, adding an equal-weight Reject All button, and keeping an exportable consent log. That's exactly what GetCookies automates:

- Auto-blocks Analytics & Marketing tags until the visitor opts in
- Equal-weight Accept All / Reject All by default — compliant on install
- Google Consent Mode v2 + GTM ready
- Recurring scans that alert you when new cookies appear
- Audit-ready, exportable consent records

Scan your full site and fix it free → getcookies.co

This guide and extension are for informational purposes and do not constitute legal advice.