

The Consent and Privacy-Aware Measurement Cookbook

How to set up cookie consent, Google consent mode and GA4 data settings, where server-side tagging helps and does not, and how to document data flows before you ask counsel to review them.

Contents

01 What the law asks of you, in practical terms

02 Cookie consent that changes what the tags do

03 Google consent mode: what it does and what it does not

04 GA4 settings to choose on purpose

05 Server-side tagging: the benefit and the limit

06 Documenting data flows, with a build checklist

Key Takeaways & Sources

01

What the law asks of you, in practical terms

Two regimes drive most of the work for a site with visitors in both Europe and California, and they ask for different things. In the EU, the baseline is prior consent. The GDPR sets conditions for valid consent, and the ePrivacy Directive requires consent before storing or reading information on a visitor's device, with narrow exceptions for what is strictly necessary to deliver the service the visitor asked for. The UK has a parallel rule in the Privacy and Electronic Communications Regulations (regulation 6), which was substituted in February 2026 by the Data (Use and Access) Act 2025 and now works through listed exceptions, so check the current UK text rather than assuming it matches the EU. On what counts as consent, the GDPR's Recital 32 describes a clear affirmative act that is freely given, specific, informed and unambiguous, and says silence, pre-ticked boxes or inactivity should not constitute consent. The European Data Protection Board's guidelines on consent expand on these conditions.

California works differently. The CCPA, as amended by the CPRA, is built around notice and the right to opt out of the sale or sharing of personal information, and it covers businesses that meet its thresholds. The statute (California Civil Code section 1798.135) lets a business meet the opt-out requirement through a "Do Not Sell or Share My Personal Information" link or by honouring an opt-out preference signal sent with the consumer's consent. The state's privacy agency publishes the implementing regulations and was still running rulemaking activity on opt-out preference signals when we last checked, so confirm the current text. In practice, that means a visitor may be able to opt out through a link on your site or through a browser signal, and your tags need to respect whichever route applies to you. Whether the law applies to you at all depends on your size and what you do with data, so this is a question for counsel before it is a question for your tag manager.

None of this is a substitute for advice. Consent rules vary by country and change by guidance and enforcement, so treat the points here as an outline for the conversation with counsel, not as a conclusion. The most useful preparation you can do is document what your site actually does, which is the subject of the data flow section below.

Whether the law applies to you at all depends on your size and what you do with data, so this is a question for counsel before it is a question for your tag manager.

02

Cookie consent that changes what the tags do

A consent management platform, or CMP, shows the banner, records the visitor's choice and exposes it to your tags. The test of a good setup is behavioural: with consent refused, do analytics and advertising tags stop setting identifiers, and does the page still work? Open the site in a clean browser profile, refuse everything, and check what cookies and network requests appear. Do this again after any tag or banner change, because a new marketing tag added by someone else is the usual way a working setup breaks.

Design the choices honestly. Rejecting should be as easy as accepting, and the categories should match what tags really do. Group tags by purpose, such as strictly necessary, analytics, advertising and functional, and make sure each tag in your tag manager is assigned to one category and fires only when that category has consent. Keep the visitor's choice for a defined period, make it easy to change later, and keep a record of the consent state that your CMP supports. If your CMP offers a regional rule set, configure the defaults separately for regions where prior consent is required and where an opt-out model is allowed, and have counsel confirm the mapping.

- Refuse-all test in a clean profile after every tag or banner change
- Every tag assigned to exactly one consent category
- Reject as prominent as accept, with no pre-ticked categories
- A visible control to reopen preferences and change the choice
- Regional defaults set deliberately and reviewed by counsel

Rejecting should be as easy as accepting, and the categories should match what tags really do.

03

Google consent mode: what it does and what it does not

Consent mode is a way for your site to tell Google tags what the visitor has agreed to, so the tags adjust their behaviour. Google's documentation lists the consent types: `ad_storage`, `analytics_storage`, `ad_user_data` and `ad_personalization`. You set a default state, normally denied for regions that require prior consent, before the tags load, and then update it when the visitor makes a choice. The documentation also describes a `wait_for_update` setting that holds the default for a short time so a CMP can pass a stored choice before tags fire, and `url_passthrough` and `ads_data_redaction` settings that change how Google handles ad click information when storage is denied.

It helps to understand the two implementation styles described in Google's documentation. In a basic implementation, Google tags are blocked from loading until the visitor consents. In an advanced implementation, tags load with defaults set to denied and send limited signals that do not use cookies or

identifiers, and Google can use those signals for modelling in some of its products. Which is right for you is a legal and a business decision. The advanced option collects more signal; whether it is acceptable for your audience and jurisdictions is for counsel to confirm.

Consent mode is not a CMP, and installing it does not collect a lawful consent. It carries the choice your CMP collected. If your banner is misleading, consent mode will faithfully pass along a misleading choice. Check that your CMP is integrated with the Google tag, that the default and update calls fire in the right order, and use tag diagnostics to confirm the consent states Google tags see.

It helps to understand the two implementation styles described in Google's documentation.

04

GA4 settings to choose on purpose

Google Analytics 4 has a handful of settings that determine how long data is kept and what extra signals it collects. Event-level data retention is configurable, so check the setting in each property rather than assuming the default, and choose the period you can justify against your reporting needs. Google's help documentation describes which reports the setting affects and which retention options are available; read the current version when you decide, since the options can change.

Review the data collection settings: whether Google signals is on, whether user-provided data collection is enabled, what advertising features are linked, and which data-sharing settings are active. Each of these widens what is collected or shared, so each should be a documented decision with an owner. Also check that you are not sending personal data into analytics by accident. URLs and event parameters are the common leak: email addresses in query strings after a form submission, names in page titles, or customer IDs in custom dimensions. The Google Analytics Terms of Service (section 7) say you must not pass information to Google that Google could recognise as personally identifiable information, with limited exceptions for features that permit hashed data, so audit URLs and parameters, and strip them at the source or with tag manager rules.

Finally, consider IP handling and data deletion. Know how to process a deletion request in the properties you operate, and who is responsible for doing so. This is part of the operating procedure and belongs in the register.

Setting	Decision to make	Record
Event data retention	How long do reports and explorations need user-level data?	Chosen period and reason

Setting	Decision to make	Record
Google signals	Do you need cross-device or demographic reporting enough to enable it?	On or off, and who approved it
User-provided data collection	Do you send hashed contact data for enhanced conversions or similar?	Enabled or not, with the legal basis counsel confirmed
Advertising product links	Which Google Ads or other accounts receive data?	List of linked accounts and owners
Data-sharing and access	Who outside the company can see the property?	Access list reviewed quarterly
URL and parameter hygiene	Do any URLs or events contain personal data?	Audit date and fixes made

05

Server-side tagging: the benefit and the limit

In server-side tagging, the browser sends events to an endpoint you control, and that server forwards them to analytics and advertising vendors. Google Tag Manager supports this with a server container. The benefits are practical. Google lists better page performance, more detailed privacy controls and better data quality among the benefits, and the setup lets you serve the tagging endpoint from your own domain. In practice that means you can decide which fields leave your environment, and you can reduce the number of third-party scripts in the page.

The limit is that server-side tagging does not change whether you need consent. If a visitor refused consent for advertising, forwarding the same event from your server to an advertising platform is, in our view, still processing the data for that purpose. The server needs to receive the consent state with each event and honour it in the forwarding logic. Treat the server container as a place to enforce the rules, not a way around them. It also adds cost and operational work: hosting, monitoring and a person who knows how to maintain it. For a small site with a handful of tags, a clean client-side setup with a working CMP is often the better first step.

06

Documenting data flows, with a build checklist

A data flow register lists every place your site collects data, what is collected, why, where it goes, how long it is kept and who owns it. For each tag, cookie, form and integration, record the vendor, the purpose, the consent category, what happens when consent is refused and the retention period. The GDPR expects some organisations to keep records of processing activities, and whether yours must is a question for counsel, but the register is useful regardless. It lets a new team member understand the setup in an hour and lets counsel review facts rather than guesses.

Build the register from evidence. Crawl the site with a clean browser profile and list the cookies and requests you see before and after consent. Compare that with the tag manager. Differences between the two are where problems hide: tags hard-coded in templates, scripts added by plugins, and embedded content such as videos and maps that set their own cookies. Then work through the checklist below and re-run it whenever a tag is added.

Step	Owner	Gate to pass before moving on
Crawl the site in a clean profile and export cookies and third-party requests before consent	Analytics lead	Every request and cookie is matched to a vendor and a purpose, or flagged as unknown
Assign each tag in the tag manager to a consent category	Analytics lead	No tag is left without a category; no tag fires before its category is granted
Configure the CMP with defaults per region and test refuse-all	Web developer	Refuse-all test shows no analytics or advertising identifiers set
Set consent mode defaults and updates, and test the order of calls	Web developer	Tag diagnostics show denied by default and updated after choice
Set GA4 retention, signals and data-sharing and record the reasons	Analytics lead	Each setting has an owner and a written reason in the register
Audit URLs, parameters and form events for personal data	Analytics lead	No email addresses, names or IDs appear in analytics reports
Send the register and privacy notice to counsel for review	Business owner	Written feedback received and actions assigned
Schedule a re-test after each tag change and every quarter	Business owner	Next review date entered in the register

Key Takeaways

- Consent is a state your tags must respect before they fire. A banner that records a choice but does not change tag behaviour is decoration.
- Google consent mode passes consent signals to Google tags. It does not collect consent, and it does not make a site compliant by being installed.
- Set GA4 data retention, Google signals and user-level data deliberately, and write down what you chose and why.
- Server-side tagging gives you more control over what leaves the browser. It does not remove the need for consent.
- A data flow register, kept current, is the most useful thing you can hand to counsel. This cookbook is a practical outline and not legal advice.

Sources

1. Consent mode overview and implementation (Google tag platform) — <https://developers.google.com/tag-platform/security/guides/consent>
2. Server-side tagging with Google Tag Manager — <https://developers.google.com/tag-platform/tag-manager/server-side>
3. Google Analytics Terms of Service — <https://marketingplatform.google.com/about/analytics/terms/us/>
4. GDPR Recital 32: conditions for consent — <https://gdpr-info.eu/recitals/no-32/>
5. Privacy and Electronic Communications Regulations 2003, regulation 6 (legislation.gov.uk) — <https://www.legislation.gov.uk/uksi/2003/2426/regulation/6>
6. California Civil Code section 1798.135 (opt-out links and preference signals) — https://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV§ionNum=1798.135
7. Regulation (EU) 2016/679, the General Data Protection Regulation — <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
8. Directive 2002/58/EC, the ePrivacy Directive — <https://eur-lex.europa.eu/eli/dir/2002/58/oj>
9. EDPB Guidelines 05/2020 on consent under Regulation 2016/679 — https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en
10. California Attorney General: California Consumer Privacy Act — <https://oag.ca.gov/privacy/ccpa>
11. California Privacy Protection Agency: regulations — <https://cppa.ca.gov/regulations/>