Published on *The National Law Review* https://natlawreview.com

Austrian DPA Finds Data Transfers Resulting from Analytics Cookie Use to Be in Violation of GDPR Data Transfer Requirements

Article By:

Hunton Andrews Kurth's Privacy and Cybersecurity

The Austrian data protection authority (the "Austrian DPA") recently published a decision in a case brought against an Austrian website provider and Google by the non-governmental organization co-founded by privacy activist Max Schrems, None of Your Business ("NOYB"). The Austrian DPA ruled that the use of Google Analytics cookies by the website operator violates both Chapter V of the EU General Data Protection Regulation ("GDPR"), which establishes rules on international data transfers, and the *Schrems II* judgment of the Court of Justice of the European Union.

The ruling could have far-reaching implications in other EU Member States and result in a ban of Google Analytics across the EU.

Background

On August 17, 2020, NOYB filed 101 identical complaints before 30 European Economic Area ("EEA") data protection authorities regarding the use of Google Analytics and Facebook Connect by various companies. The complaints related to the question of whether transfers of EU personal data to Google and Facebook in the U.S. resulting from the use of cookies are still permitted after the *Schrems II* judgment. The European Data Protection Board ("EDPB") subsequently created a taskforce to coordinate the response to the complaints filed by NOYB.

The Austrian DPA's decision is the first one issued with respect to the 101 complaints filed by NOYB.

Austrian DPA's Decision

In its decision, the Austrian DPA concluded that the use of Google Analytics cookies by an Austrian website involved the collection and subsequent transfer of personal data to Google in the U.S., including unique user identification numbers, IP addresses and browser parameters.

The Austrian DPA found that the Standard Contractual Clauses ("SCCs") entered into between the website operator and Google did not provide an adequate level of protection under the GDPR, as: (1) Google qualifies as an electronic communications service provider and is therefore subject to

surveillance by U.S. intelligence agencies under U.S. surveillance law (i.e., FISA 702); and (2) Google's additional safeguard measures were not effective in closing the legal protection gaps identified in the *Schrems II* judgment. Key takeaways from the Austrian DPA's decision include the following:

- The Austrian DPA found that the technical measures implemented by Google, in addition to the SCCs, are not effective because they do not eliminate the possibility of surveillance of, and access to, personal data by U.S. intelligence agencies. According to the Austrian DPA, encryption of data at rest is not sufficient to prevent access to personal data by government authorities, as long as Google has the possibility to access the data in plain text. In addition, the Austrian DPA highlighted that the organizational and contractual measures implemented by Google (including an obligation to (i) notify data subjects about government access requests, (ii) publish transparency reports, (iii) maintain a policy on the handling of government authority requests, and (iv) carefully assess each government authority request) are generally insufficient and ineffective to ensure an adequate level of protection for personal data transferred to the U.S.

- The Austrian DPA rejected the argument that the personal data collected through cookies and subsequently transferred to the U.S. did not relate to or directly identify specific individuals. The Austrian DPA found that IP addresses and online identifiers qualify as personal data because they allow for individuals to be identified. According to the Austrian DPA, actual and immediate identification is not necessary for data to be considered identifiable. According to the Austrian DPA, the fact that information enabling identification of an individual is held by various stakeholders, as opposed to one party, is also irrelevant to whether the data is identifiable.

- The Austrian DPA also rejected the argument that Chapter V of the GDPR and the SCCs follow a risk-based approach and that, in this case, the risk to data subjects was low, as the likelihood of U.S. government access to the relevant data was low.

- The Austrian DPA did, however, argue that the rules of Chapter V of the GDPR on data transfers apply only to EU exporting entities, and not to U.S. importers. This is in line with recent EDPB guidelines on what constitutes an international transfer under the GDPR. The Austrian DPA therefore found that the violation was attributable to the website operator, and not to Google.

The Austrian DPA concluded that because no other data transfer mechanism available under Chapter V of the GDPR could be used by the website operator to transfer personal data to Google in the U.S., there was not an adequate level of protection for personal data collected through Google Analytics cookies and transferred to Google in the U.S., constituting a violation of Article 44 of the GDPR.

In addition, recently, the Dutch DPA published an update to its guide on how to configure Google Analytics cookies. In the update, the Dutch DPA refers to the December 2021 decision by the Austrian DPA, and indicates that the Dutch DPA currently is investigating two similar complaints about the use of Google Analytics in the Netherlands. The Dutch DPA states that these investigations, which are expected to be completed in early 2022, will help to determine whether the use of Google Analytics is permitted in the Netherlands.

Read the Austrian DPA decision (in German).

National Law Review, Volumess XII, Number 24