CLIENT ALERTS & INSIGHTS

Google Analytics Ruled Unlawful by Austrian Data Protection Authority Under the GDPR and Schrems II Decision

FEBRUARY 3, 2022

Authors: Ryan T. Sulkin

More, possibly similar decisions are expected in the coming months, throwing cross-Atlantic data transfers and trade into doubt as diplomats seek a Privacy Shield replacement.

In late December, the Austrian Data Protection Authority ("**DPA**") ruled that a local Austrian website's use of Google Analytics-specifically, the sharing of personal data with the U.S.-based provider-violated the privacy protections set forth in the General Data Protection Regulation ("**GDPR**") as clarified in the *Schrems II* decision.

In order to transfer data from a location within the E.U. to a location outside of the E.U., an entity must either (1) be sending the personal data to a country that the E.U. Commission has determined provides "adequate" safeguards equivalent to those in the E.U.; or (2) making the transfer subject to appropriate safeguards. Those safeguards can take the form of the Standard Contractual Clauses ("**SCCs**"), binding corporate rules, or additional contractual safeguards.

Prior to July 2020, data transfers between the U.S. and E.U. were subject to Privacy Shield, which was set up between the U.S. and E.U. to ensure that the U.S. provided adequate safeguards for data transfers. Numerous entities utilized Privacy Shield in order to properly transfer personal data from locations within E.U., to locations in the U.S. without running afoul of the GDPR or E.U. DPAs. However, Privacy Shield was rejected by the E.U. courts in 2020.

Diplomats from both the E.U. and U.S. have been working on a new agreement meant to both assure that individual privacy rights and freedoms of Europeans are upheld, and to allow the free flow of the technology trade (and with it, personal data) to continue between the E.U. and the U.S.

The ruling from the Austrian DPA highlights the need for a new cross-Atlantic privacy framework as one of the largest analytics and advertising-tech tools has been ruled unlawful. Google Analytics, and other U.S.-based technology service providers might see similar rulings in the future as similar complaints have been filed with multiple DPAs across the E.U.

EU-US Data Flow Background

In *Schrems II*, the Court of Justice of the European Union famously struck down the E.U. - U.S. Privacy Shield. The main concern and issue raised by the court was that U.S. law (and Privacy Shield) did not grant sufficient protection to an individual's privacy as compared to the GDPR. Specifically, the court was most concerned with unauthorized federal government access to personal data under the Foreign Intelligence Surveillance Act ("**FISA**

"), and the lack of measures in place for European citizens to challenge such access or government requests.

The Court also called into question the validity of the old **SCCs**. The SCCs are a contractual tool that entities use to ensure that personal data shared over the course of a cross-border contractual relationship is properly protected and the rights guaranteed to European individuals are upheld.

While cumbersome, the SCCs have become a common mainstay in technology transactions that involve data transfer from the European Economic Area ("**EEA**") to other geographical locations. To address the concerns the Court raised in *Schrems II*, the European Commission adopted the new SCCs, which have been in place since this past summer and required since this past fall.

Google Analytics

It is important to note that this particular ruling has no bearing on the validity of the new SCCs because the clickthrough agreements and contractual language used when an entity employs Google Analytics do not include the SCCs.

Google Analytics, like many other advertising or analytics providers, uses cookies to track users and aggregate statistics that are useful to build out marketing strategies. Such tools are subject to GDPR, and similar privacy laws, because cookies generally gall within the definition of personal data. When an individual goes to a website using Google Analytics, or similar tools, a cookie (small piece of code) is placed on their device. The cookie then assigns an individualized, random identification to the individual and device. It can track the number of times the individual comes to a website, how they interact with the website, and be used to aggregate information about how that individual interacts with other websites.

While on the surface such technology seems anonymous and de-identified, as the cookie assigns a random number or identifier to the individual, privacy laws like the GDPR broadly define personal data to include anything that ***could*** relate to an individual, not just data that readily does identify an individual.

Here, while the cookie does not readily identify an individual, it falls within the definition of personal data because it could be combined with other information to identify the individual (as the random identification is linked to the individual and their devices). Cookies are also not sufficiently de-identified to the point that it is ***ensured*** they could not be used to identify an individual or that such identification is impossible.

Therefore, Google Analytics' use of cookies falls squarely within the scope of the GDPR and requires adherence to the *Schrems II* decision requiring extra steps and protections to ensure proper protection of E.U. personal data when it is transferred to and resides in the U.S.

Moving Forward

The Austrian DPA found that Google Analytics was not offering an adequate level of protection. Specifically, the personal data that was transferred was not protected from potential U.S. government surveillance under FISA.

Google Analytics claimed that their supplementary measures in place (including transparency reports on government access and encryption of data) were adequate. The Austrian DPA squarely

rejected that claim, highlighting that an individual in the E.U. still had no path or reasonable possibility to challenge or reject such government access.

Unless there is a breakthrough on a new cross-Atlantic privacy framework, entities will need to rely on stronger security and privacy contractual measures in the new SCCs or risk scrutiny and fines from the various DPAs across the E.U. Currently the negotiations are in their second year. While a breakthrough is always possible, there is no guarantee a deal will be brokered anytime soon.

Without such a deal or reliance on the SCCs, entities will face case-by-case analysis and decisions by the DPAs on whether a given U.S.-based service provider has provided enough supplementary protection measures in order to afford adequate protection. Examples of possible supplementary measures include end-to-end encryption, pseudonymization, and any measure that appropriate protects personal data from unauthorized access or use.

If no cross-Atlantic privacy framework is reached and DPAs continue to rule that the use of U.S.-based service providers is unlawful, some European entities may move towards E.U.-based service providers, and move away from service providers like Google as E.U. privacy law moves closer to requiring data localization.

As European authorities clarify the aftermath of *Shrems* II and the trans-Atlantic relationship between the U.S. and E.U. evolves, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Ryan T. Sulkin at rsulkin@beneschlaw.com or 312.624.6398.

Lucas Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.