

An Uncertain Future for EU-US Data Transfers

Gary Kibel, *Partner*, gkibel@dglaw.com

Oriyan Gitig, *Counsel*, ogitig@dglaw.com

Zachary N. Klein, *Associate*, zklein@dglaw.com

In the wake of the Court of Justice of the European Union's invalidation of the EU-US Privacy Shield Framework (Privacy Shield), which was established to allow for the transfer of personal data from the EU to the United States in compliance with the EU's General Data Protection Regulation (GDPR), businesses are forced to consider other mechanisms to legally execute such cross-border data transfers.

EU Privacy Law

The EU requires that, in the absence of an "adequacy decision" by the European Commission (Commission), transfers of personal data of EU data subjects from the EU to jurisdictions outside the EU are permitted only if appropriate safeguards are in place. The EU found that the United States did not fulfill that condition, based, in part, on the United States' lack of a comprehensive federal privacy law. And so, in the hope of creating a reliable legal mechanism that would allow for the authorized transfer of personal data from the EU to the United States, the parties negotiated and established the Privacy Shield.

In its pivotal July 2020 *Schrems II* decision, however, the Court of Justice of the European Union (the Court) invalidated the EU-US Privacy Shield, holding that the Privacy Shield failed to meet the necessary conditions under the GDPR, highlighting U.S. surveillance activities as a violation of the EU Charter of Fundamental Rights. As a result, businesses are required to consider legal mechanisms other than the Privacy Shield to legally execute cross-border data transfers.

EU Standard Contractual Clauses

The most widely-accepted method of attempting to satisfy EU cross-border data transfer law has been the use of EU Standard Contractual Clauses (SCCs) — contracts pre-approved by the Commission that establish certain controls to safeguard data as per the GDPR. The *Schrems II* decision upheld SCCs as a valid transfer mechanism in the aftermath of Privacy Shield. In June 2021, the Commission issued updated SCCs, in part, to satisfy the *Schrems II* ruling.

The new SCCs require the data exporter and importer to warrant that they have no reason to believe that the laws and practices in the recipient country prevent the data importer from fulfilling

its obligations under the SCCs. The revised SCCs also require a data importer to notify the data exporter (and, where possible, the data subject) if it "[r]eceives a legally binding request from a public authority" or "[b]ecomes aware of any direct access by public authorities to personal data transferred." The revised SCCs are already required for new contracts and processing operations as of September 2021, and the Commission has stated that all existing contracts and data transfer agreements must be retrofitted with the new SCCs by December 22, 2022.

For now, the revised SCCs appear to offer a reliable, legal basis for data transfers in the wake of *Schrems II*. However, a recent decision by the Austrian Data Protection Authority (Austrian DPA) threatens to upend the state of EU-US data transfers yet again, as the legality of the new SCCs comes under question. In its [Google Analytics](#) decision, the Austrian DPA found that the updated SCCs used by a website operator and Google did not provide an adequate level of protection under the GDPR because the SCCs still subject Google to U.S. intelligence surveillance laws and did not enable Google's additional safeguards to eliminate the possibility of surveillance by U.S. intelligence agencies. These safeguards included obligations to: (1) notify data subjects about government access requests; (2) issue transparency reports; (3) implement a policy on handling government requests; and (4) carefully evaluate any such request.

The Austrian DPA's decision is the first of 101 similar complaints filed by the non-government organization "None of Your Business." It remains to be seen whether other European regulators and courts will echo the reasoning of the Austrian DPA. However, with additional scrutiny over the new SCCs, businesses hoping for some consistency in the area of EU-US data transfers may be disappointed.

What Businesses Can Do Now

- Business should already be using the new SCCs, and preparing to amend older contracts with the new form.
- A close eye should be kept on the developments in the EU which could significantly impact cross-border data transfers.