

BIG CHANGES TO GOOGLE ANALYTICS AND GOOGLE ADS COMING IN JUNE: IS YOUR BUSINESS PREPARED?

Insights
May 20, 2026

Big Changes to Google Analytics and Google Ads Coming in June: Is Your Business Prepared?

Are you ready for the significant changes to Google Analytics and Google Ads that are coming on June 15? Your business may need to take immediate action by updating your structural configurations in Google Analytics and Google Ads, as well as your privacy notice, and cookie management platform (CMP). Now is the time to ensure collaboration between your legal, marketing, and web development teams and to review compliance with state and international consumer privacy laws. Here's what you need to know about the changes and three steps your business should consider taking before the deadline.

What's Changing?

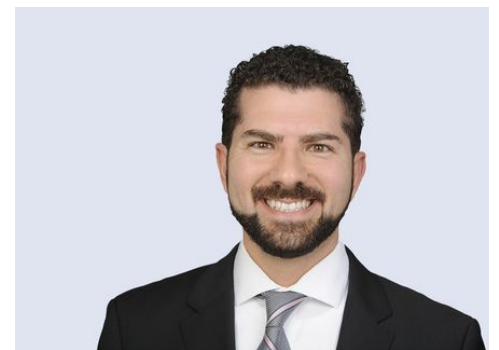
Google is consolidating controls based on where data is used and removing redundant settings between Google Analytics and Google Ads. Until June 15, when linking your Google Analytics to your Google Ads account, you enabled the flow of data from your property to Google Ads. That data was controlled by Google Ads and subject to its terms and conditions. Additionally, existing settings in Google Analytics via Google Signals also allowed you to control the collection of Google Ads cookies and IDs through your account in conjunction with Consent Mode in Google Ads.

Related People



Jasper L. Hall
Associate

415.490.9033



Usama Kahf, CIPP/US
Partner

949.798.2118

Now, Consent Mode will be the single control center for Google Ads data including data shared by Google Analytics – not Google Signals. Meanwhile, Google Analytics will exclusively control data used within Google Analytics for behavioral reporting.

According to Google, this simplifies controls and streamlines the consent process, so that user preferences are enforced consistently between Google Analytics and Google Ads. The company says this will also allow users' privacy selections, managed via Ads Consent Mode settings, to exclusively govern how data is collected and used.

What Does This Look Like in Practice?

Prior to the changes, data would flow in through two gates: through Google Analytics via Google Signals and through Google Ads by Consent Mode. Google Signals also functioned as a control over advertising data flows, so if a company wanted to prevent Google Ads from linking a website visitor to their personal Google account, you could turn Google Signals off in Google Analytics. Even if your business made a mistake in CMP and Consent Mode, Google Signals would block data flow.

Many privacy and legal teams used Google Signals to limit how Google Analytics data connects with Google Ads without modifying Consent Mode. This prevented visitor data from being tied to Google account identities. For years, privacy and legal teams have also developed compliance documentation, including privacy notices and CMPs with this backstop in mind.

Starting June 15, however, one of the gates that data flows through and an important backstop will be removed, specifically, the Google Analytics settings via Google Signals that override Google Ads behavior. Google Ads will stop considering Google Analytics' settings and rely exclusively on Consent Mode and the code contained on your company's website.

The changes will also present businesses with a choice of either:

1. granting consent to "ad storage," which could provide Google Ads full permission to use cookies, device IDs, and personal profile linking; or

Service Focus

Consumer Privacy Team

Privacy and Cyber

2. denying consent to “ad storage,” preventing Google Ads from accessing this information.

This will impact the compliance obligations for businesses that use Google Analytics and Google Ads, specifically as it relates to their privacy notices, consent banners, and CMPs.

Legal Risks to Manage

Businesses should act quickly to ensure compliance under international and state privacy laws before these changes take effect on June 15. Here are some of the potential legal risks:

European Union Law

Under the EU’s comprehensive data privacy and security law, the **General Data Protection Regulation (GDPR)**, a material change to a privacy policy occurs when a significant modification to how a company collects, uses, or stores personal data requiring proactive notification and sometimes, fresh consent from users.

Google’s changes to the Google Analytics and Google Ads platforms, and the transition to Consent Mode as the single control for collection of data, are likely material changes for third-party sharing purposes under the GDPR.

The downstream effects on businesses will also create compliance challenges for many companies, requiring many to update consent banners, privacy notices, and CMPs while balancing the effectiveness of advertising campaigns against the risks associated with legal compliance.

US State Laws

These changes can also impact notice requirements under many state laws. For example, under the **Colorado Privacy Act (CPA)**, a material change is a significant update to a business’s data processing practices that would require notifying consumers and potentially obtaining new consent.

The transition from having two security gates (Google Analytics via Google Signals and Google Ads via Consent Mode) - to one gate (Consent Mode) that relies solely on the user’s consent banner and CMP, will likely constitute a material change that would require a notice to consumers and potentially a new consent from those consumers.

Under other state laws, such as **California's CCPA**, Google Analytics is currently considered a service provider as an entity that receives consumers' personal information from a business and processes personal information on their behalf, pursuant to a written contract that restricts the service provider from selling or using the data for their own commercial purposes or outside the context of the services provided. This is largely due to a party's selection in the Google Analytics Platform, specifically, using Google Signals, and turning off advanced matching and data sharing across Google Platforms, as well as checking the box to opt-in Google's CCPA-compliant service provider terms and conditions.

However, based on the changes to Google Analytics and Google Ads, including their respective changes to terms and conditions, this may impact Google Analytics' ability to be deemed a service provider under CCPA. Instead, the law may categorize Google Analytics as a third party to which businesses are selling data unless the steps discussed below are taken. Concerningly for businesses in California, and in light of the surge of California Invasion of Privacy Act (CIPA) claims, companies could be subject to a deluge of claims if they do not promptly update their privacy policies and CMPs prior to June 15.

3 Steps to Consider Taking Now

1. Review and Update Your Privacy Policy and Cookie Notices

Determine whether the changes to Google Analytics and Google Ads alter how data is collected, when data is collected, and how consent can be interpreted and enforced. Another consideration is whether your company's privacy disclosures mention or assume that Google Signals functionality in the Google Analytics platform previously functioned as a backstop for data collection. If so, you should update your policies to accurately reflect changes in the relationship between Google Analytics and Google Ads, and that Google Ads' Consent Mode is now the single control for data collection.

Additionally, since the GDPR and some state laws have transparency obligations regarding privacy notices – including advance notice related to material changes in high enforcement jurisdictions – it's important to review your

privacy notice, and if necessary, update it before the June 15 deadline.

2. Make Sure Your Cookie Management Platform is Driving Outcomes

Analyze and review how your company's CMP interacts with Consent Mode and other Google platforms. As your CMP captures user choices, such as opt-in or opt-out, Google Consent Mode will convert those choices into signals. Google platforms must be customized to act on those signals.

Be sure to align your CMP, Consent Mode, and each Google Platform you are using. Any misalignment prior to June 15 may result in your company's CMP not properly blocking or categorizing non-essential cookies when enabled by the user, exposing your company to international and domestic litigation risks.

Additionally, now that your company's CMP is the driving factor, and without Google Signals to override errors, your CMP must send consent signals and update them regularly. After June 15, Consent Mode will only reflect your CMP and will not override it.

3. Reach Out to Legal Counsel

Consult with your FP attorney on whether updating your privacy notice in response to the Google Analytics and Google Ads changes constitutes a material change under the GDPR and applicable US state laws, as well as notice requirements. Your attorney can also assist in reviewing and auditing your business's consent banner before the deadline.

Conclusion

The deadline to review and update your privacy policy, notices, and CMP in response to the changes to Google Analytics and Google Ads is quickly approaching. If you have any questions or concerns, please reach out to the authors of this insight, your FP attorney or any attorney in our [Privacy and Cyber Practice Group](#) or on our [Consumer Privacy Team](#). We'll continue to track the latest developments, so make sure you are subscribed to [Fisher Phillips' Insight System](#) to get the most up-to-date information directly to your inbox.

