GDPR: What it Means for Google Analytics & Online Marketing

Posted by Angela_Petteys

If you've been on the Internet at all in the past few months, you've probably seen plenty of notices about privacy policy updates from one service or another. As a marketer, a few of those notices have most likely come from Google.

With the General Data Privacy Regulation (GDPR) set to go into effect on May 25th, 2018, many Internet services have been scrambling to get in compliance with the new standards – and Google is no exception. Given the nature of the services Google provides to marketers, GDPR absolutely made some significant changes in how they conduct business. And, in turn, some marketers may have to take steps to make sure their use of Google Analytics is allowable under the new rules. But a lot of marketers aren't entirely sure what exactly GDPR is, what it means for their jobs, and what they need to do to follow the rules.

What is GDPR?

GDPR is a very broad reform that gives citizens who live in the European Economic Area (EEA) and Switzerland more control over how their personal data is collected and used online. GDPR introduces a lot of new rules and if you're up for a little light reading, you can check out the full text of the regulation online. But here are a few of the most significant changes:

- Companies and other organizations have to be more transparent and clearly state what information they're

collecting, what it will be used for, how they're collecting it, and if that information will be shared with anyone else. They can also only collect information that is directly relevant for its intended use. If the organization collecting that information later decides to use it for a different purpose, they must get permission again from each individual.

- GDPR also spells out how that information needs to be given to consumers. That information can no longer be hidden in long privacy policies filled with legal jargon. The information in disclosures needs to be written in plain language and "freely given, specific, informed, and unambiguous." Individuals also have to take an action which clearly gives their consent to their information being collected. Pre-checked boxes and notices that rely on inaction as a way of giving consent will no longer be allowed. If a user does not agree to have their information collected, you cannot block them from accessing content based on that fact.
- Consumers also have the right to see what information a company has about them, request that incorrect information be corrected, revoke permission for their data to be saved, and have their data exported so they can switch to another service. If someone decides to revoke their permission, the organization needs to not only remove that information from their systems in a timely manner, they also need to have it removed from anywhere else they've shared that information.
- Organizations must also be able to give proof of the steps they're taking to be in compliance. This can include keeping records of how people opt in to being on marketing lists and documentation regarding how customer information is being protected.
- Once an individual's information has been collected, GDPR sets out requirements for how that information is stored and protected. If a data breach occurs, consumers must be notified within 72 hours. Failing to comply with

> GDPR can come with some very steep consequences. If a data breach occurs because of non-compliance, a company can be hit with fines as high as €20 million or 4% of the company's annual global revenue, whichever amount is greater.

Do US-based businesses need to worry about GDPR?

Just because a business isn't based in Europe doesn't necessarily mean they're off the hook as far as GDPR goes. If a company is based in the United States (or elsewhere outside the EEA), but conducts business in Europe, collects data about users from Europe, markets themselves in Europe, or has employees who work in Europe, GDPR applies to them, too.

Even if you're working with a company that only conducts business in a very specific geographic area, you might occasionally get some visitors to your site from people outside of that region. For example, let's say a pizza restaurant in Detroit publishes a blog post about the history of pizza on their site. It's a pretty informative post and as a result, it brings in some traffic from pizza enthusiasts outside the Detroit area, including a few visitors from Spain. Would GDPR still apply in that sort of situation?

As long as it's clear that a company's goods or services are only available to consumers in the United States (or another country outside the EEA), GDPR does not apply. Going back to the pizza restaurant example, the other content on their site is written in English, emphasizes their Detroit location, and definitely doesn't make any references to delivery to Spain, so those few page views from Spain wouldn't be anything to worry about.

However, let's say another US-based company has a site with the option to view German and French language versions of

pages, lets customers pay with Euros, and uses marketing language that refers to European customers. In that situation, GDPR would apply since they are more clearly soliciting business from people in Europe.

Google Analytics & GDPR

If you use Google Analytics, Google is your data processor and since they handle data from people all over the world, they've had to take steps to become compliant with GDPR standards. However, you/your company are considered the data controller in this relationship and you will also need to take steps to make sure your Google Analytics account is set up to meet the new requirements.

Google has been rolling out some new features to help make this happen. In Analytics, you will now have the ability to delete the information of individual users if they request it. They've also introduced data retention settings which allow you to control how long individual user data is saved before being automatically deleted. Google has set this to be 26 months as the default setting, but if you are working with a US-based company that strictly conducts business in the United States, you can set it to never expire if you want to – at least until data protection laws change here, too. It's important to note that this only applies to data about individual users and events, so aggregate data about high-level information like page views won't be impacted by this.

To make sure you're using Analytics in compliance with GDPR, a good place to start is by auditing all the data you collect to make sure it's all relevant to its intended purpose and that you aren't accidentally sending any personally identifiable information (PII) to Google Analytics. Sending PII to Google Analytics was already against its Terms of Service, but very often, it happens by accident when information is pushed through in a page URL. If it turns out you are sending PII to

Analytics, you'll need to talk to your web development team about how to fix it because using filters in Analytics to block it isn't enough – you need to make sure it's never sent to Google Analytics in the first place.

PII includes anything that can potentially be used to identify a specific person, either on its own or when combined with another piece of information, like an email address, a home address, a birthdate, a zip code, or an IP address. IP addresses weren't always considered PII, but GDPR classifies them as an online identifier. Don't worry, though – you can still get geographical insights about the visitors to your site. All you have to do is turn on IP anonymization and the last portion of an IP address will be replaced with a zero, so you can still get a general idea of where your traffic is coming from, although it will be a little less precise.

If you use Google Tag Manager, IP anonymization is pretty easy. Just open your Google Analytics tag or its settings variable, choose "More Settings," and select "Fields to Set." Then, choose "anonymizeip" in the "Field Name" box, enter "true" in the "Value" box," and save your changes.

If you don't use GTM, talk to your web development team about editing the Google Analytics code to anonymize IP addresses.

Pseudonymous information like user IDs and transaction IDs are still acceptable under GDPR, but it needs to be protected. User and transaction IDs need to be alphanumeric database identifiers, not written out in plain text.

Also, if you haven't already done so, don't forget to take the steps Google has mentioned in some of those emails they've sent out. If you're based outside the EEA and GDPR applies to you, go into your Google Analytics account settings and accept

the updated terms of processing. If you're based in the EEA, the updated terms have already been included in your data processing terms. If GDPR applies to you, you'll also need to go into your organization settings and provide contact information for your organization.

Privacy policies, forms, & cookie notices

Now that you've gone through your data and checked your settings in Google Analytics, you need to update your site's privacy policy, forms, and cookie notices. If your company has a legal department, it may be best to involve them in this process to make sure you're fully compliant.

Under GDPR, a site's privacy policy needs to be clearly written in plain language and answer basic questions like what information is being collected, why it's being collected, how it's being collected, who is collecting it, how it will be used, and if it will be shared with anyone else. If your site is likely to be visited by children, this information needs to be written simply enough for a child to be able to understand it.

Forms and cookie notices also need to provide that kind of information. Cookie consent forms with really vague, generic messages like, "We use cookies to give you a better experience and by using this site, you agree to our policy," are not GDPR compliant.

GDPR & other types of marketing

The impact GDPR will have on marketers isn't just limited to how you use Google Analytics. If you use some particular types of marketing in the course of your job, you may have to make a few other changes, too.

Referral deals

If you work with a company that does “refer a friend”-type promotions where a customer has to enter information for a friend to receive a discount, GDPR is going to make a difference for you. Giving consent for data to be collected is a key part of GDPR and in these sorts of promotions, the person being referred can’t clearly consent to their information being collected. Under GDPR, it is possible to continue this practice, but it all depends on how that information is being used. If you store the information of the person being referred and use it for marketing purposes, it would be a violation of GDPR standards. However, if you don’t store that information or process it, you’re OK.

Email marketing

If you’re an email marketer and already follow best industry standards by doing things like only sending messages to those who clearly opt in to your list and making it easy for people to unsubscribe, the good news is that you’re probably in pretty good shape. As far as email marketing goes, GDPR is going to have the biggest impact on those who do things that have already been considered sketchy, like buying lists of contacts or not making it clear when someone is signing up to receive emails from you.

Even if you think you’re good to go, it’s still a good time to review your contacts and double check that your European contacts have indeed opted into being on your list and that it was clear what they were signing up for. If any of your contacts don’t have their country listed or you’re not sure how they opted in, you may want to either remove them from your list or put them on a separate segment so they don’t get any messages from you until you can get that figured out. Even if you’re confident your European contacts have opted in, there’s no harm in sending out an email asking them to confirm

that they would like to continue receiving messages from you.

Creating a double opt-in process isn’t mandatory, but it would be a good idea since it helps remove any doubt over whether or not a person has agreed to being on your list. While you’re at it, take a look at the forms people use to sign up to be on your list and make sure they’re in line with GDPR standards, with no pre-checked boxes and the fact that they’re agreeing to receive emails from you is very clear.

For example, here’s a non-GDPR compliant email signup option I recently saw on a checkout page. They tell you what they’re planning to send to you, but the fact that it’s a pre-checked box placed underneath the more prominent “Place Order” button makes it very easy for people to unintentionally sign up for emails they might not actually want.

Jimmy Choo, on the other hand, also gives you the chance to sign up for emails while making a purchase, but since the box isn’t pre-checked, it’s good to go under GDPR.

Marketing automation

As is the case with standard email marketing, marketing automation specialists will need to make sure they have clear consent from everyone who has agreed to be part of their lists. Check your European contacts to make sure you know how they’ve opted in. Also review the ways people can opt into your list to make sure it’s clear what, exactly, they’re signing up for so that your existing contacts would be considered valid.

If you use marketing automation to re-engage customers who have been inactive for a while, you may need to get permission to contact them again, depending on how long it has been since they last interacted with you.

Some marketing automation platforms have functionality which will be impacted by GDPR. Lead scoring, for example, is now considered a form of profiling and you will need to get permission from individuals to have their information used in that way. Reverse IP tracking also needs consent.

It’s also important to make sure your marketing automation platform and CRM system are set to sync automatically. If a person on your list unsubscribes and continues receiving emails because of a lapse between the two, you could get in trouble for not being GDPR compliant.

Gated content

A lot of companies use gated content, like free reports, whitepapers, or webinars, as a way to generate leads. The way they see it, the person’s information serves as the price of admission. But since GDPR prohibits blocking access to content if a person doesn’t consent to their information being collected, is gated content effectively useless now?

GDPR doesn’t completely eliminate the possibility of gated content, but there are now higher standards for collecting user information. Basically, if you’re going to have gated content, you need to be able to prove that the information you collect is necessary for you to provide the deliverable. For example, if you were organizing a webinar, you’d be justified in collecting email addresses since attendees need to be sent a link to join in. You’d have a harder time claiming an email address was required for something like a whitepaper since that doesn’t necessarily have to be delivered via email. And of course, as with any other form on a site, forms for gated content need to clearly state all the necessary information

about how the information being collected will be used.

If you don’t get a lot of leads from European users anyway, you may want to just block all gated content from European visitors. Another option would be to go ahead and make that information freely available to visitors from Europe.

Google AdWords

If you use Google AdWords to advertise to European residents, Google already required publishers and advertisers to get permission from end users by putting disclaimers on the landing page, but GDPR will be making some changes to these requirements. Google will now be requiring publishers to get clear consent from individuals to have their information collected. Not only does this mean you have to give more information about how a person’s information will be used, you’ll also need to keep records of consent and tell users how they can opt out later on if they want to do so. If a person doesn’t give consent to having their information collected, Google will be making it possible to serve them non-personalized ads.

In the end

GDPR is a significant change and trying to grasp the full scope of its changes is pretty daunting. This is far from being a comprehensive guide, so if you have any questions about how GDPR applies to a particular client you’re working with, it may be best to get in touch with their legal department or team. GDPR will impact some industries more than others, so it’s best to get some input from someone who truly understands the law and how it applies to that specific business.

Sign up for The Moz Top 10, a semimonthly mailer updating you on the top ten hottest pieces of SEO news, tips, and rad links

uncovered by the Moz team. Think of it as your exclusive digest of stuff you don’t have time to hunt down but want to read!

http://tracking.feedpress.it/link/9375/9220491?utm_medium=feed&utm_source=feedpress.me&utm_campaign=Feed%3A+mozblog