

**TO:** Chris Pedigo  
SVP, Government Affairs  
Digital Content Next

**FROM:** Tanya L. Forsheit

**DATE:** April 12, 2018

**SUBJECT:** Google's GDPR Position on Consent and Publishers

---

## **EXECUTIVE SUMMARY**

On March 22, 2018, Google officially announced its public position around changes to its advertising services policies to comply with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("GDPR"). In a short AdWords blog post entitled "Changes to our ad policies to comply with the GDPR," Google's president of partnerships for Europe, the Middle East and Africa stated that Google's "revised policy will require that publishers take [unspecified] *extra steps* in obtaining consent from their users" for the use of Google's advertising services.<sup>1</sup> The company also indicated that, before May, it will launch an unspecified "solution to support publishers that want to show non-personalized ads." The blog post included no specifications or details on the nature of these proposed solutions or what non-personalized might mean in a GDPR landscape where even IP addresses and device information are considered personal data.<sup>2</sup>

Google's vague pronouncement leaves publishers in the lurch and appears to be designed to distract EU regulators away from Google's own activities while inappropriately attempting to transfer the GDPR's heightened consent burdens to Google's publisher customers, even in

---

<sup>1</sup> <https://adwords.googleblog.com/2018/03/changes-to-our-ad-policies-to-comply-with-the-GDPR.html>.

<sup>2</sup> For an example of other potential difficulties associated with purportedly "non-personalized ads," see PageFair Blog, "Google adopts non-personal ad targeting for the GDPR," March 27, 2018, available at [https://pagefair.com/blog/2018/googles-nonpersonal-ads/#\\_ftnref4](https://pagefair.com/blog/2018/googles-nonpersonal-ads/#_ftnref4) ("Although Google's "non-personalized ads" may seem promising to advertisers and publishers who are concerned about GDPR liability, more work must be done before they can be considered safe. Unique tracking IDs are currently vital to Google's ability to perform frequency capping and bot detection. Meanwhile, data leakage is a problem caused by 3rd party ad creatives liberally loading numerous tracking pixels. Google has been silent on fixing these problems. Therefore, it may be that Google will merely target ads with non-personal data, but will continue to perform tracking as usual. Clarity on this point will be important for advertisers seeking safe inventory").

circumstances where Google affirmatively seeks to play a joint controller role with its customer. Such an approach is inconsistent with the letter and spirit of the GDPR's consent requirements, and untenable as a business matter for Google's publisher customers.

Google's position, explained in more detail below, is that Google (a) is a controller under the GDPR with respect to certain of the services it provides to publishers in the Ad Tech ecosystem; (b) therefore needs a lawful basis for processing personal data obtained through publisher customer properties; (c) has decided to use consent as that legal basis; and (d) seeks to off-load full responsibility for obtaining that consent on its customer publishers. This memorandum is designed to address and provide guidance on Google's position.

## **BACKGROUND**

Google monetizes its services through the placement of ads directly on its own online platforms as well as through technology embedded on third party publisher websites and apps. Google allows advertisers to place ads on its Google-owned services, including Google Search, Gmail, and YouTube, as well as on third party websites and apps that use Google's ad serving technology services, such as DoubleClick and AdSense.

The EU adopted the GDPR in 2016 and it will be enforced effective May 25, 2018; the law includes extraterritorial jurisdiction provisions designed to reach certain companies that are not based in the EU but that reach out to or monitor data subjects in the EU.<sup>3</sup> The GDPR allows regulators to seek penalties of up to four percent of total annual turnover of the preceding financial year for violations of the GDPR's basic principles for processing, including conditions for consent.<sup>4</sup>

A "controller" for purposes of the GDPR is the natural or legal person which, alone or jointly with others, "determines the purposes and means of the processing of personal data." GDPR Article 4(7). Google's announcement on March 22 stakes out the position that, at least with

---

<sup>3</sup> Article 3 of the GDPR sets forth the territorial scope of the GDPR as follows (in relevant part):

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

<sup>4</sup> While this memorandum is focused on the flaws in Google's proposed approach to consent-based processing where Google claims to be a data controller, some types of digital marketing may be covered by the legitimate interest basis for processing, as explicitly recognized in the text of the Recital 47 of the GDPR. Legitimate interest processing is not addressed herein, and this memorandum is not intended to address any legal basis available to publishers as controllers in online behavioral advertising context.

respect to certain services, Google is a joint controller with the customer, and will unilaterally make decisions regarding how the personal data collected by its customers is used in providing advertising services, but nonetheless expects its publisher customers to obtain legally valid consent on behalf of the publisher itself and Google. Google's updated EU User Consent Policy, effective May 25, 2018, available at <https://www.google.com/about/company/consentstaging.html>, states as follows:

If your agreement with Google incorporates this policy, or you otherwise use a Google product that incorporates this policy, you must ensure that certain disclosures are given to, and consents obtained from, end users in the European Economic Area. If you fail to comply with this policy, we may limit or suspend your use of the Google product and/or terminate your agreement.

#### Properties under your control

For Google products used on any site, app or other property that is under your control, or that of your affiliate or your client, the following duties apply for end users in the European Economic Area.

You must obtain end users' legally valid consent to:

the use of cookies or other local storage where legally required; and  
the collection, sharing, and use of personal data for personalization of ads or other services.

When seeking consent, you must:

retain records of consent given by end users; and  
provide end users with clear instructions for revocation of consent.

You must clearly identify each party that may collect, receive, or use end users' personal data as a consequence of your use of a Google product. You must also provide end users with prominent and easily accessible information about that party's use of end users' personal data.

#### Properties under a third party's control

If personal data of end users of a third-party property is shared with Google due to your use of, or integration with, a Google product, then you must use commercially reasonable efforts to ensure the operator of the third-party property complies with the above duties. A third-party property is a site, app or other property that is not under your, your affiliate's, or your client's control and whose operator is not already using a Google product that incorporates this policy.

Google also published on its website "Google Ads Controller-Controller Data Protection Terms", available at <https://privacy.google.com/businesses/controllerterms/> (the "Google Controller

Terms”), which cover, *inter alia*, AdWords programs and services accessible to customer through their AdWords account, DoubleClick Ad Exchange, and DoubleClick for Publishers (the “Controller Services”).<sup>5</sup> The Google Controller Terms spell out that Google will be an *independent* controller with respect to *any* personal data that is processed by *either party* under the Google Controller Terms in connection with its provision or use (as applicable) of the Controller Services (“Controller Personal Data”). Google Controller Terms § 4.1(a). They further specify that that Google will *individually determine* the purposes and means of its processing of Controller Personal Data. *Id.* § 4.1(b).

## **ANALYSIS**

- **The consent structure proposed by Google fails to meet the transparency, specificity, and granularity standards required by the GDPR for purposes of obtaining legally valid end user consent.**

To rely on consent as a lawful basis for processing personal data under the GDPR, a company must be able to demonstrate that, prior to processing the personal data, the company provided the individual with clear notice of how it will process his or her personal data, and the individual *unambiguously* and *freely* agreed to such processing. See GDPR, Articles 4 and 7. Article 5(1)(a), which requires that personal data be processed in a transparent manner, and Article 5(1)(b), which requires that it be “collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.”

The element of “specific” requires that the controller apply “(i) [p]urpose specification as a safeguard against function creep, (ii) [g]ranularity in consent requests, and (iii) [c]lear separation of information related to obtaining consent for data processing activities from information about other matters.” Article 29 Working Party in its Guidelines on Consent Adopted on 28 November 2017 (WP29 Guidelines on Consent) at 12.

Moreover, a request for consent must be presented “in a manner which is clearly distinguishable from the other matters.” GDPR, Article 7. As noted in Recital 43 and highlighted by the Article 29 Working Party in its WP29 Guidelines on Consent:

consent is presumed not to be freely given if the process/procedure for obtaining consent does not allow data subjects to give *separate* consent for personal data processing operations respectively (e.g. only for some processing operations and not for others) despite it being appropriate in the individual case.

... If the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom. This granularity is closely related to the need of consent to be specific, . . . When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose.

---

<sup>5</sup> <https://privacy.google.com/businesses/adsservices/>.

WP29 Guidelines on Consent at 11.

The consent currently proposed by Google – i.e., that publishers obtain on Google’s behalf broad and blanket consent for all “collection, sharing, and use of personal data for personalization of ads *or other services* from its users” – does not and cannot meet the GDPR standards for consent: specificity, granularity, or transparency.

Google knows that it cannot rely on any prior or prospective consent bundled with the use of its services. Rather, Google seeks to place the full burden of obtaining new consent on the publisher without providing the publisher with the specific information needed to provide sufficient transparency or to obtain the requisite specific, granular, and informed consent under the GDPR.

Also of note in Google’s attempt to transfer liability for consent to the publisher (if not surprising) is Google’s standard technique of limiting liability. In this case to the exclusions and limits of liability under its primary agreement with the publisher or, to the extent US law is found to apply, to the “maximum monetary or payment-based amount at which that party’s liability is capped under the Agreement.” Google Controller Terms § 7.

- **Google’s Controller Ad Services may constitute automated decision-making, in which case they require an even higher threshold of explicit consent not anticipated in Google’s proposed consent model.**

Many of Google’s Ad Services are designed to be automated. Indeed, DoubleClick’s Support pages themselves describe and tout the use of automation in the service:

DoubleClick Search (DS) bid strategies optimize your advertising spend across the engine accounts within an advertiser. They monitor the performance of keywords and product groups, and adjust bids to achieve the highest number of conversions, the greatest amount of revenue, the best position, or highest number of clicks your campaign budgets allow. Depending on the engine, bid strategies also set or recommend bid adjustments for your location targets, mobile devices, and remarketing targets. Instead of manually setting bids and bid adjustments in response to changes in your advertising goals or in the overall advertising landscape, *use a DS bid strategy to automate the process.*

A DS bid strategy can also *automate the processes of creating and managing location targets and product groups.*

“Introduction to DoubleClick Search bid strategies,” available at <https://support.google.com/ds/answer/6231813?hl=en> (last visited April 3, 2018) (emphasis added).

Digital advertising is not by definition automated decision-making under the GDPR. And the provision of automated decision-making services does not by itself make the organization doing the automated decision-making a controller. However, in this unique situation, Google has affirmatively taken the position that it is acting as a controller, and some of its Controller

Services appear to involve automated decision-making. Nonetheless, Google seems to ignore all of the significant hurdles required of a controller like Google when it makes the decision to engage in automated decision-making. Publishers should be given the choice (1) whether to engage in automated decision-making in the first instance; and (2) whether Google should have the right to act as a controller at all in this regard.

Data subjects have a number of rights under the GDPR with respect to automated decision-making and profiling. See GDPR, Article 21-22. Article 4 defines profiling as “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.” Thus, profiling may include fairly common and widespread forms of online behavioral advertising or targeted advertising, including the Google Controller Services like DoubleClick.

However, “automated decision-making” is not exactly the same as profiling. As noted by the Article 29 Working Party in its Revised “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018” (WP29 Guidelines on Profiling): “Solely automated decision-making is the ability to make decisions by technological means without human involvement. . . . Automated decisions can be made with or without profiling; profiling can take place without making automated decisions. However, profiling and automated decision-making are not necessarily separate activities. Something that starts off as a simple automated decision-making process could become one based on profiling, depending upon how the data is used.” WP29 Guidelines on Profiling at 8.

Article 21 provides a data subject with the right to object to automated decision-making, including profiling. Article 22(1) goes beyond Article 21, *prohibiting* certain kinds of automated processing activity in the absence of certain exceptions: “The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.” This broad prohibition does “not apply if the decision is based on, *inter alia*, the data subject’s *explicit consent*.” Article 22(2) (emphasis added). Where explicit consent is invoked to facilitate such automated decision-making, the data controller must “implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.”<sup>6</sup>

---

<sup>6</sup>Further, automated decision-making may not be based on the special categories of data as set forth in Article 9(1), *i.e.*, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation, in the absence of additional protections. In such cases, there must be suitable measures to safeguard the data subject’s rights and freedoms, legitimate interests must be in place, and either (a) the data subject must have given explicit consent to the processing of those personal data for one or more specified purposes or (b) the processing must be necessary for reasons of substantial public interest, on the basis of union or member state law which must be proportionate to the aim pursued and respect the essence of the right to data protection.

The concern underlying these rights, as the Article 29 Working Party notes, is that automated decision-making processes “can be opaque. Individuals might not know that they are being profiled or understand what is involved. Profiling can perpetuate existing stereotypes and social segregation. It can also lock a person into a specific category and restrict them to their suggested preferences. This can undermine their freedom to choose, for example, certain products or services such as books, music or newsfeeds. In some cases, profiling can lead to inaccurate predictions. In other cases it can lead to denial of services and goods and unjustified discrimination.” WP Guidelines on Profiling at 5-6.

To the extent Google’s Ad Services constitute automated decision-making, and since Google has claimed a right to be a controller, these services would require an even higher standard for explicit consent for Google to use the data as it proposes, one that Google’s broad-brush EU User Consent Policy cannot even come close to attaining. Moreover, Google has not suggested any process by which it will implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, including but not limited to facilitating the data subject’s right to obtain human intervention from Google, to express his or her point of view, and to contest the automated decision. Publishers have no visibility into or control over the mechanisms available at Google to facilitate such measures. And Google has not offered publishers any choice as to whether it will engage in such activities in the first place.

- **Google wants all the benefits of being a controller, and none of the liability.**

Google wants to be an “independent controller,” making its own unilateral and often automated decisions regarding personal data collected on publisher properties, without providing any transparency to publishers. Google nonetheless proposes a contractual structure that improperly reallocates responsibility and liability to require the publishers to take the full brunt of a regulatory or private action hit. This hit could implicate four percent of global turnover for the prior financial year should the publishers fail to obtain consent on Google’s behalf, despite the fact that the publishers must obtain such consent in the absence of sufficient information regarding Google’s intended practices. Google cannot have it both ways.

The GDPR was not designed, and does not support an attempt by the world’s largest AdTech player which plays a role in nearly every facet of transactions from the buying to selling to negotiation between the two, to place publishers in the untenable legal and economic position of shouldering the entire burden of data protection legislation designed to mitigate the significant risks to individual, fundamental rights and freedoms created by Google’s behind-the-scenes practices.

## **RECOMMENDATION**

While it may be the case that Google is sometimes operating as a controller, as that term is defined under the GDPR, by virtue of how its advertising services operate (e.g., through the use of sophisticated algorithms), that does not mean that Google has the right to make unilateral decisions about the use of personal data collected from publisher properties. Google is providing a service to its publisher customers, not the other way around. The publishers are the primary

controllers of that data and, perhaps more importantly, have the direct relationship with the consumer. For that reason, it is inappropriate and contrary to the GDPR (as discussed above) for Google to leverage its unique position to use the data in ways that neither the publisher nor the consumer understands or can control.

Google can and should modify its recently announced position and address its obligations under the GDPR vis-à-vis its publisher customers by:

- Agreeing to take responsibility for obtaining consent where it has a direct relationship with the consumer or other end user or data subject at issue;
- Providing full transparency regarding all of the current and anticipated data processing practices associated with its Controller Services and providing sample language for publisher customers to obtain the requisite consent such that, in situations where the publisher is the only consumer-facing entity, the publisher is capable of obtaining a legally valid consent for GDPR purposes;
- Representing and warranting in its agreement with publisher customers that it will never use personal data collected from or through publisher properties for any purpose other than to fulfill the goals of its publisher customers and provide its customers with recourse in the event it violates such representations and warranties.

For the avoidance of doubt, this is not to suggest that Google must always adopt a purely processor role. It is understood that some of the databases and predictive analytics technologies utilized by Google in the provision of the ad services require, by necessity, that Google will determine the purposes and means of the processing of personal data (e.g., in order to more accurately target advertising based on customer segments), thus making it a controller under GDPR definitions.

Nonetheless, Google should never use personal data collected from publisher properties in ways not anticipated and agreed upon by virtue its contractual relationship with its publisher customers.

- Google's agreements with its publisher customers should have mutual indemnification provisions and be subject to mutual and appropriate limitations on and carve-outs of liability, where necessary, which more accurately reflect an appropriate allocation of risk between the parties in light of their (a) GDPR obligations; (b) the nature, volume, scope, and sensitivity of personal data handled by them, respectively; and (c) their respective resources. The appropriate allocation of liability is likely to be specific to individual publisher customers, should be the subject of negotiation, and should not be addressed as a blanket "take it or leave it" form agreement with disproportionate protections for Google.