Whitepaper

Mastering first-party measurement

A comprehensive whitepaper on the privacy-first digital advertising era

November 2026

optout



The future of privacy-first advertising

Discover how to keep digital advertising relevant and measurable in a cookieless world.

As traditional tracking methods become less effective and consumers demand greater control over their data, advertisers face a new challenge: how to measure campaign performance without relying on cookies or personal identifiers.

In this whitepaper, we explore practical strategies, technologies, and tools to future-proof your analytics setup. From server-side tracking and consent modes to privacy-first measurement solutions.

After reading this whitepaper, you'll have actionable insights and practical guidance to optimise your analytics implementation, minimise measurement gaps, and gain a more complete picture of campaign performance, even without user consent.

01 The rise & fall of the cookie era 4
02 Under the hood: Privacy-by-design ad server 9
03 The measurement playbook 15
04 Actionable architecture 19
05 Vendor consent solutions 27
06 From setup to strategy 32
07 Market use case & final thoughts 39
A Technical appendix 45

Chapter 1

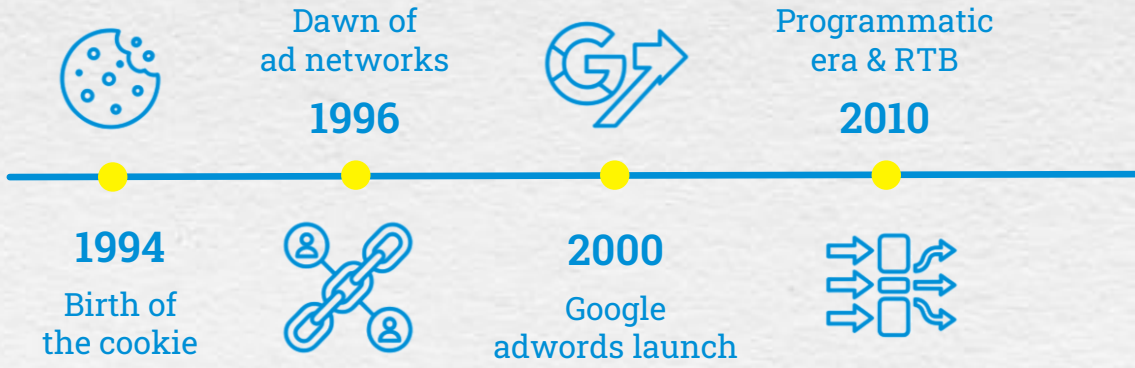
The rise & fall of the cookie era

The rise & fall of the cookie era

The evolution of digital tracking

The internet was not built to track people. In the mid-1990s, cookies were created as a simple tool to help websites remember basic things, like keeping items in a shopping cart or remember a user after logging in so they didn't have to login every time they wanted to use their account.

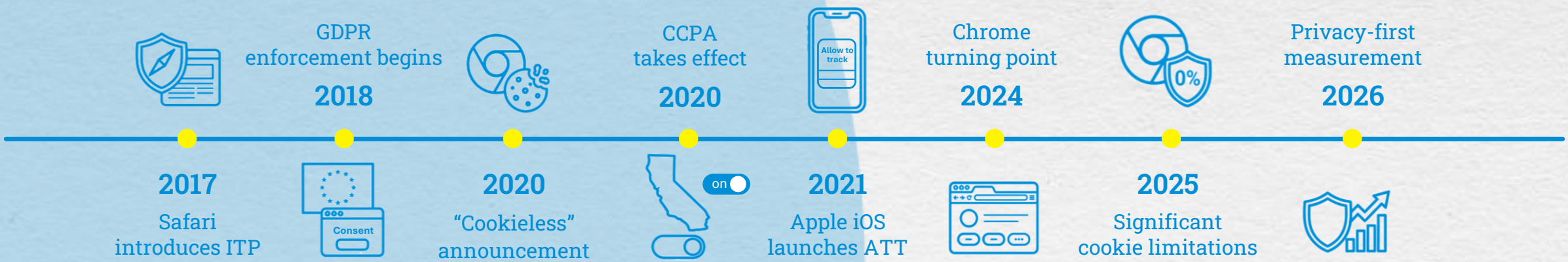
They were not meant to be used for spying on users. However, early web browsers like **Netscape Navigator and Internet Explorer ignored advice from tech experts to block third-party cookies by default.** This gave the modern digital advertising industry the perfect tool to track users across the web. As social media platforms like MySpace and Facebook became popular, users got used to sharing their personal thoughts, locations, and interests in exchange for free services.



With so much behavioral data available, the advertising industry changed its strategy. **Instead of targeting ads based on the content of a web page (contextual targeting), advertisers started building massive profiles to target individual people based on their past behavior.**

This data powered the complex real-time bidding (RTB) systems that defined the "Golden era" of digital marketing and user tracking.

The privacy reckoning



The era of tracking everything eventually broke down due to a perfect storm of three main factors.

Legislation

Governments created laws to protect users. The European Union introduced the GDPR, and California introduced the CCPA, making it mandatory for websites to ask for user consent before tracking them. The rules continue to get stricter, in order to respect the user's privacy.

Tech blockades & fragmented signals

Major technology companies have increasingly restricted cross-site tracking and user-level identifiers. Apple introduced Intelligent Tracking Prevention (ITP) in Safari to limit cross-site tracking, while App Tracking Transparency (ATT) introduced explicit permission requirements for tracking across apps on iOS.

Consumer pushback

People wanted more control over their data. Because privacy laws now require clear "Reject all" button on cookie banners. The number of users rejecting cookies has jumped from a historical 5-10% to around 25-40%.

The measurement blind spot

These changes broke the basic math of digital marketing.

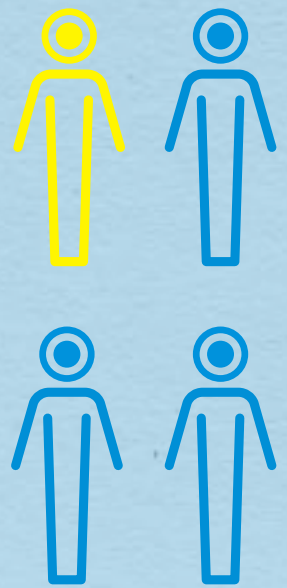
Old ways of measuring success, like **last-click attribution**, rely on tracking a user's exact path across the internet. Without cookies and user identifiers, these models no longer work properly.

For publishers, this creates a major problem. If they cannot track a user, traditional programmatic buyers will not buy the ad space. **Without preparation, ad revenue from these users can easily drop by 30% to 40% immediately.**

Advertisers also suffer. Because they can only target the shrinking group of users who still click "Accept all", there is too much competition. This drives up the cost per mille (CPM) and makes advertising much more expensive for a smaller audience.

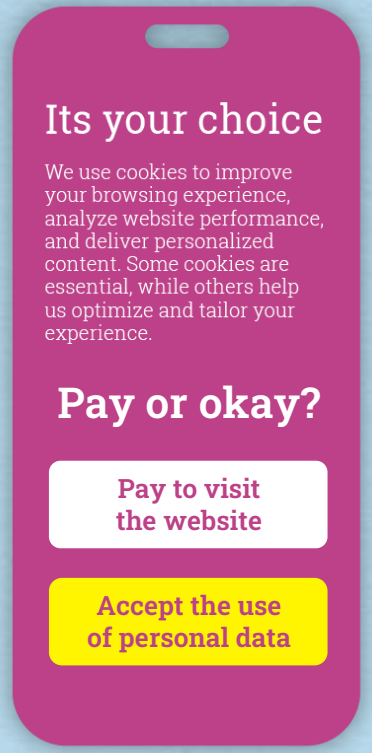


With 25% to 40% of internet traffic actively rejecting cookies, marketers are missing a huge amount of data.



To fix this revenue loss, some companies try to use risky tricks. For example, "browser finger printing" tries to identify users based on their device details (like IP address or screen size) without using cookies.

However, this is legally risky under the GDPR and is constantly blocked by new browser updates. Other websites use **"pay-or-okay" models**, where users must either pay a subscription fee or agree to be tracked. These models are facing heavy legal pressure and fines from European regulators. For instance, DerStandard, an Austrian newspaper was taken to court for introducing the 'Pay or okay' model.



The crossroad: Workarounds vs real solutions

Instead of fighting the privacy trend with these workarounds, forward-thinking brands and publishers are adopting a genuine, future-proof alternative: a privacy-by-design ad server.

This approach goes beyond just non-consent, for instance, political ads are prohibited from using any personal data, even when consent has been provided.

Source: Court decides "Pay or okay" on DerStandard.at is illegal

Chapter 2

Under the hood: What is a privacy-by-design ad server

Under the hood: What is a privacy-by-design ad server

Defining the technology

A privacy-by-design ad server is a new type of technology built specifically for the privacy era. It is a privacy-first infrastructure designed to deliver highly relevant ads and measure performance without reading, writing, storing, or requiring user identifiers (cookies, IP addresses or otherwise).

This makes it possible to serve ads to people who opt out of using their data for advertising purposes, but also to serve ads where user identifiers are not allowed in any case.

The core philosophy of a privacy-by-design ad server is simple: you do not need to know who a person is to know what they are interested in at that exact moment.

By separating ad relevance from personal identity, this system respects user privacy entirely while still delivering the results that brands need.

The core philosophy: Decoupling relevance from identity

The mechanics of a consentless ad

The trigger

A user visits a website and clicks "Reject all" on the cookie banner. Because of this choice, the system respects their privacy:

No cookies are stored in their browser, and no personal ID is created or passed along



Contextual 2.0

(Real time AI)

Because the server cannot scan the user's history, it instantly scans the environment instead. Using artificial intelligence and natural language processing (NLP), the server analyzes the webpage in a matter of milliseconds.

This advanced technology goes far beyond simply matching keywords. It understands the true semantic meaning of the text.

The match

The server matches the advertiser's intent with the suitable domains and page's context, serving the ad instantly.

How does it actually work? Here is a step-by-step breakdown of how the server operates:

The mechanics of a consentless ad

Contextual 2.0

(Real time AI)

- It knows the difference between an article about **"Jaguar" the animal** and **"Jaguar" the luxury car** brand.
- It also performs **"sentiment analysis"** to check if the tone of the article is positive, negative, or neutral, which keeps the advertiser's brand safe.
- But it also uses **panel data** to determine if one domain is mostly visited by a certain target audience.
- **No one-on-one match is being made,** but there is a strong likelihood that you will reach your target audience on those domains.

Example



JAGUAR

Targeting in a consentless world

In this new world, advertisers must change how they define their audiences.

Instead of relying on behavioural profiles like, "Target 18-35-year-old males who like sports," the strategy shifts to "Target high-attention environments discussing upcoming athletic events with a positive tone."

Advertisers can also use environmental triggers, like the local weather or the time of day, to make the ads even more relevant to the user's current situation.



Target 18-35-year-old males who like sports.

Target high-attention environments discussing upcoming athletic events with a positive tone.



Quality over quantity: The shift to attention metrics



Stop counting impressions, start counting attention

In traditional advertising, "reach" (how many times an ad loads on a page) is the main goal. But reach is a useless vanity metric if users are instantly scrolling past the ads. **Studies show that only about 30% of viewable ads are actually looked at by users.**



The power of being relevant

When you place ads based on the content of the page, rather than tracking the user across the internet, people naturally stop and look. **This contextual alignment creates a "high-attention" environment.**



Measuring what matters

Instead of relying on cookies to track users, forward-thinking brands prove campaign success by measuring "attention." **This means looking at how long users actually look at an ad, also known as 'dwell' time.**

Research proves that high-attention ads deliver real business impact, leading to a 130% increase in conversion rates compared to low-attention ads.

Source: Attention technology: What advertisers need to know survey: The attention metrics landscape in 2024

Chapter 3

The measurement playbook: Proving ROI without trackers

The measurement playbook: Proving ROI without trackers

Moving past last-click



For years, marketers relied on a method called "Last-click" attribution. This method gives 100% of the credit for a sale to the very last ad a person clicked.

However, this is a flawed system because it completely ignores all the other ads and research the customer did before making a purchase.

In a privacy-first world where tracking users is restricted by updates like Apple's App Tracking Transparency (ATT), trying to follow the exact path of a single person is practically impossible.

Marketers must abandon the illusion of perfect tracking and embrace new methods that measure success without needing personal identifiers.

The return of Marketing Mix Modelling

Because tracking individual users is getting harder, an older but powerful method is making a huge comeback: Marketing Mix Modeling (MMM).

MMM does not look at individual people, instead, it analyzes large sets of aggregated data. It compares a company's total advertising spend across different channels with outside factors like the season, the economy, or competitor actions.

Using statistical modelling, MMM estimates the incremental contribution of different marketing channels to business outcomes such as sales or revenue.

MMM

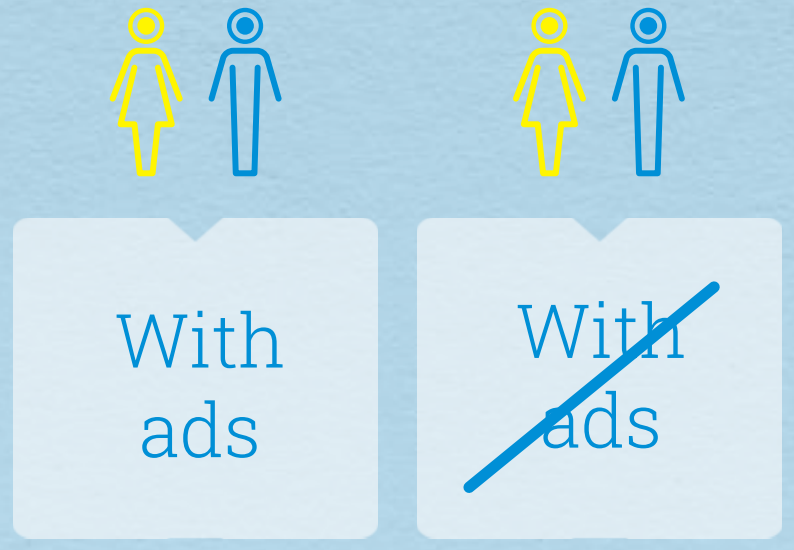
Because MMM operates on aggregated marketing and business data rather than individual user journeys, it does not depend on browser cookies or user-level identifiers.

Incrementality testing

When it comes to budgets, business leaders really only care about one question:

"Would this customer have bought our product even if they never saw the ad?".

Incrementality testing answers this questions by running real-world experiments.



Instead of just tracking clicks, marketers will show ads to one group of people (or one city) and hide them from another similar group.

By comparing the sales between the two groups, they can see the exact, real impact the advertising had.

This proves the true return on investment (ROI) without relying on any personal trackers.

Chapter 4

Actionable architecture: Future-proofing your stack

Actionable architecture: Future-proofing your stack

In the modern digital ecosystem, advertisers frequently encounter strict "no-consent environments." These occur when traffic originates from privacy-first browsers (like Brave or Safari with ITP enabled), strictly regulated publisher apps, or regional broadcasters operating under rigid local interpretations of the ePrivacy Directive and GDPR.

When a user explicitly denies consent, the tracking infrastructure fundamentally breaks. Client-side cookies cannot be written or accessed. Standard ad click identifiers, such as Google's gclid or Meta's fbclid, are frequently stripped by browser link-tracking protection features.

However, despite these restrictions, certain stateless data inherently remains available immediately post-click. **Before any script executes or a consent banner is interacted with, the initial HTTP server request still transmits the referrer data, the timestamp, and most importantly, the URL query parameters.**

Capturing these parameters ethically is the foundation of no-consent measurement.

The current landscape & the “No-consent” challenge

Transitioning to event-based data

To survive in a world without tracking cookies or user identifiers, businesses need to change the technical foundation of their websites. In the past, analytics tools focused on tracking who the user was by following their session or user ID using cookies.

As these personal identifiers disappear, companies must shift their focus to what happened. This is called an "event-based" data model. In this model, every single action, like loading a page, clicking a button, or buying a product, is measured as an independent event, without needing to know the identity of the person who did it.

This makes tracking highly flexible and safe for the future.

Advanced UTM architecture for stateless tracking

When third-party identifiers are blocked, standard Urchin Tracking Module (UTM) parameters `(utm_source, utm_medium, utm_campaign, utm_content, utm_term)` **provide a durable layer of campaign metadata** that can preserve campaign context even when user-level identifiers are unavailable.

UTMs do not require cookies to function, they are simply text appended to a URL.

To utilize UTMs effectively in a no-consent world, organizations must deploy an advanced, standardized naming convention framework.

utm_source
utm_medium
utm_campaign
utm_content
utm_term

Strict lowercase enforcement

Analytics platforms are case-sensitive.

`utm_source=Optout`

and

`utm_source=optout`

will fragment your data into two separate sources.

Enforce strict lowercase across all variables.

The key-value or positional model

Instead of basic naming, advanced advertisers use intentional structure within the utm_campaign parameter to pack in trackable variables. For example, structuring it as country-objective- product-date, i.e:

`utm_campaign=nl-awareness-fashion-q4`

Ensures that even if all other data is lost, the URL alone provides deep campaign context.

Eliminate spaces

Never use spaces, which render as “%20” and break URL parsing.

Use hyphens (-) or underscores (_) consistently.

To utilize UTMs effectively in a no-consent world, **organizations must deploy an advanced, standardized naming convention framework.**

Server-side tracking as a shield

The most important technical upgrade a company can make today is moving to server-side tracking (SST).

Traditionally, tracking happened on the "client-side." This meant third-party code (like Google or Facebook tags) ran directly in the user's web browser, collecting data and sending it to external companies. This old method is vulnerable to ad blockers and strict browser privacy rules. Server-side tracking changes the game. Instead of letting third parties collect data directly from the user's browser, the website sends a single stream of data to its own secure, company private server.



The company acts as a shield. It can clean this data, remove any personally identifiable information (PII) like IP addresses, user agents, names or emails remaining in the URLs, and only share what is strictly necessary and legal.

First-party data: Leveraging user IDs and hashed emails

Deterministic user IDs

If a user logs in or registers on your site, assign them a unique, internal user ID.

Passing this ID to your analytics tool allows you to stitch their behavior across devices, browsers, and offline channels without relying on fragile, client-side cookies.

The platform match

When users fill out a form or complete a purchase, capture their email address, **hash it locally using secure SHA-256 encryption,** and pass it to your server-side container.

Hashed customer data

(emails, phone numbers, postal code)

These secure, hashed emails are used by platforms (like Google's Enhanced Conversions or Meta's Conversions API) to match the anonymous website interaction back to a logged-in Google or Facebook account.

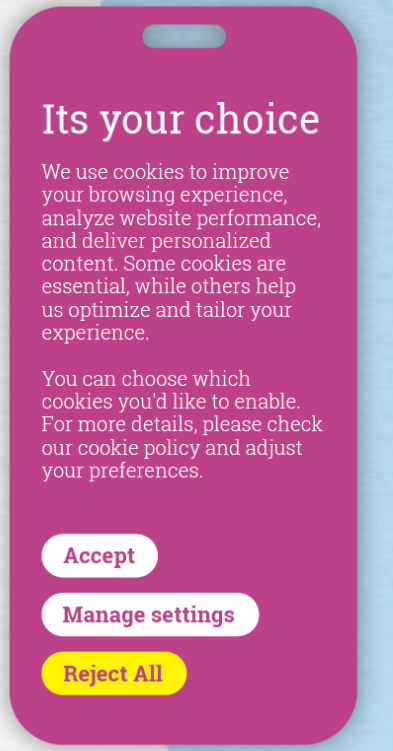
This restores precise attribution for users who completed a conversion after clicking an ad, even if they rejected cookies on your website.

When browser cookies are blocked, your best alternative is consented first-party data. **Instead of relying on anonymous browser signals, you use deterministic, user-provided identifiers to stitch customer journeys together.**

The smart gatekeeper

A secure server is useless if it does not respect what the user actually wants. This is where the consent management platform (CMP), the cookie banner you see on websites, acts as a "Smart gatekeeper."

When a user clicks "Accept" or "Reject all" on the banner, that choice must be instantly sent to the server. The server then uses this "consent state" as a strict rule before processing any data. If the user rejects cookies, the server blocks all personal trackers and only allows anonymous cookieless pings to pass through.



Keeping the cookie banner and the server perfectly synchronised ensures that no personal data is accidentally leaked, keeping the business completely compliant with laws like the GDPR and protecting user trust.

Chapter 5

Vendor consent solutions: Google & Microsoft

Vendor consent solutions: Google & Microsoft

Filling the gaps with cookieless pings



What happens to website analytics when a user is redirected to the advertisers' landing page and clicks "Reject all" on the cookie banner?

Instead of losing all data, modern systems use something called "cookieless pings". When a user rejects tracking, the system respects their choice and does not store any cookies or personal IDs.

Instead, it sends a basic, anonymous signal (a "ping") to the server that simply says an action happened, like a page being viewed or a button being clicked.

Because these pings do not contain any personal data, they allow businesses to estimate overall website traffic and understand basic trends without invading anyone's privacy.

Some companies have already developed these kinds of consent solutions. On the next pages we show some of the most known: Google Consent Mode and Microsoft Consent Mode.

Google | Google Consent Mode

Fundamentals of Google Consent Mode

Consent Mode lets advertisers indicate consent status of a user, enabling Google to model for gaps in conversions.
Two different implementations:

Basic Consent Mode

Prevents the collection of any user data, including consent status itself. Tags are inactive and will only load if the user grants consent.

Advanced Consent Mode

Activates Google tags before the user interacts with the consent banner. Respecting user privacy, Google collects anonymous data through cookieless pings, without using cookies or personal identifiers.

Basic CoMo

Google tags blocked until consent is granted.

- Behavior modelling in GA4
- Conversion modelling in GA4
- Conversion Modelling in Ads

Advanced Como

Google tags loaded before consent banner appears. Tags send cookieless pings when cookie consent is denied.

- Behavior modelling in GA4
- Conversion modelling in GA4
- Conversion Modelling in Ads

Required consent types parameters by Google

ad_storage

This indicates whether Google tags are permitted to use cookies on the user's device for advertising purposes.

- **GCS value: G110 | G111**

analytics_storage

This indicates whether Google tags are permitted to use cookies on the user's device for analytics purposes.

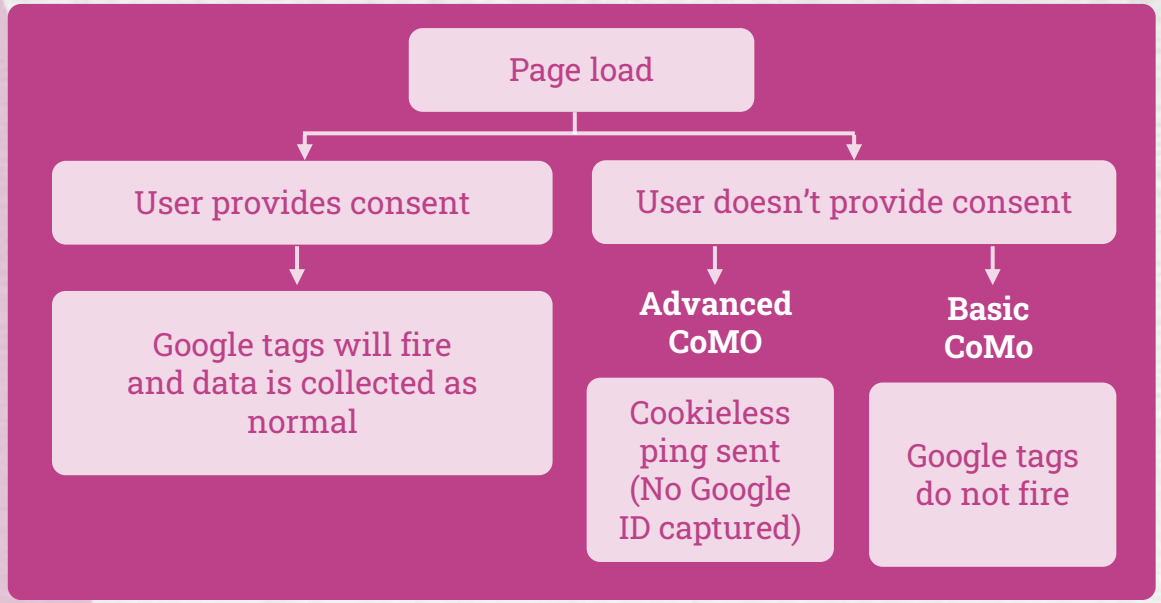
- **GCS value: G101 | G111**

ad_user_data (new in CoMo V2)

Sets consent for sending user data to google platforms for advertising purposes. If disabled - no user_id collection and Enhanced Conversions won't work.

ad_personalization (new in CoMo V2)

Sets consent for personalized advertising via google platforms. If disabled - remarketing for Google products is disabled.



How will you see data in GA4 depending on the Reporting Identity settings?

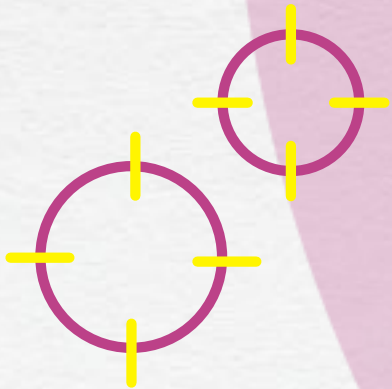
Observed & device based	Blended
No data modelling	Modelled data reported based on observed data + cookieless pings

Microsoft | Microsoft Consent Mode

Fundamentals of Microsoft Consent Mode

Microsoft requires all advertisers serving users in the European Economic Area (EEA), the UK, and Switzerland to provide valid user consent signals when using Universal Event Tracking (UET) tags. **If valid consent signals are missing, Microsoft will disable conversion tracking and remarketing features for those users.**

Consent Mode is set via a property in UET called "ad_storage". Microsoft Consent Mode offers two implementation paths:



Basic Consent Mode

The UET tag is entirely blocked from loading until the user explicitly grants consent. No data is sent prior to consent.

Advanced Consent Mode

The UET tag loads immediately upon page load, but the consent state is defaulted to "denied". If consent remains denied, first-party cookies are not read or written, and third-party cookies are read-only strictly for fraud and spam prevention, not for advertising. The tag only collects anonymized data, which Microsoft aggregates prior to precise modelling.

Chapter 6

From setup to strategy: Measuring without cookies

Technical configuration: Measuring the "Immediate post-click"

Server-side tracking (SST) and personally identifiable information (PII) redaction

Using server-side tagging is the most robust way to measure consentless traffic securely. The workflow operates as follows:

1. The user clicks an ad and lands on the website. The web container sends the raw HTTP request containing the UTMs to your first-party sGTM container (e.g., hosted on a custom subdomain like metrics.yourdomain.com or a folder within your domain like yourdomain.com/metrics).

2. The sGTM server reads the user's consent state transmitted from the consent management platform (CMP).

3. If consent is denied, sGTM intercepts the data stream. It strictly strips all personally identifiable information (PII) from the payload before it ever touches a third-party vendor

First-party data & "Zero-party" conversion strategies

When operating without cookies, the most effective way to transition a non-consented click into a measurable event is to motivate the user to identify themselves willingly. This is the foundation of "Zero-party data": information a user intentionally and proactively shares with a brand.

Instead of relying on invisible pixels, marketers can architect specific post-click experiences:

Immediate value exchanges

Offering a localized promo code specific to a regional broadcaster's audience directly on the landing page in exchange for an email address.

Interactive onboarding forms

Using quizzes or preference centers immediately post-click to gather data on what the consumer is looking for, seamlessly tying the initial contextual ad click to a declared first-party profile.

Generating additional strategies: The future of measurement

Edge computing analytics

Edge computing moves data processing away from centralized cloud servers and pushes it to the "edge" of the network, closer to the user (e.g., utilizing tools like Cloudflare Workers).

Because this logic executes at the CDN level during the initial HTTP request, it can instantly extract UTM parameters, route A/B testing variations, and send analytics pings in single-digit milliseconds.

This provides highly accurate, real-time marketing analytics that bypass traditional client-side JavaScript vulnerabilities entirely.

Advanced marketing mix modeling (MMM)

As mentioned earlier, MMM is increasingly important in environments where user-level attribution is incomplete. Because MMM relies on aggregate inputs such as media spend, sales, pricing, promotions and other business drivers rather than individual user paths, its operation is inherently independent of browser cookie availability.

This makes MMM resilient to cookie rejection and other gaps in user-level tracking. However, MMM is not immune to measurement error: its reliability still depends on data quality, model design, sufficient variation in marketing activity and appropriate validation.

Privacy-safe data clean rooms (DCRs)

While traditional cross-site tracking is dead, data clean rooms (DCRs) allow two parties (e.g., a publisher and an advertiser) to safely collaborate using the first-party and zero-party data they have legitimately collected. In a DCR, data is heavily encrypted. Algorithms overlap the datasets to provide aggregate insights, such as determining how many users who saw an ad on a premium publisher's site eventually purchased on the retailer's site, without either party ever exposing the raw, individual identities to one another.

This guarantees measurement accuracy while ensuring mathematical compliance with global privacy laws.

Top 3 actions to preserve campaign tracking when users reject cookies

1 Implement accurate consent status setup & consent modeling

Instead of completely blocking your tracking tags when a user rejects cookies, configure your consent management platform (CMP) and analytics tracking setup to send anonymous, cookieless signals.

Ensure that the consent choices are accurately updated right after the user makes a consent decision.

How it works

Platforms like Google (via advanced Consent Mode) or other analytics providers receive "pings" without personal identifiers.

The payoff

You still capture basic event counts, and the platform's machine-learning models use this raw data to estimate and restore lost campaign conversion metrics

Preserve campaign context with UTMs and server-side controls

2

Campaign information does not inherently require a cookie. UTM parameters and other campaign identifiers can be included directly in the landing-page URL, allowing the initial visit to retain information about the campaign that generated the click.

A server-side architecture can then provide greater control over how these signals are processed, filtered and shared with analytics or advertising platforms.

If consent is denied, the system should apply the appropriate privacy rules before forwarding data to third parties and should remove unnecessary personal information from the payload.

How it works

The user clicks an ad containing campaign parameters → the landing page receives those parameters → the measurement architecture captures the permitted campaign context → server-side processing filters or transforms the data before it is shared.

The payoff

Campaign context can be preserved even when browser-based identifiers are unavailable. This does not mean that the user can be followed or deterministically attributed across their entire journey; it means that the campaign information associated with the landing-page interaction can remain available for permitted measurement.

Move beyond deterministic attribution with aggregate and experimental measurement

3

When user-level signals are unavailable, campaign performance should not be evaluated solely through last-click or deterministic attribution. Instead, complement the remaining digital signals with methods that do not depend on identifying individual users.

Two particularly useful approaches are incrementality testing and marketing mix modeling (MMM).

How it works

Incrementality testing compares outcomes between exposed and control groups to estimate whether advertising generated additional conversions and MMM uses aggregated data to estimate the contribution of different marketing channels.

The payoff

You can evaluate the business impact of campaigns without needing to reconstruct an individual user's journey. This shifts the measurement question from "Which user converted after seeing this ad?" toward the more robust question: "Did this campaign generate incremental business value

Chapter 7

Market use case & final thoughts

Market use case & final thoughts

Market validation: Measuring unconsented traffic for an energy provider

When a user clicks an advertisement and arrives at a landing page, the immediate challenge is measuring that session if the user declines cookies (or makes no choice) on the consent banner.

A prominent energy provider in the Netherlands recently demonstrated how to solve this exact challenge at scale by combining the Opt Out Ad Server with a custom, privacy-first measurement stack.

To run programmatic campaigns targeting the privacy-conscious users, the energy provider utilized the Opt Out Ad Server.

The technical integration happens post-click. The brand uses Relay42 as its tag management system (TMS) alongside Piano Analytics as their analytics tool. When the unconsented user lands on the website, Relay42 utilizes an API integration with Piano Analytics to provide consent management platform (CMP) enrichment the exact moment the URL is loaded.

However, instead of relying on standard UTMs or fragile third-party identifiers that get blocked by browsers, the brand utilizes a custom URL tagging framework.

They build their URLs using internal identifiers (for example, appending “?cmp=XXX-123-4567” to the end of the destination URL). This custom code acts as the ultimate stateless identifier, mapping cleanly back to the specific campaign, source, and medium in their own databases.

Because Piano Analytics features strict, GDPR-compliant anonymous tracking modes (such as "exemption" or "extended opt-out" modes), it can legally record basic, non-identifiable session events.

Even when the user's cookie consent status explicitly registers as "no choice" or "rejected", the analytics platform successfully tracks the page views and sessions, attributing them directly to the custom XXX campaign code.

For the advertiser, this represents a massive victory. By integrating the privacy-by-design delivery of the Opt Out Ad Server with a sophisticated, custom-coded tag management and analytics architecture, the brand gains crystal-clear visibility into the performance of their campaigns.

The report in Piano Analytics would look similar to this table

The majority of users decided to deny cookies after landing in the advertiser’s landing page. Consent opt-out rates are consistently increasing because users are more conscious about their privacy while navigating on the internet. Opt Out Advertising tool unlocks an easier approach to target these privacy-first users.

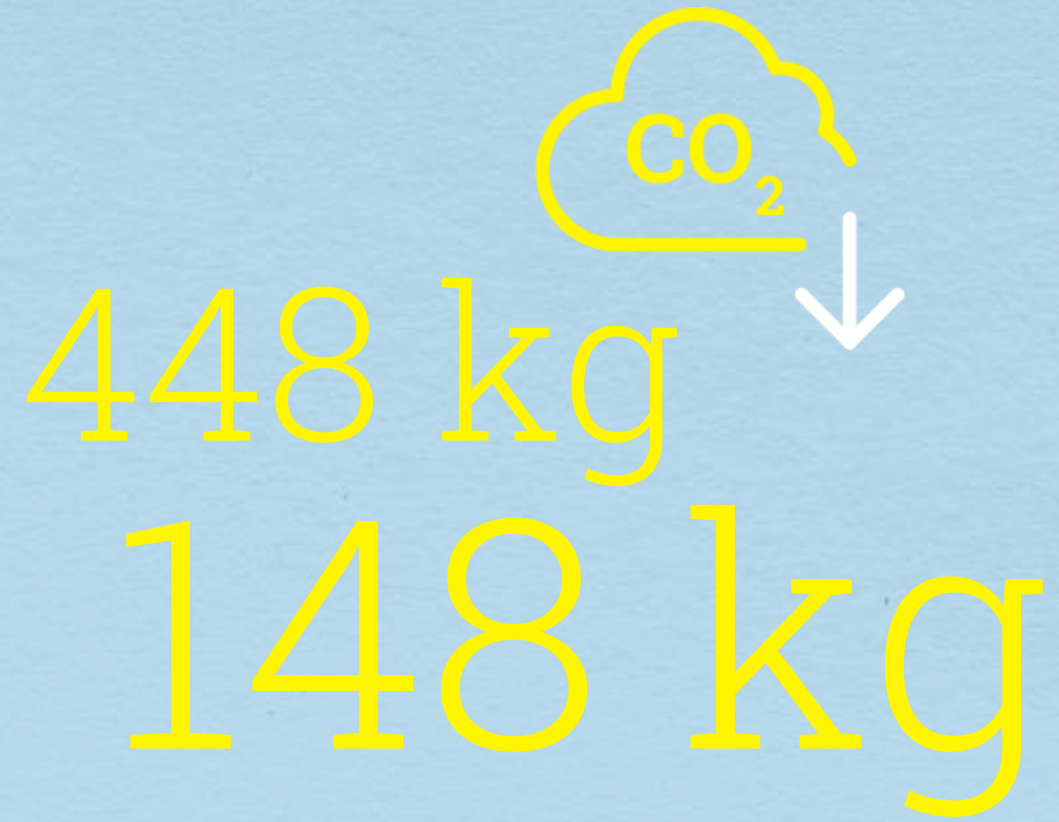
Campaign source	Campaign name	Cookie consent	Session amount
Opt Out	XXX-789-1234	No choice	5.788
Opt Out	XXX-789-1234	Accepted: Necessary only	774
Opt Out	XXX-789-1234	Accepted: All	255
Meta	YYY-123-4567	No choice	XXX
dv360	ZZZ-456-1234	Accepted: All	XXX

The environmental bonus: Slashing the carbon footprint

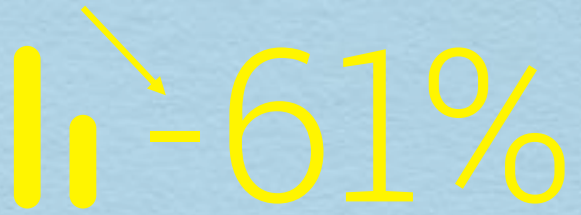
Beyond protecting user privacy, abandoning traditional tracking creates a massive environmental benefit.

The legacy programmatic advertising system is incredibly energy-intensive. Across just five major global economies, programmatic advertising generates over 215,000 metric tons of carbon emissions every single month, an energy expenditure equivalent to burning more than24 million gallons of gasoline.

The average programmatic ad generates roughly 514.8 grams of CO2 per thousand impressions (gCO2PM).



Same advertising goal 61% less carbon



This massive carbon footprint is caused by the thousands of servers constantly communicating to sync user IDs and hold multi-layered auctions every time a webpage loads. By switching to a privacy-by-design ad server, you bypass this heavy tracking infrastructure entirely. Removing complex behavioral supply paths slashes the volume of bid requests by nearly 45%, resulting in a corresponding 45% drop in carbon emissions during the ad selection process.

Recent joint research conducted by Omnicom Media and Opt Out Advertising provides concrete evidence of this sustainability advantage. In a 50/50 split test comparing standard open-market programmatic delivery (measured via Scope3) against consentless inventory, the structural differences became clear. A traditional consented page view triggers multiple server requests, pinging ad servers, analytics platforms, third-party verification services, and various supply-side platforms (SSPs). In contrast, a consentless page view operates with just one direct ad call and a single server request. This architectural efficiency translates directly into massive carbon reductions.

The study revealed that running campaigns on consentless inventory reduced total CO2 emissions by 62 - 67% (dropping from 448 KG on the open market to just 148 KG).

When looking at the average grams of CO2 per thousand impressions (gCO2PM), consentless delivery averaged just 108g compared to the open market's 281g, a 61% reduction.

Specific display formats, such as the standard 300x250 and 300x600 banners, saw the largest savings, with open market ads generating 46% more CO2 than their consentless counterparts.

Ultimately, by selecting domains with lower baseline emissions and utilizing a privacy-by-design ad server that eradicates third-party ad calls, advertisers can strip away bloated tracking scripts, make webpages load significantly faster, and easily hit their corporate social responsibility (CSR) goals.

Conclusion | The future-proof marketer

The decline of deterministic user-level tracking and the rise of stricter privacy requirements are not temporary hurdles to be solved with clever workarounds.

They represent a permanent architectural shift in how digital advertising and measurement operate.



The future-proof marketer

The future is therefore not simply “cookieless.” It is a move towards measurement architectures that can operate across a spectrum of signal availability: from consented first-party identifiers to privacy-preserving aggregate signals and experimental measurement.

Appendix

Technical appendix: Debugging & PII redaction

Technical appendix: Debugging & PII redaction

Troubleshooting advanced & basic **Google Consent Mode**

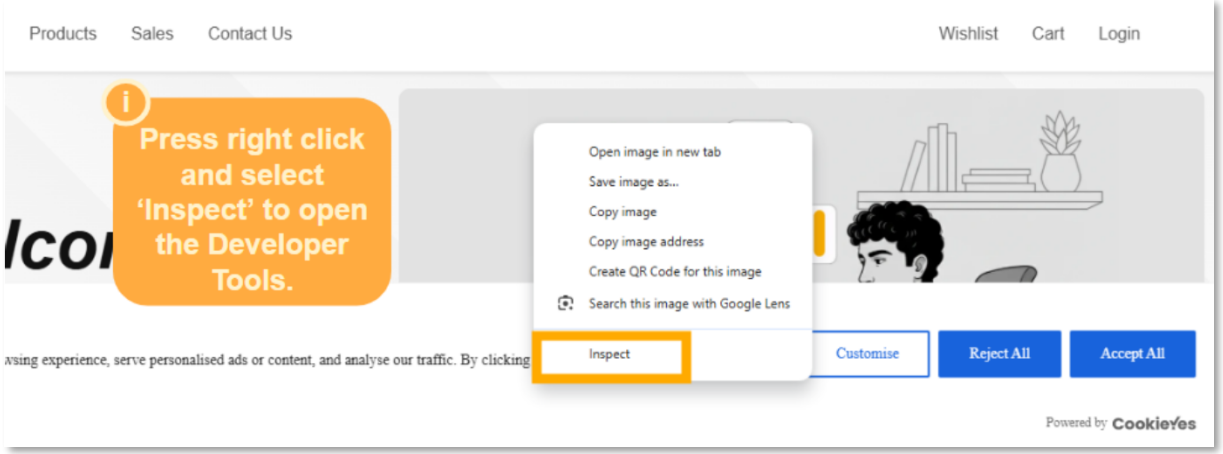


Before you start

All the following checks are done in the client's landing page, where the users are redirected after clicking an ad in the publisher website, where the ads are hosted.

1

In the website, press right click and select **“Inspect”** to open the **developer tools**

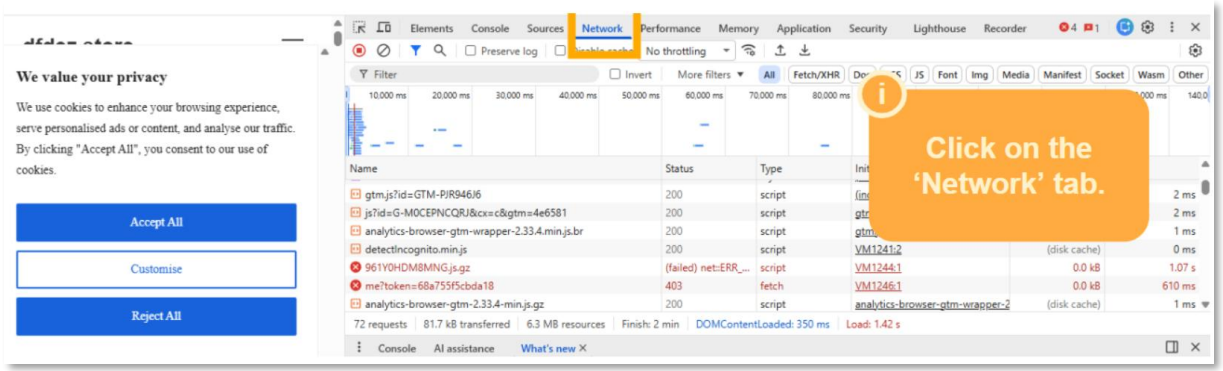


Check the “gcs” parameter in the GA4 requests.

Follow these steps

2

Once open, click on the **“Network”** tab

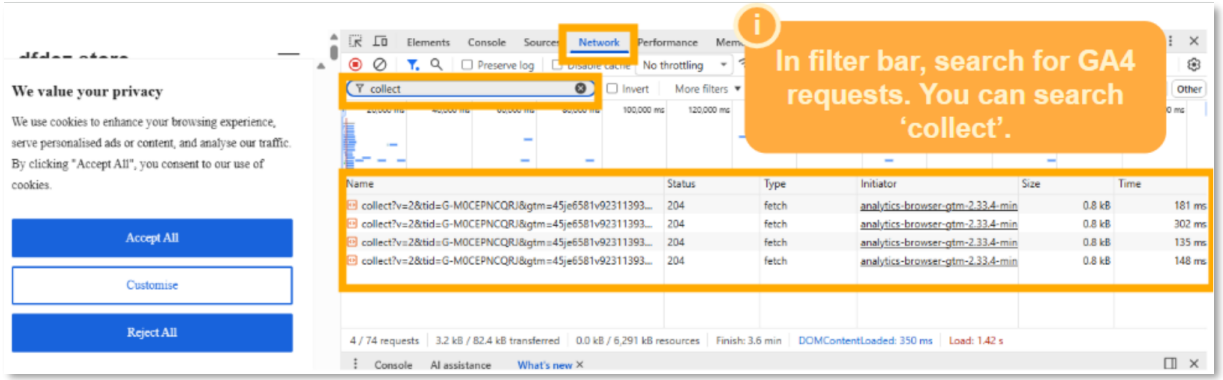


Advanced Google Consent Mode

3

Search for GA4 requests in the search bar.

You can search for **“collect”, “google analytics” or the GA4 measurement ID you’re testing**



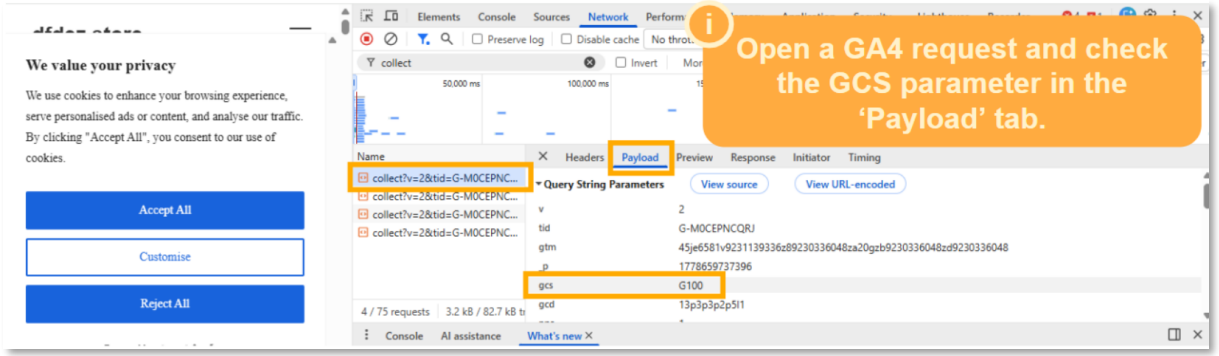
This website is using advanced Consent Mode, meaning that Google Analytics requests are sent even when users have not interacted with the cookie banner yet or they reject cookies.

In the case of a basic Consent Mode setup, no GA4 requests (collect?) will be shown in the Network tab until the user accepts cookies.

Advanced Google Consent Mode

4

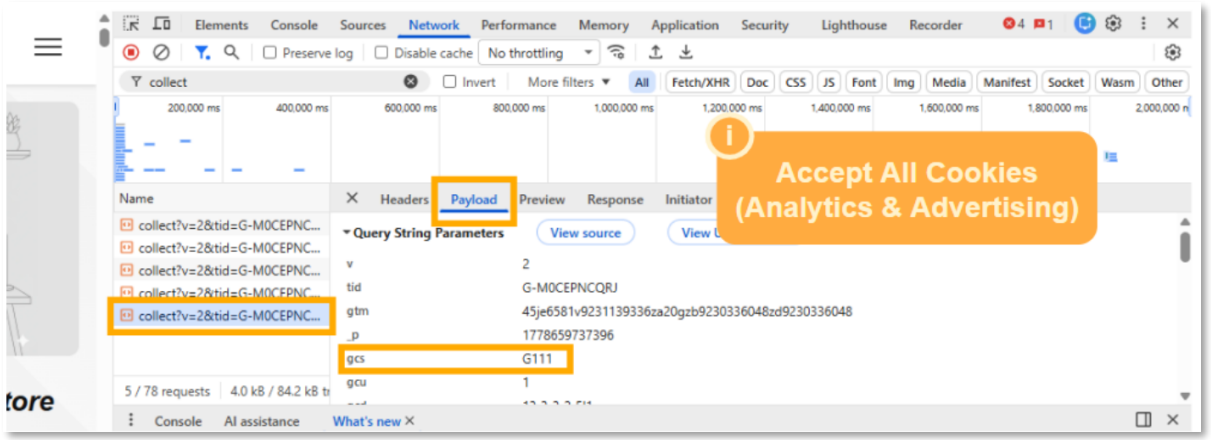
Open one of the GA4 requests and check the “Payload” tab. Then look for the **GCS (Google consent status) parameter value**



In this case, the GCS value is G100 because the user has not accepted any consent yet.

5

Accept all cookies (Analytics & advertising cookies)

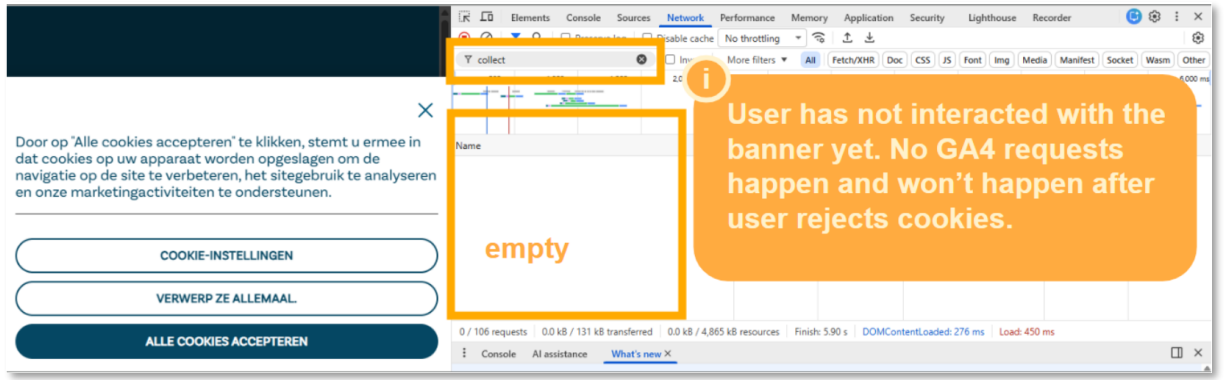


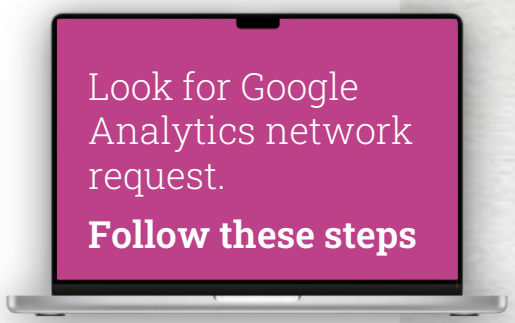
At this stage, the user has accepted all cookies and the GCS value for the next GA4 Network request is G111, meaning that analytics and advertising consent have been granted.

Advanced Google Consent Mode

1

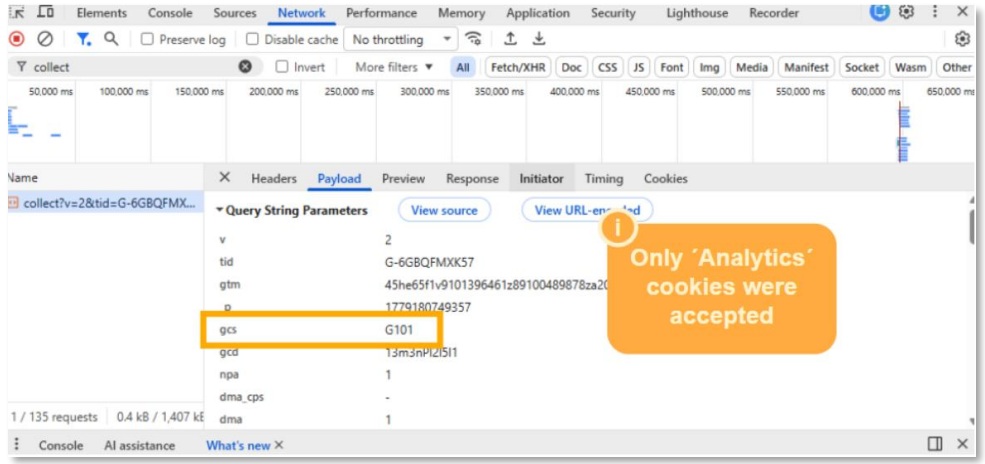
Follow the same steps as you followed to check “Advanced” Google Consent Mode: **Open the developer tools and filter by ‘collect’ in the Network tab.**





2

Once cookies are accepted, then you will be able to see GA4 requests. **Depending on your cookie choice, the GCS parameter will differ.** For this example, only analytics cookies were accepted:



Possible GCS values

- **G100** No consent was accepted
- **G101** Only analytics cookies
- **G110** Only advertising cookies
- **G111** Analytics + advertisingcookies

Basic Google Consent Mode

Technical appendix: Debugging & PII redaction

Troubleshooting advanced & basic **Microsoft Consent Mode**

In order to enable Microsoft basic or advanced Consent Mode, advertisers must implement 2 custom events: **'Consent Default' & 'Consent Update' in order to let Microsoft know the user consent choice.**

Within any Bing event network request (Consent Default, Consent Update, PageView...) there will always be a 'ASC' parameter which stands for 'Ads consent'.

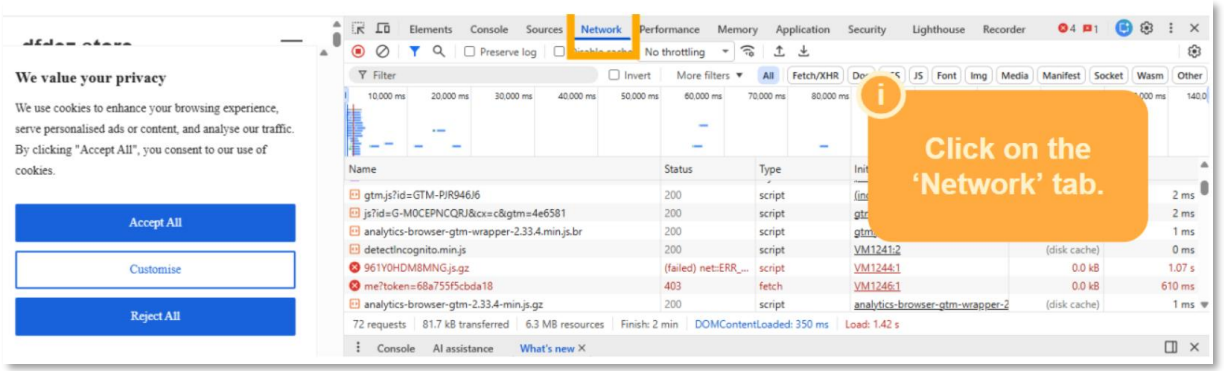
Possible 2 values for this parameter:

D **Denied**

G **Granted**

1

When located in the website, press right click and select “inspect” to open the developer tools.
Then select the "Network" tab



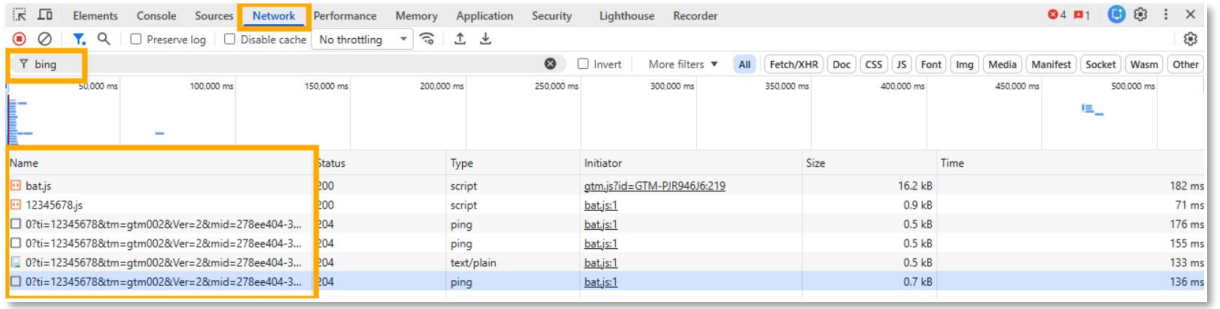
Check the “ASC” parameters in the Bing requests.

Follow these steps

2

In the search bar, filter by the Bing requests.

You can search for “bing”:

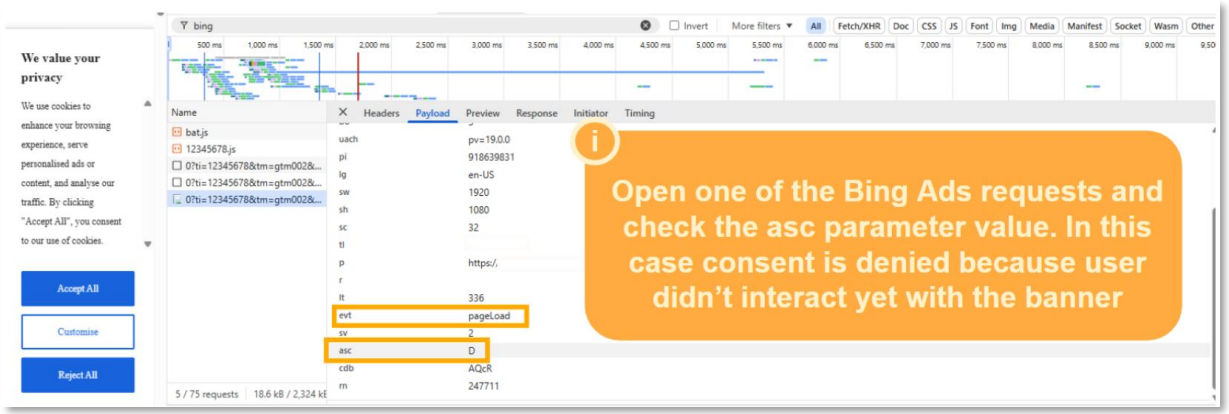


This website is using advanced Microsoft Consent Mode, meaning that Bing requests are sent even when users have not interacted with the cookie banner yet or they reject cookies. In the case of a basic Microsoft Consent Mode setup, no Bing requests will be shown in the Network tab until the user accepts cookies.

Advanced Microsoft Consent Mode

3

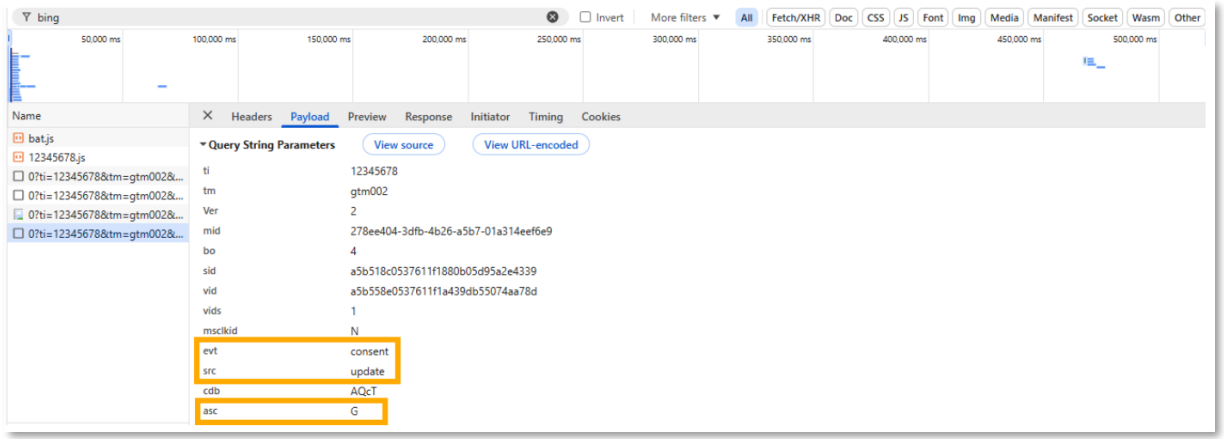
Open one of the Bing requests and check the **“Payload”** tab. Then look for the event name parameter (evt) just to see which event you are looking at. **Then, check the value of the “asc” parameter:**



4

Consent is denied because the user has
not interacted with the cookie banner yet.

As soon as the user accepts advertising cookies, there will be a new Bing Ads network request that will send a ‘Consent Update’ event with the asc parameter value set as **‘G’.** Check it here:

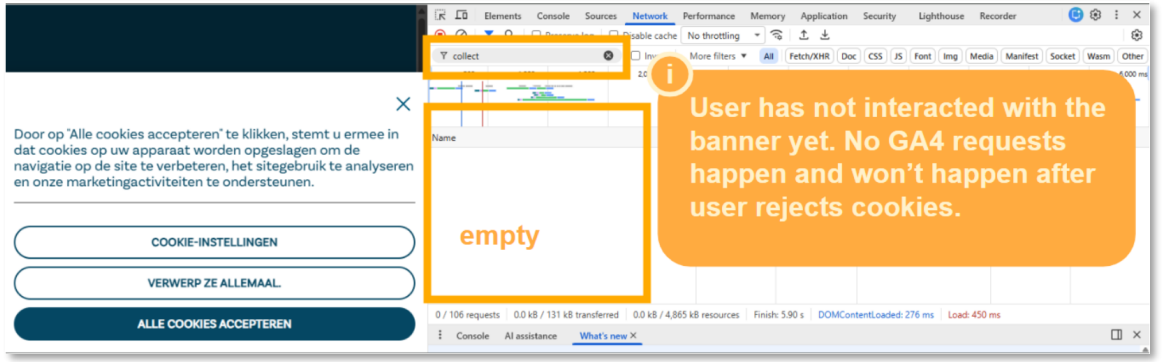


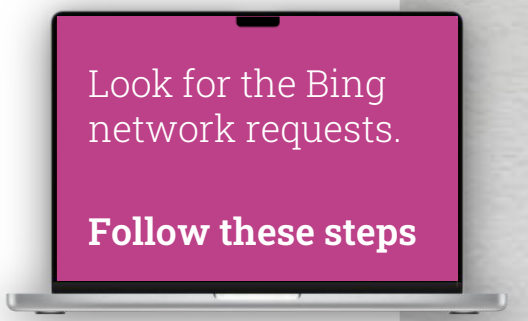
All the following events will include the consent parameter ‘asc’ with the value of granted.

Advanced Microsoft Consent Mode

1

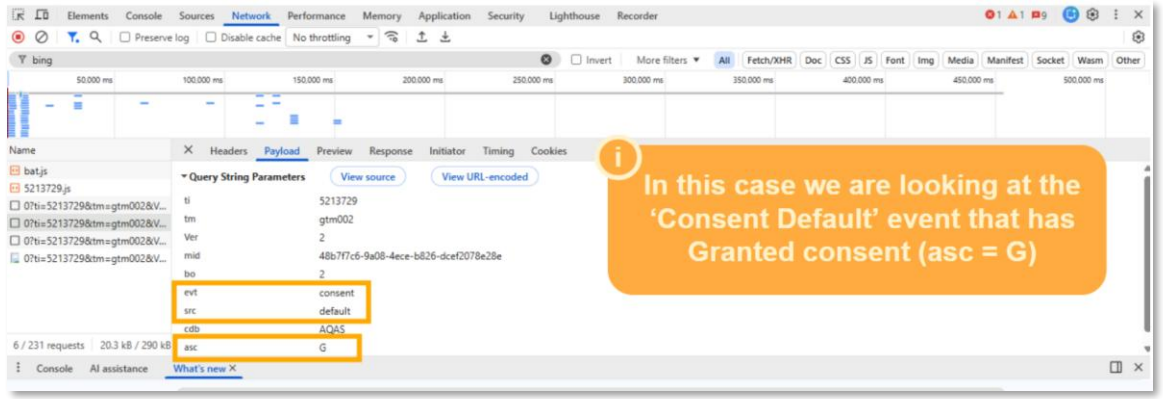
Follow the same steps as you followed to check the **"Advanced"** Microsoft Consent Mode: **Open developer tools and filter by 'collect' in the Network tab.**





2

Once cookies are accepted, then you will be able to see Bing Ads requests. Bing doesn't take into account analytics cookies, the only relevant cookies are the advertising ones. **This means that the asc parameter will only return 'G' if the user accepts advertising cookies, not if they accept only analytics cookies.**

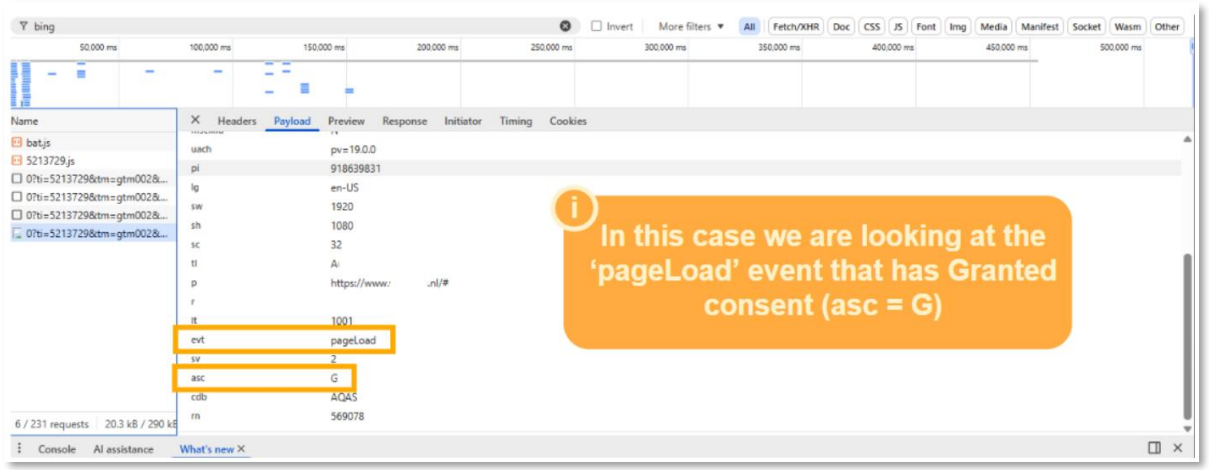


The Consent Default parameter has a granted consent value because the event is processed after the user has accepted cookies.

Basic Microsoft Consent Mode

3

To check the consent status for every other standard Bing event, like the PageLoad event, you can simply open the rest of requests and **look for the 'evt' (event name) and check the "asc" parameter value.**



In this example the event triggered was a PageLoad with the granted consent status

Basic Microsoft Consent Mode

Technical Configuration: Measuring the "Immediate Post-Click"

Server-Side Tracking (SST) and Personally Identifiable Information (PII) Redaction

Using Server-Side Tagging is the most robust way to measure consentless traffic securely. The workflow operates as follows:

1. The user clicks an ad and lands on the website. The web container sends the raw HTTP request containing the UTMs to your first-party sGTM container (e.g., hosted on a custom subdomain like metrics.yourdomain.com or a folder within your domain like yourdomain.com/metrics).

2. The sGTM server reads the user's consent state transmitted from the Consent Management Platform (CMP).

3. If consent is denied, sGTM intercepts the data stream. It strictly strips all Personally Identifiable Information (PII) from the payload before it ever touches a third-party vendor

1 Use this piece of sandboxed JavaScript to create the template:

```javascript
const createRegex = require('createRegex');

// Get the URL passed into the variable
const urlPayload = data.inputURL;

if (!urlPayload || typeof urlPayload !== 'string') {
  return urlPayload;
}
// Pass the regex as a string. Notice the \\. to properly escape
the dot
const emailRegex = createRegex('[^@&=]+@[^@&=]+\\.[^@&=]+', 'ig');

if (emailRegex) {
// Replace with a placeholder instead of '' so you don't leave "="
signs
  return urlPayload.replace(emailRegex, 'redacted');
}
return urlPayload;
```

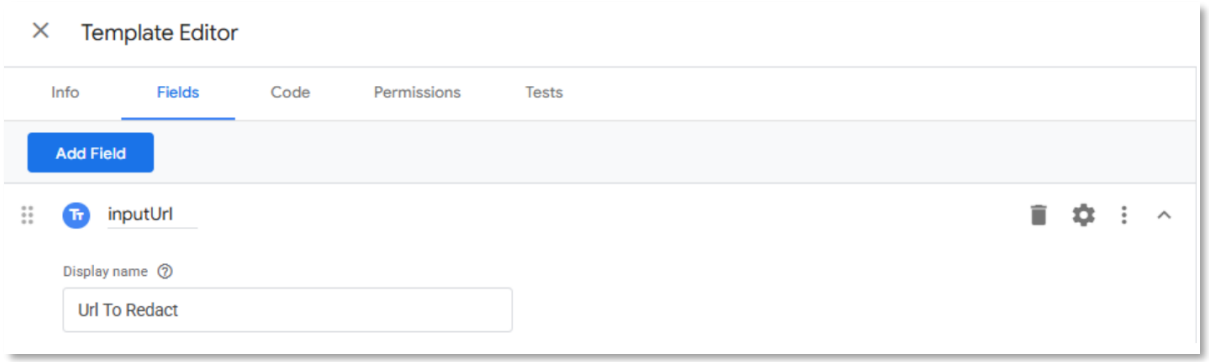
Custom RegEx template variable in server-side Google Tag Manager

To ensure compliance, you can configure a custom variable template in server-side GTM that uses regex to automatically detect and overwrite PII (like accidentally appended email addresses) within the URL string before it is sent to analytics or advertisement platforms.

Logical rule configuration example:

2

Create a text input field labeled as **'inputURL'** and **SAVE.**

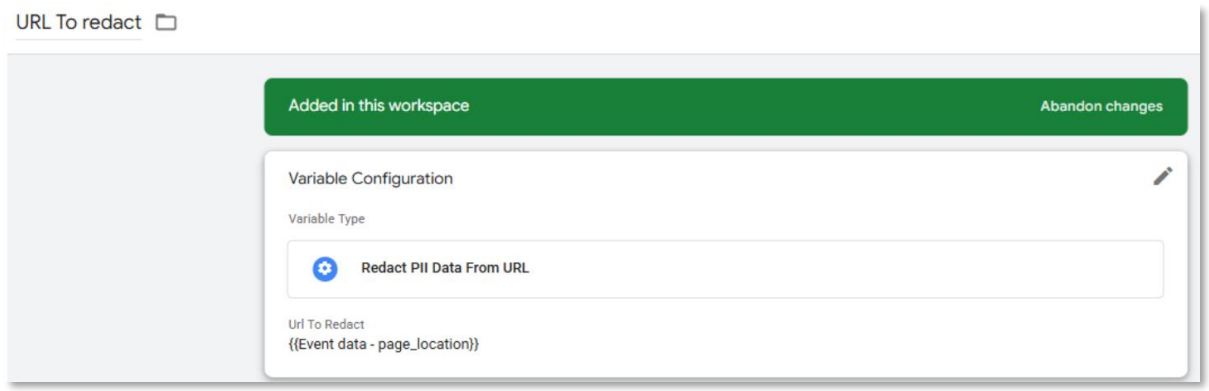


3

Create a variable using the new template you have just created: Make sure to add the variable you are using to collect the page URL in your sGTM container.

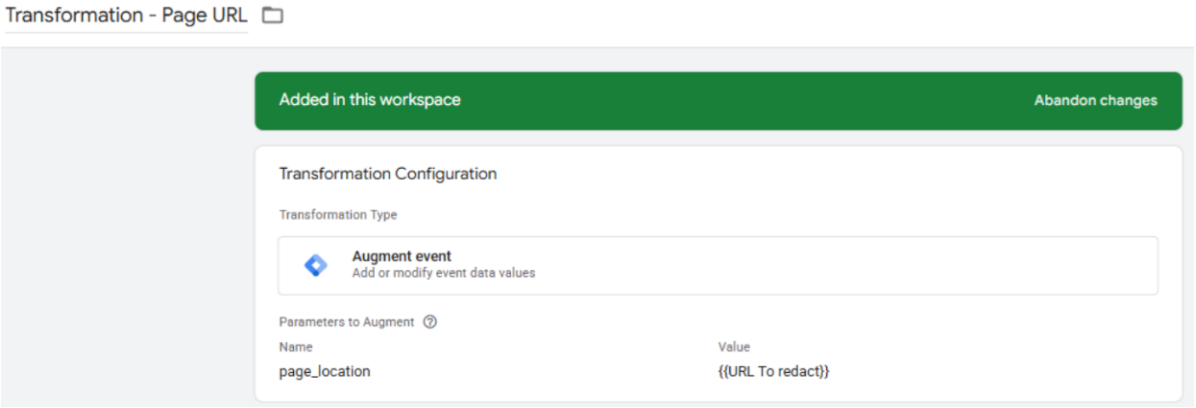
Example:

```
{{Event Data -
page_location}}
```



4

Create a transformation and use the Augment feature to override the **'page_location'** parameter with the output of your new variable:



5

When testing, the output should look like this.

You can see that the email from the original URL 'daniel@gmail.com' was redacted from the final output, which is the one sent to the analytics and advertisement platforms.



Interested to hear more about the options for your campaigns or platform?

Drop us a line at **info@optoutadvertising.com**
or call us at **+31(0)970 102 57050**

We're happy to tell you everything about unlocking consentless inventory.

opt out

