Enforcement by European DPAs against data transfers

What can organisations do if they have relied on Google Analytics to measure the effectiveness of their website? **Katharina A. Weimer** of Fieldfisher Germany explores the issues.

In the immediate aftermath of the ECJ ruling *Schrems II* (C311/18), there was a stunned silence, while companies and data protection authorities alike grappled with the consequences. The data protection authorities started issuing guidelines and opinions, making it quite clear that there was no grace period for making the necessary changes and that it was their obligation to enforce the ruling, with all its consequences. And of those there are many. Most notably, any transfer (including making available) of personal data from the EU/EEA to a recipient outside of the EU/EEA now entailed a whole host of new assessments and documentation, without the help of the Privacy Shield for transfers to the US. It seemed that all of a sudden, the question of "adequate level of safety" for the data transferred was now to be taken seriously, even for transfers to the US.

What this means in practice is that for all transfers, the data exporter must assess (i) its data transfers, (ii) the transfer mechanism relied upon (i.e. standard contractual clauses, binding corporate rules, individual consent, or other), (iii) effectiveness of the transfer mechanism (by assessing inter alia the laws and practices in the recipient country), and (iv) the supplementary measures necessary, if any, to ensure the adequate level of safety for the personal data which is to be transferred (organizational, contractual and technical measures).

Without recapping all the details of the legal landscape in the US which was subject to the *Schrems II* ruling, and going into the fineprint of the US Clarifying Lawful Overseas Use of Data (CLOUD) Act, the implications of these legislative acts seem clear:

They generally allow for access to (or request for) personal data of EU citizens in the control of (certain types of) US companies and/or their subsidiaries outside of the US, by certain US governmental and/or national security bodies and agencies, subject to certain conditions. Such access cannot be barred by the companies which are subject to these laws, although there are legal remedies against this access/request. It can also not be excluded by contract, due to the very nature of national administrative laws granting powers to governmental or national security agencies.

In essence this means that transfer of personal data to the US seems possible only with comprehensive technological safeguards which render a deciphering of the personal data by unauthorized recipients in the US (and elsewhere) impossible.

In recent months, there have been several decisions by courts and data protection authorities relating to such transfer to recipients outside the EU/EEA, all of them relating to the US. What seems important is the level of detail in which the transfers have been investigated, and the arguably negligible amount and type of data that was transferred. While it had seemed clear to most companies transferring data to recipients outside the EU/EEA that they would have to investigate their main business activities, the material data transfers and in particular assess any transfers of sensitive data, this regulatory and judicial review goes far beyond any such initial review. It aims at the fundamental principles of the functionalities of the Internet and global communication as we currently use it, and requires meaningful changes that will come at a price.

Hochschule RheinMain

In a preliminary injunction administrative proceeding before the administrative court in Wiesbaden (Hessen), an individual required the Hochschule RheinMain, a public educational institution (Hochschule), to refrain from using the service "Cookiebot" for the purposes of obtaining consent to cookies if that includes the transfer of personal or personally identifiable data (including IP address) to servers operated by US group Akamai Technologies Inc.

The Hochschule uses a Cookiebot for its cookie consent management tool. The Cookiebot collects the IP address (although it was in dispute as to whether it was anonymized with the last three digits set to "0", or not), date and time of consent, user agent of the browser, URL, an anonymous, random and encrypted key, and the consent status of the data subject. For its services, it uses the content delivery network of Akamai Technologies, Inc. (Akamai) for requesting the consent script which is hosted on Akamai's servers. According to the data processing agreement provided by Akamai, the time stamps of the visited websites and the respective IP addresses, as well as the geographical location based on the IP address and telemetric data are also collected.

The administrative court of Wiesbaden held that this constitutes a transfer which is without legal basis and therefore not permissible, as none of the legal bases of Art. 48/49 GDPR are applicable. The user has not consented to the transfer, a legitimate interest cannot be determined, and there is no indication for any other justification. The court went into great detail to determine how the collected data can be combined to identify the user, with the help of the IP address – even if the name of the user is not known, the individual can be identified.

The fact that the contractual partner of the Cookiebot operator Cybot A/S is the German Akamai Technologies GmbH, was of no relevance because the server structure of the parent company Akamai Technologies Inc. was being used for the Content Delivery Network services. The existence of model clauses between Cybot A/S and Akamai was also not discussed.

The decision was upturned upon appeal but only because the Higher Administrative Court held that there were no grounds for a decision in preliminary proceedings due to lack of urgency. In the Higher Administrative Court's opinion, the complexity of the case, as well as its importance, do not permit a decision in preliminary proceedings, and have to be assessed in proceedings on their merits. This case on the merits is currently pending with the Administrative Court of Wiesbaden.

The takeaway from this proceeding is that users and courts are now prepared to take a deep-dive into the details of functionalities that are being used, and that companies have to be prepared to respond to this method in a granularity previously unseen. This extends to seemingly irrelevant / unimportant data such as (anonymized) IP addresses, URLs, time stamps, and other machine information, as the combination of these can lead to creating profiles of individual users. Transfers of such personal data to recipients outside the EU/EEA require a valid justification (e.g. consent).

Google Analytics

The last couple of months have also seen several decisions by Data Protection Authorities (DPAs) involving Google Analytics. Some of these decisions result from investigations following complaints launched by NOYB, the organisation founded by Max Schrems. NOYB had submitted roughly 100 formal complaints with all European data protection authorities regarding the use of cookies (including Google Analytics) on websites. It is important to note that the European DPAs have orchestrated their responses / decisions on these complaints.

a) Austria's DPA: In December 2021, the Austrian DPA decided on a complaint by NOYB against a website operator who had implemented the cost-free version of Google Analytics. The Austrian DPA determined that the combination of information collected by Google Analytics (such as browser type, operating system, host name, referrer and language, screen resolution, and others) with the Unique User Identification (UUI) numbers (which uniquely identify the browser and the device, respectively, of the user) placed by Google Analytics cookies, and the IP address, together with, in this specific case, the information on the Google Account user (because the individual complainant was logged into his/her Google Account at the time of surfing) constitutes personal data of the individual who is surfing and whose browsing behaviour is tracked. It is not necessary, in the view of the Austrian DPA, that a specific "face" of an individual, meaning in particular his/her name, is identifiable, with reference to the possibility of "singling out" an individual set forth in recital 26 of GDPR. In addition, a digital footprint is commonly deemed sufficient for uniquely identifying a device, and thereby a concrete user, and thus constitutes personal data. The circumstance that another person (in this case, Google in the US because of the log-in into the Google Account, and possibly US surveillance agencies) had access to further information which may lead to the identification of the individual was a supporting factor in the determination of the individual being identifiable, and thus the data being personal data.

Because the website operator transferred personal data to the recipient outside of the EU by using Google Analytics, it had to comply with the requirements set out by Art. 45, 46, and 49 of the GDPR. While the parties had agreed on standard contractual clauses as a transfer mechanism, it is clear since the *Schrems II* judgment that adopting standard contractual clauses alone cannot provide an adequate level of data protection. Following this judgement, Google has implemented supplementary measures to provide for additional protection and thereby, in its view, afford European personal data the level of protection required by the GDPR.

The Austrian DPA though, in its examination of the supplementary measures, questioned whether the contractual and organisational measures (such as information to the data subject in case of a request and publication of a transparency report) supported by Google are even effective in ensuring additional protection. The same applies, in the DPA's view, to the technical measures – encryption and protection in transit and "on-site security".

The relevant take-aways of the Austrian DPA's decision in summary:

- Information collected and transferred by Google Analytics constitutes personal data;
- A digital footprint is sufficient to count as personal data;
- The supplementary measures implemented by Google to protect the data transferred through Google Analytics are not effective measures.

b) France's DPA: France's DPA, the CNIL issued a press release according to which it has received complaints by NOYB regarding the data collected by Google Analytics and investigated the conditions of this service. It also comes to the conclusion, in line with the decision by the Austrian data protection authority, that such transfers are illegal. Consequently, it ordered a French website manager to comply with the GDPR (within one month) and, if necessary, discontinue using this service.

In substance, the CNIL makes the same determinations as the Austrian data protection authority and adds the noteworthy point of using Recital 30 GDPR as additional support for the analysis that online identifiers (such as IP address and cookie information) can commonly be used to identify an individual.

As the CNIL also finds that the data transferred constitutes personal data, it reviews the transfer mechanism, standard contractual clauses, which needs to be supplemented by the supplementary contractual, organisation and technical measures. It highlights the general issue with contractual measures that they can of course not bind the authorities of a third country and therefore require combining them with technical and organisational measures. However, the same applies to organisational measures which, in itself, are again not sufficient to ensure meeting the "essential equivalence" standard required by EU law. It comes down to adopting appropriate technical measures so that potentially infringing access by foreign authorities cannot identify the data subjects.

The CNIL also investigates the measures implemented by Google and

comes to the same conclusion as the Austrian data protection authority that neither the contractual and organisational, nor the technical measures implemented by Google factually prevent or reduce access.

c) Norway's DPA: Norway's DPA announced on 28 January this year an audit of Telenor ASA and confirmed that it was investigating a complaint regarding Telenor's use of Google Analytics.[1]

Information on a case before Norway's DPA, *Datatilsynet* references both the Austrian data protection authority's case as well as the CNIL's decision. In its press release it refers to the decision of Austria's and France's DPAs on the use of Google Analytics.[2]

d) EDPS: Similarly, the European Data Protection Supervisor (EDPS) issued a decision against the European Parliament in which it found that the European Parliament violated data protection laws ("GDPR for EU institutions", 2018/1725) in using Google Analytics, among others. This decision also followed a complaint by NOYB in January 2021 and confirmed that an internal Corona testing website transferred personal data to the US without ensuring contractual, technical or organisational measures to ensure essential equivalence of the level of protection.

What is next?

It seems clear that other European DPAs will follow suit regarding the NOYB complaints pending with them, and issue orders of compliance and/or cessation. Website operators are currently in limbo: often their entire analytical framework for website traffic is based on Google Analytics, and they have made considerable investments into this structure, leaving them reluctant to investigate alternatives which may not provide the level of insight Google Analytics can provide. However, it is currently not possible for them to use Google Analytics in a GDPR-compliant manner – or is there a way?

While there is no official "way forward" from Google yet, the use of server-side tagging[3] may bring some light to the end of the tunnel. Google claims that the server container for the tags and the data runs in the website operator's own platform or environment, and it has complete control over which data is sent and to where. Without having investigated the technical details, it seems to present a potential solution if the website operator is willing to invest the time to adopt and configure this solution carefully.

However, it can also be expected that Google will react to this concentrated effort at a more general level to address these fundamental concerns.

Conclusion

With the ever-increasing use of the Internet by individuals, and the information about individuals' preferences, likes, and activities that can be deducted through such individuals' use even by only collecting mere technical information (the digital footprint), Internet users become increasingly transparent for website operators. In fact, they have been for a long time and companies have capitalized on this knowledge for years – and have gotten away with it because the information was "only technical information".

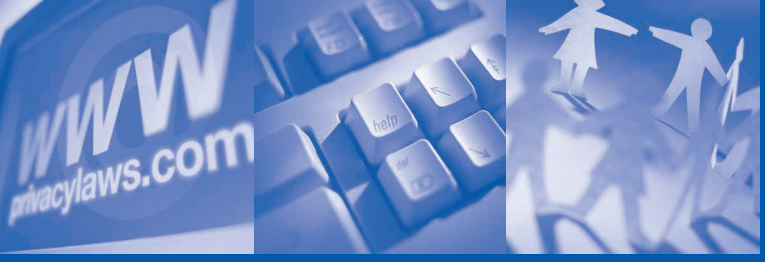
However, it is now abundantly clear that such technical information is the gateway to the digital individual, and data controllers have to concern themselves with all the details of the technical information they collect and ensure compliance with GDPR (and of course other legislation).

AUTHOR

Katharina A Weimer is a Partner at Fieldfisher Germany.
Email:
Katharina.Weimer@fieldfisher.com

REFERENCES

1 www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/tilsyn-med-telenor/
2 See (in Norweigan) www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/google-analytics-kan-vare-ulovlig/
3 See developers.google.com/tag-platform/tag-manager/server-side/intro



ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Now 157 countries: 12 data privacy laws in 2021/22

Sri Lanka, Oman and the United Arab Emirates have adopted new data protection laws in 2022. **Graham Greenleaf** reports on recent developments.

Despite the Covid pandemic, countries across the globe have continued to enact data privacy laws. At the start of 2021, 145 countries had done so,[1] but in the year since then a further 12 countries have enacted such laws, giving a total of 157 by mid-March 2022. As has become familiar, most of these laws are influenced substantially by the EU's GDPR, but with many variations in such implementations. The

Continued on p.3

Apple AirTag debacle shows we need to diversify privacy

Diversifying privacy means more than diversifying product development and privacy teams. We need to broaden the aperture and centre marginalized voices. By **Abigail Dubiniecki**, Privacy lawyer and consultant.

"Apple's website states that 'privacy is a fundamental human right,' but one of its new products apparently didn't get the memo."[1]

Apple has long made privacy a key brand differentiator, with cutting-edge privacy engineering baked into its offering. Yet the PR fallout from privacy risks that surfaced soon

Continued on p.9

Issue 176 **APRIL 2022**

INTERNATIONAL report

ISSUE NO 176 APRIL 2022

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS

Katharina A. Weimer
Fieldfisher, Germany

Nicole Wolters Ruckert and Tim Sweerts
Allen & Overy, Netherlands

Elizabeth Canter and Natalie Dugan
Covington & Burling, US

Abigail Dubiniecki
Independent privacy lawyer and consultant, Canada

Gabriela Kennedy and Joshua T. K. Woo
Mayer Brown, Hong Kong

Nada Ihab
Access Partnership, UK

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

The many faces of AI

Recently, Italy's Data Protection Authority imposed a fine of €20 million on Clearview, and banned any further processing of citizens' facial biometrics (p.11).

Clearview has also been the target of regulatory action in the UK, France, Australia and Canada. The UK ICO conducted a thorough investigation into Clearview's processing of personal data in cooperation with the Office of the Australian Information Commissioner culminating in ordering the company to stop processing data. In France, the DPA has taken similar action.

Although the company has been heavily criticised for not having an adequate legal basis for its processing, now in Ukraine this facial recognition technology has been used to identify Russian soldiers that have died in Ukraine. While the power of AI can be advantageous in reuniting refugee families or identifying the dead, what happens if the database falls into the wrong hands?

I would be interested in hearing how your company is reacting to the war in terms of data transfers to and from Russia, and processing operations in both countries. Please let me know if you can share your experience with *PL&B* readers.

There is now positive news regarding the EU-US data transfer situation – the parties have announced that they have agreed, in principle, a new framework (p.31). The teams of the US Government and the European Commission will now continue their cooperation with a view to translate this outline arrangement into legal documents that will need to be adopted on both sides to put in place this new Trans-Atlantic Data Privacy Framework. For that purpose, these US commitments will be included in an Executive Order that will form the basis of the Commission's assessment in its future adequacy decision, the EU says. Both sides want to avoid a *Schrems III* banning judgement from the Court of Justice of the European Union.

This is welcome progress as it is expected that the final agreement will be ready this Spring. In the meantime, another three US states, Colorado (p.13),Virginia and Utah (p.15) have adopted data privacy laws (the California Consumer Privacy Act was adopted in 2018).

Internationally, Professor Graham Greenleaf reports (p.1) on 12 new data privacy laws in 2021/22, including the more recent ones in Oman, Sri Lanka and the United Arab Emirates.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 168+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 168+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection and related laws.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

> *PL&B International Report* is a very useful and business-friendly publication that allows our team to easily and frequently keep up with developments in countries outside our jurisdictions of activity.
>
> **Magda Cocco and Inês Antas de Barros, Partners and Isabel Ornelas, Managing Associate, Information, Communication & Technology Practice, Vieira de Almeida, Lisbon**

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of data protection legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business strategy.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.