Website Tracking & Consent Checklist

A plain-language review guide for business owners before installing or continuing to use Google Analytics, Google Tag Manager, Meta/Facebook Pixel, Microsoft Ads, email tracking, abandoned cart tools, or other third-party scripts.

Purpose: Use this checklist to understand what your website tracks, which third parties receive data, what happens before and after consent, and whether your privacy policy matches what your website actually does.

This checklist is educational and is not legal advice. For legal decisions, review your setup with qualified legal counsel.

1. Inventory Every Tracking Tool

Start by identifying every script, pixel, tag, plugin, and outside platform connected to the website. Do not assume analytics tools are the only tools collecting data.

- ■ Google Analytics is installed or confirmed not installed.
- ■ Google Tag Manager is installed or confirmed not installed.
- ■ Meta/Facebook Pixel is installed or confirmed not installed.
- ■ Microsoft/Bing Ads tracking is installed or confirmed not installed.
- ■ Email marketing, abandoned cart, review, chat, heatmap, affiliate, and retargeting tools have been reviewed.
- ■ A written list of all third-party scripts and tools has been created.

2. Identify What Each Tool Collects

For each tool, document the data it may collect or receive. Vague answers like "just analytics" are not specific enough.

- ■ Page views are reviewed.
- ■ Clicks, button clicks, and form interactions are reviewed.
- ■ Add-to-cart, checkout, purchase, and conversion events are reviewed.
- ■ Product names, categories, order values, transaction IDs, or purchase totals are reviewed.
- ■ Names, email addresses, phone numbers, addresses, or account details are reviewed.
- ■ Cookies, client IDs, user IDs, ad click IDs, IP addresses, browser, device, or location data are reviewed.
- ■ The business knows whether any personal or customer data is sent to analytics or advertising platforms.

3. Review Consent Timing

The timing of tracking matters. A consent banner is only meaningful if the website behavior matches the user choice.

Question	Why It Matters
What loads before the user makes a choice?	This shows whether tracking happens before consent.
What happens when the user clicks reject?	Reject should mean something real, not just close the banner.
Which tags are considered necessary?	Necessary tools should be limited to what the website truly needs to function.

Question	Why It Matters
Which tags are analytics?	Analytics tools should be separated from advertising and personalization when possible.
Which tags are marketing or advertising?	These usually carry higher privacy risk and should be handled carefully.
Is any purchase or customer data being shared?	Transaction data may create higher risk if it can be tied to a user.
Can the business prove how consent works?	Documentation matters if the setup is ever questioned.

4. Classify Tools by Purpose

Not every tool has the same privacy risk. Separate tools by what they do so users can be given meaningful choices.

Category	Examples	Consent Review
Necessary	Shopping cart, security, fraud prevention, basic site functionality	Should be limited to what the site truly needs to function.
Analytics	Google Analytics, analytics events, reporting tools	Review whether these load before consent and what identifiers are used.
Marketing / Advertising	Meta Pixel, Google Ads, Microsoft Ads, retargeting tools	Usually higher risk; should be handled carefully and often blocked until consent.
Personalization	Recommendations, behavioral personalization, user profiling	Review whether this creates profiling or tracking over time.
Email / Abandoned Cart	Email capture, browse abandonment, checkout abandonment	Review carefully because these may involve identifiable customer behavior.

5. Compare Common Consent Choices

There is not one perfect setup for every business. The best choice is the one the business can clearly explain, document, and defend.

Consent Setup	How It Works	Risk Level
No tracking until consent	Analytics and marketing scripts do not load unless the user accepts.	Lowest privacy risk; less reporting visibility.
Basic analytics before consent	Limited analytics may load, while marketing and personal-data tracking are blocked.	Medium risk; depends heavily on setup.
Full tracking unless rejected	Tracking starts on page load unless the user opts out.	Higher risk; weaker user control.
Category-based consent	Users choose between analytics, marketing, personalization, or other categories.	Low/Medium risk if configured correctly.
No third-party tracking	The website avoids outside analytics or marketing tools.	Lowest privacy risk; high business cost.

6. Match the Website to the Privacy Policy

The privacy policy, cookie banner, and website behavior should tell the same story. If the policy says certain tracking only happens after consent, the website should actually work that way.

- ■ The privacy policy lists the major categories of tracking tools used.
- ■ The cookie banner explains choices in plain language.
- ■ The reject option blocks nonessential analytics, marketing, and advertising tags as intended.
- ■ The accept option updates consent settings and allows only the tags that match the user choice.
- ■ The privacy policy and actual website behavior have been compared by someone technical.

7. Keep Documentation

Documentation helps show that the business made a thoughtful decision instead of guessing. Keep a record of what was reviewed and why the final setup was chosen.

- ■ A tracking inventory has been saved.
- ■ Consent settings and GTM/tag settings have been documented.
- ■ Screenshots or notes show what happens before consent, after accept, and after reject.
- ■ The business has documented why it chose its consent approach.
- ■ A reminder has been set to review the setup again when tools, laws, or marketing platforms change.

> **Final check:** A business owner should be able to answer four questions clearly: What are we collecting? Who receives it? When does tracking start? What happens when the user says no?