Is Google Analytics compliant with GDPR?

GDPR (General Data Protection Regulation) is set to revolutionize how we process and store data in the digital age, with the aim of giving individuals more control of their personal data.

Google Analytics will act as the data processor and your organization as the data controller since your organization is in control of what data you send to Google Analytics once the Universal Analytics tracking code implementation is up and running.

This article will explore the steps Google Analytics is taking to become GDPR compliant, as well as what *your business* can do to make sure you too are compliant with GDPR.

What steps is Google taking?

Google recently released a statement declaring their commitment to compliance with data protection laws in line with GDPR. Google went on to explain that they have measures in place relating to privacy and data processing. For a comprehensive look at Google's processing terms, you can learn more by reading their Google Ads Data processing terms, which is set to replace and supersede the Analytics Data Processing Amendment.

Google encourages data controllers to be vigilant about how they collect and handle data. Numerous GDPR-related guides online can help you to ensure you are knowledgeable about GDPR and the effects it could have on your company.

Google has updated Google Analytics with a new feature called 'User and event data retention'. This feature allows the data controller to decide how long to store and retain data.

The feature relates specifically to data associated with cookies, user identifiers, or advertising identifiers. As the data controller, you can set a fixed time limit before expiry. You can also choose not to include an automatic expiry time limit.

The ‘User and event data retention’ feature is set to come into play on May 25– the day when GDPR regulations hit.

Google recently released a statement on the topic:

We have all opened emails and messages like this one lately regarding GDPR updates. Moreover, you might be tempted to ignore or delete it without paying it much attention. However, we strongly urge you to take your time to read the email that Google sent, and to review your user and event data retention setting in Google Analytics.

GDPR means securing your website is more important than ever

A great way to help secure your users' data is to install an SSL certificate for your website. Adding a secure sockets layer certificate helps ensure that all data sent between the web server and the browser is secure. An SSL certificate also

comes with the added bonus of being a ranking factor in Google’s SERPs.

Securing your website and securing client data is vital. Non-compliance could lead to hefty fines of up to €20 million or 4% of annual turnover, whichever is the greater sum.

We know that many readers here at Search Engine Watch use a WordPress CMS for their websites.

If you use a WordPress website, we suggest that you make sure all of your plugins are up-to-date. You should also install plugins such as Wordfence and WP Limited Login Attempts.

For a comprehensive guide to securing a WordPress website, see here.

https://searchenginewatch.com/2018/05/09/is-google-analytics-compliant-with-gdpr/