The Computer & Internet Lawyer

Volume 40 ▲ Number 2 ▲ February 2023

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Danish Data Protection Authority Joins Pan-European Approach to Google Analytics

By Matthew R. Baker and Nick Palmieri

The Danish Data Protection Authority (DPA), Datatilsynet, has determined that the use of Google Analytics is violative of the European General Data Protection Regulation (GDPR) because it enables companies to move individual's personal information outside of the European Union (EU) without appropriate safeguards and protections.

This decision follows similar recent decisions by the Austrian, French, and Italian DPAs, which likewise found that the use of Google Analytics generally violated the GDPR.

Google did implement various modifications to the tool as a result of the Austrian decision in January 2022 but Datatilsynet found the modifications were insufficient.

Datatilsynet did not issue a fine, but the decision, coupled with the others, will require organizations to review their use of Google Analytics and consider "supplementary measures" to ensure lawful use of this tool in their operations.

Matthew R. Baker, a partner in the San Francisco office of Baker Botts L.L.P., focuses his cross-disciplinary practice on data privacy, cybersecurity, crisis management, and incident response for a broad range of industries. **Nick Palmieri** is an associate in the firm's Intellectual Property Practice in New York. The authors may be contacted at matthew.baker@bakerbotts.com and nick.palmieri@bakerbotts.com, respectively.

PAN-EUROPEAN APPROACH

The Google Analytics tool has recently come under fire among the EU Member States. While each DPA conducted their own investigation, Datatilsynet noted what it called a "pan-European position" among Austria, France, Italy, and Denmark. This approach demonstrates the increasing coordination and communication between the (nominally) independent DPAs of different EU Member States, which offers more consistency in the application of the GDPR.

CONSIDERATIONS FOR THE USE OF GOOGLE ANALYTICS

Datatilsynet decision, coupled with the previous decisions, creates doubt as to whether (and how) companies may continue using Google Analytics in their operations. While the DDPA concluded that the tool's general use violated the GDPR, it said companies may be able to use [Google Analytics] with added "supplementary measures," including pseudonymization.

Further, Datatilsynet also points to the French DPA's guidance on the subject. In this guidance, the French DPA indicates that the use of Standard Contractual Clauses is insufficient on its own to bring Google Analytics into GDPR compliance. According to the French DPA, "only solutions allowing to break [the] contact between the terminal and the server" can reconcile the use of Google Analytics with the GDPR. As such, one proposed solution – suggested by the French DPA – is to use a proxy with certain criteria, including:

- The IP address should only be on the proxy server, and should not be transferred to the servers of the analytics tool;
- Pseudonymization should be implemented on the proxy server (consistent with Datatilsynet's recommendation);
- External referrer information should be removed;
- Parameters contained with collected URLs should be removed;
- Information that may be used to generate a fingerprint should be reprocessed;
- No cross-site or lasting identifiers should be collected; and
- Any data that may lead to re-identification should be deleted.

Both of these proposed solutions provide guidance to companies eager to continue using Google Analytics in the EU, but the adoption of either will depend upon the specific use cases.

CONCLUSION

These decisions require companies using Google Analytics in the EU to re-evaluate and potentially modify their processes.

However, it is important to note that the DPAs in these four countries have not completely prohibited the use of Google Analytics. Rather, they have suggested the use of additional supplemental protection measures, specifically pseudonymization, to ensure the protection of EU citizens' data.

As a result, companies should consider whether they need supplemental protection measures to operate in the EU or to transfer data outside of the EU to a third country.