Whitepaper

Google Analytics – Data Protection Risk and Damage

About the widespread use of Google Analytics, the first bans in EU countries, the current status in Germany and possible implications for cyber insurance.

Marcel Arnold
Florian Emmerich
Jonas Schwade
Jan Spittka

CONTENT

Management summary

- The EU General Data Protection Regulation (GDPR) and the invalidity of the Privacy Shield between the EU and the USA raise considerable doubts about the legally compliant use of Google Analytics in Europe.
- The transfer of IP addresses to Google constitutes a transfer of personal data to a third country within the meaning of the GDPR.
- The first national data protection authorities have already imposed concrete bans on the integration of Google Analytics on websites of domestic operators.
- A study using the cyber risk assessment tool cysmo® clearly shows that Google Analytics is still embedded in the vast majority of European corporate websites. This is true even for countries that have officially banned it.
- Even the option granted by the analytics tool to anonymise the IP address is not universally used by website operators in Germany; more than one fifth have not activated this setting.
- Given the factual and legal situation, a ban on Google Analytics in Germany is to be expected.
- Whether cyber insurances have to pay for any damages resulting from the use of Google Analytics – such as claims for damages by third parties based on a personal data breach – depends on the wording of the respective policies.
- In any case, insurance companies should make their customers aware of the consequences of a ban as soon as it is issued. This way, they can prove in case of doubt that the policyholders had knowledge of their unlawful conduct.

Google Analytics – a curse and a blessing at once?

The dispute between data protectionists and marketing specialists about Google Analytics, its functions and their legal assessment has been smouldering for a long time. However, at the latest since the invalidity of the Privacy Shield in 2018[1], there are serious doubts about the lawful use of the analytics tool within the scope of the European General Data Protection Regulation (GDPR). After all, the transfer of IP addresses to Google also constitutes a transfer of personal data to a third country. Recently, even authorities of individual countries within the EU have issued bans on the use of the analytics tool.

What is Google Analytics?

In short, Google Analytics is an analysis tool that enables you to evaluate the performance, especially the behaviour of customers, on your own website.

For this purpose, Google Analytics[2] can analyse, among other things, the number of website visitors and their time spent on the website. Depending on the configuration, even information about the location of website visitors and their spending amounts in web shops can be determined. The tool is provided by Google mostly free of charge, but in return some of the information collected is passed on to Google. This allows Google to combine the data with information from other services such as Youtube or Google Ads[3] and to determine further characteristics such as age or gender to create extensive user profiles.

Depending on the configuration, Google Analytics even provides location data and sales information on website visitors.

[1] Media release of the German data protection conference, 28/07/2020
[2] Google LLC / Google Ireland Ltd., Google Analytics FAQ
[3] Google LLC / Google Ireland Ltd., Google Analytics FAQ

Which European countries have banned the use of Google Analytics?

For the first time at the end of 2021[4] and again in spring 2022[5], the Austrian data protection authority decided that the use of Google Analytics violates the GDPR and the tool may therefore no longer be used. Austria was thus the first country in Europe to pronounce a ban in such concrete terms. After a short time, the supervisory authorities in France[6], Italy[7] and most recently Denmark[8] followed suit. In Spain and Luxembourg[9], on the other hand, complaints with the same wording were reportedly rejected, albeit not due to a legally different opinion, but because the respective companies removed the tools before a decision was made. Some other countries, specifically the Netherlands[10], Norway[11] and Liechtenstein[12], have issued warnings about the use of Google Analytics and referred to alternative services in view of the review coordinated by the task force[13] of the European Data Protection Board.

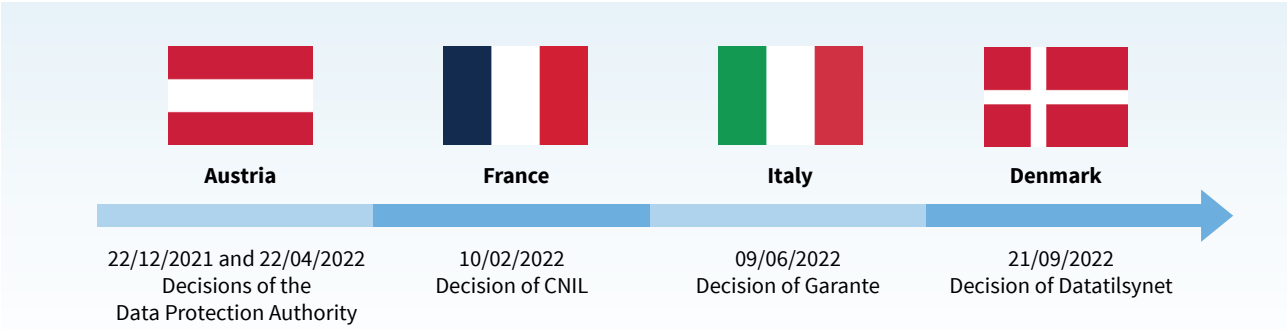
Some countries have issued warnings first; bans on Google Analytics may follow there as well.

It therefore seems only a matter of time before these and other countries will issue a ban as well. However, it must be taken into account that the aforementioned "bans" are merely the legal interpretations of the respective data protection supervisory authorities. Court decisions confirming this opinion are not yet available.

The opinions of the data protection authorities have not yet been confirmed by the courts.

[4] Data protection authority, Austria, ZI. D155.027, 2021-0.586.257
[5] NOYB: Auch für CNIL Datenübertragung an Google Analytics rechtswidrig, 10/02/2022
[6] CNIL, Information dated 10/02/2022
[7] GPDP, Information dated 23/06/2022
[8] Datatilsynet, Information dated 21/09/2022
[9] NOYB: Italienische Datenschutzbehörde: Datenübermittlung an Google Analytics illegal, 05/07/2022
[10] Autoriteit Persoonsgegevens, Handleiding of 22/04/2022
[11] Datatilsynet, Information dated 26/01/2022
[12] Data protection authority of the Principality of Liechtenstein, Information dated 03/03/2022
[13] European Data Protection Board, 37th plenary session, 04/09/2020

Ban on the use of Google Analytics in European countries



Source: PPI AG

Austria led the way: in the medium term, the number of countries that ban the use of Google Analytics on websites will continue to increase.

Why is Google Analytics not considered GDPR-compliant by default?

In principle, analytics tools can be used in a GDPR-compliant manner. For example, the French supervisory authority CNIL has considered the measurement of website visitors per page and the collection of statistics, in particular on dwell time and user actions such as clicks, selections and scroll depth, a necessary measure for the proper management of a website[14]. However, it depends on the concrete design of the respective tool. For Google Analytics, even in the current version 4, the problem of data transfer to Google in the USA keeps coming up time and again. Although Google itself states[15] that Google Analytics 4 "does not log or store individual IP addresses" and the data is collected "through domains and on servers based in the EU", it is ultimately[16] forwarded to the "Analytics processing servers [in the USA] and made available to you in the Analytics platform".

By forwarding IP addresses to the USA, Google Analytics is in a conflict of principle with the GDPR that is difficult to resolve.

"Google can make as many adjustments as they want, the supervisory authorities will not let up."

[14] CNIL, Information dated 23/09/2021
[15] Google LLC / Google Ireland Ltd., Google Analytics FAQ
[16] Google LLC / Google Ireland Ltd., Google Analytics FAQ

Problematic legal situation in the USA

It is precisely this transfer of data that is a thorn in the side of the courts and supervisory authorities. In the USA, for example, much-discussed legislation makes it possible for security authorities to access data. And it is precisely this theoretical possibility that is the crucial point, because a risk-based approach to third-country transfers – as is otherwise quite common in the GDPR – is not decisive according to the supervisory authorities. Therefore, users of Google Analytics cannot plead that the probability of actual access is low and that their interest in the data transfer outweighs this.

The supervisory authorities essentially justify the alleged illegality of Google Analytics with three points:

1. The GDPR does not acknowledge any risk-based approach, which at least contradicts previous views of German supervisory authorities.
2. The IP anonymisation only concerns the IP address and not other online identifiers or device data stored by cookies.
3. The data would in any case only be encrypted by Google itself after it had already been transferred to Google, in which case it is apparently irrelevant for the supervisory authorities that the encryption takes place on EU servers.

As a small ray of hope, the French supervisory authority has issued a recommendation[17], to which the Danish authority also refers, according to which Google Analytics can be used in a GDPR-compliant manner by means of a workaround. For this purpose, however, a proxy server must be set up between data collection and transmission on which the information is pseudonymised beforehand. This not only means a cost-intensive technical effort, but also leads to the loss of essential functions of Google Analytics.

An intermediate proxy server could make Google Analytics GDPR-compliant.

[17] CNIL, Information dated 20/07/2022

cysmo® provides distribution statistics

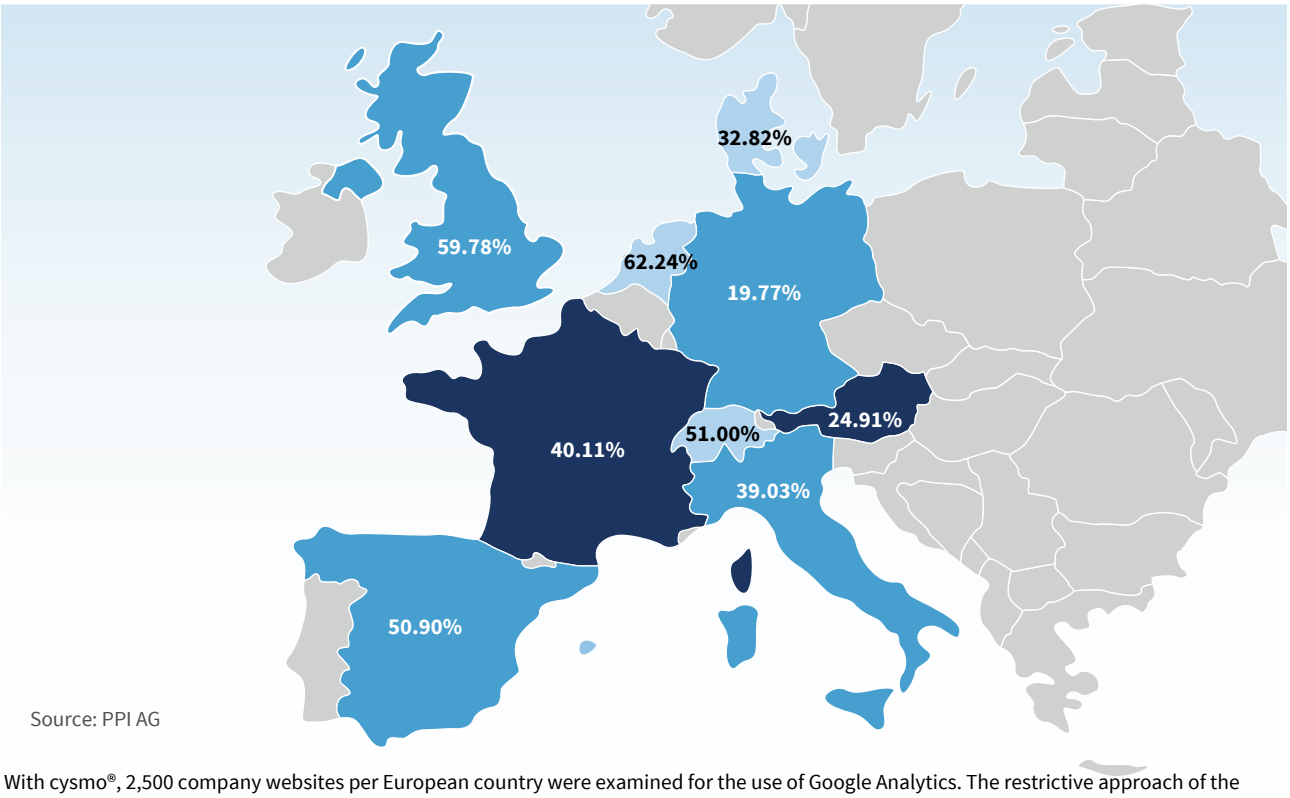
A large number of companies worldwide use Google Analytics to be able to evaluate the user behaviour of their website visitors more precisely. But how widespread is it actually among the companies?

In order to obtain more precise figures, an evaluation was carried out with the fully automated cyber risk assessment tool cysmo®. In addition to assessing current threats such as DDoS, phishing, exploits and data breaches in real time, the use of trackers can also be identified and evaluated by cysmo®. The tool is mainly used by insurance companies in the field of cyber insurance to identify risks even better and assess them correctly.

With the help of cysmo®, the actual usage of Google Analytics on European corporate websites was checked.

For the evaluations, websites of 2,500 companies in each of nine European countries were checked with cysmo® for the use of Google Analytics: Germany, Denmark, France, Italy, the Netherlands, Austria, Switzerland, Spain and Great Britain. The following map shows the identified percentages of use.

Google Analytics usage rates on corporate websites



With cysmo®, 2,500 company websites per European country were examined for the use of Google Analytics. The restrictive approach of the data protection authorities shows clear effects.

The cysmo® evaluation clearly shows: although four countries have already issued a ban on the use of Google Analytics, it is still used extensively in these countries.

In Italy 984, in Denmark 817 and in France 815 of the 2,500 companies tested still use Google Analytics. In Austria, 577 users also show that the ban is not yet implemented by the majority of companies.

How is the situation in Germany?

In Germany, too, a decision by the Higher Regional Court of Karlsruhe in the context of a procurement procedure and a ruling by the Munich Regional Court I[19] on Google Fonts have recently caused a stir. The Data Protection Conference (DSK) has already pointed out in its guide on telemedia[20] that in the case of analytics tools, often no sufficient supplementary measures will be possible, which is why in this case, the services concerned may not be used, i.e. may not be integrated into the website either.

Accordingly, the decisive factor is whether sufficient protective measures are taken against access by authorities in third countries, i.e. whether and how Google Analytics can even be configured. As early as 2020, the German supervisory authorities pointed out in special instructions on the use of Google Analytics[21] that the transmitted IP address must be shortened and thus pseudonymised. In Google Analytics 4, this is activated by default and IP addresses would allegedly neither be logged nor stored[22]. However, the supervisory authorities take a different view. Nevertheless, as many as 675 of the 2,500 companies checked by the cysmo® analysis had not shortened the IP addresses.

According to German supervisory authorities, the IP address must be pseudonymised when using Google Analytics.

"A ban on Google Analytics seems inevitable in Germany as well."

[18] OLG Karlsruhe, Decision of 07/09/2022, 15 Verg 8/22
[19] LG München I, Judgement handed down 20/01/2022, 3 O 17493/20
[20] Orientation handout of the data protection conference dated 20/12/2021
[21] Decision of the data protection conference dated 12/05/2020
[22] Google LLC / Google Ireland Ltd., Google Analytics FAQ

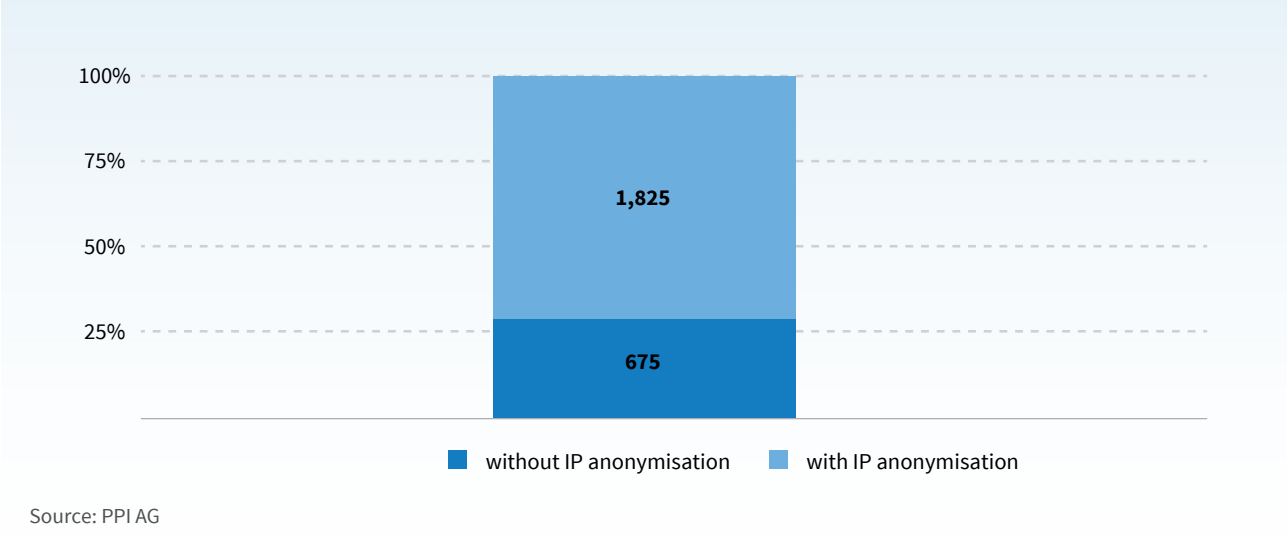
From the supervisory authorities' perspective, obtaining consent for the use of Google Analytics from the website visitor does not help either, as the legal basis of Article 49 para. 1 lit. (a) of the GDPR is essentially not applicable for two reasons:

1. The article constitutes an exceptional provision which can therefore not be used for recurrent and mass data transfers.
2. Google uses the data for its own purposes, which is why this is considered to be a processing by joint controllers and not – as necessary for Article 49 GDPR – a processing by a processor.

It therefore seems inevitable that a ban on Google Analytics will also follow in Germany – especially considering that the German supervisory authorities often apply stricter standards than those of their European neighbours. Just recently[23] the authorities addressed the topic Google Analytics again at their data protection conference.

German supervisory authorities often apply stricter standards than the data protection authorities of other European countries.

Proportion of Google Analytics users with IP anonymisation



Source: PPI AG

The shortening of the transmitted IP address, which is actually a standard feature of Google Analytics 4, is not utilised by around 30 percent of the German corporate websites surveyed, which clearly contradicts the legal opinions of the supervisory authorities.

[23] Minutes of the intermediate session of the data protection conference dated 22/06/2022

What impact will a ban have on cyber insurance?

A uniform evaluation for all insurances is difficult, as the different cyber policies often contain different definitions of an “information security breach” and “data protection breach”.

General statements on the effect of a ban on cyber policies cannot be made due to the large number of possible definitions in the conditions.

From the review of a large number of terms and conditions of individual insurance companies, three main cases can be identified for possible damages in relation to Google Analytics:

1. Such damages are not covered per se, as the insurance policy does not cover a data breach without an information security breach, such as a ransomware attack.
2. Such damages are covered by the insurance policy, but exclusions apply.
3. Such damages are covered by the insurance policy and the insurer has to pay.

In some policies, a data protection breach – regardless of its specific definition – is only covered if it occurs in connection with an information security breach. In other policies, exclusions for fines or claims for damages by data subjects are included, which is why no case of coverage occurs here either. However, we have also found that some wordings insure a data protection breach independently of an information security breach.

There are cases where a data protection breach is covered even without an information security breach.

One common definition of a data protection breach is as follows:

"A data protection breach occurs if, in accordance with the General Data Protection Regulation (GDPR), the German Federal Data Protection Act (BDSG) or other rules on data protection, an invalid or incorrect

- collection,
- processing or
- use

of personal data of third parties is carried out by the policyholder. This also applies in the event of a violation of comparable foreign legal standards."

In such a definition, the use of Google Analytics, i.e. the collection of data on the website as well as the processing in the form of third country transfer by the analytics tool itself, in contradiction to a potential ban, would be included. Insurers would therefore have to pay for corresponding damages.

"Even small amounts can lead to huge damages."

Such damages, in addition to a fine of up to 20 million euros or four percent of the annual global turnover, can also be caused by commercial damage claims under Article 82 GDPR made by lone fighters or legal tech providers. The Google Fonts ruling was already followed by mass claims against companies in Germany. Since Google Analytics processes far more extensive information, such claims and lawsuits are all the more to be expected after a ban. Even an amount of 200 euros per website visitor would mean a whole 10 million euros for 50,000 visitors, which is likely to exceed many an insurance policies – not including the costs for legal advice and defence.

The extent of damage can quickly exceed the sum insured of a policy.

However, the obligation to pay may lapse according to Sec. 81 (1) of the Insurance Contract Act (VVG). For that, the website operator would have to consider it possible and accept that the use of Google Analytics could lead to a breach of data protection, which would result in damage and the occurrence of the insured event. Should the management be aware of a ban, this will regularly be affirmed on the grounds of a systematic unlawful use of the tool. In the case of a ban – if an exclusion is not intended anyways – insurance companies should point out the issue to their policyholders, to be able to prove the latter's knowledge of it. The same also applies to claims for damages by data subjects pursuant to Sec. 103 VVG, since the required unlawfulness already lies in the breach of the GDPR.

Insurance companies should make their policyholders aware of a ban on Google Analytics in order to be able to prove their knowledge of it.

Content partners

CLYDE&CO

Clyde & Co is a leading global law firm, specializing in the sectors that underpin global trade and commercial activity, namely: insurance, transport, infrastructure, energy, and trade and commodities. With over 60 offices and associated offices across six continents and 3,200 legal professionals worldwide, we offer a comprehensive range of contentious and non-contentious legal services and commercially-minded legal advice to businesses operating across the world. In Germany, more than 60 lawyers in our offices in Düsseldorf, Hamburg and Munich combine deep local market understanding with a global overview. In the area of cyber and data protection, our global cyber risk group offers one-stop advice – from product design to conflict resolution in relation to cyberattacks or data leaks. We can draw on our wealth of experience from over 2,000 cyber incidents in cyber and data security – including some of the largest and most high-profile incidents worldwide.

Clyde & Co
Dreischeibenhaus 1
40211 Düsseldorf
www.clydeco.com

ppi

PPI AG has been working successfully as a consulting and software company for financial institutions, insurance companies and financial services providers for over 30 years. As a steadily growing, family owned joint-stock company, we combine business and technology expertise to realise projects competently and in an uncomplicated manner. Our about 700 employees are entirely focused on our customers' success. PPI offers insurance companies excellent technical and methodological solutions for all core processes of the insurance business. PPI's advantage: high-quality, easy-to-integrate software solutions made in Germany. For the development of cysmo® as an innovative rating tool for cyber risk assessment, PPI has combined know-how in insurance and IT with the expertise of white-hat hackers.

PPI AG
Moorfuhrtweg 13
22301 Hamburg
www.ppi.de/en

Authors

Marcel Arnold
Cyber Consultant
PPI AG
M: +49 160 90873531
marcel.arnold@ppi.de

Jonas Schwade
Product Manager
PPI AG
M: +49 151 26737115
jonas.schwade@ppi.de

Florian Emmerich
Lawyer and Associate in Data Protection Law and Cybersecurity
Clyde & Co Europe LLP
T: +49 211 8822 8828
florian.emmerich@clydeco.com

Jan Spittka
Lawyer and Partner in Data Protection Law and Cybersecurity
Clyde & Co Europe LLP
T: +49 211 8822 8863
jan.spittka@clydeco.com