D&G | Davis & Gilbert LLP
ATTORNEYS AT LAW

NOVEMBER 2020

DIGITAL MEDIA, TECHNOLOGY & PRIVACY

>> ALERT

EU-U.S. DATA TRANSFERS POST SCHREMS II

In July, the EU-US Privacy Shield was invalidated by the Court of Justice of the European Union (the Court) (see our prior alert).

While the Court upheld the Standard Contractual Clauses (SCC's) as a sufficient transfer mechanism, it indicated that supplementary measures, to address inadequate privacy protections of some foreign jurisdictions, might be necessary, requiring a case-by-case assessment.

Since that time, the U.S. Department of Commerce has spoken out about the legal basis for cross-border data transfers, the European Data Protection Board (the EDPB) has provided guidance on supplementary measures and now the SCC's have been updated by the European Commission (the Commission), and remain subject to a public comment period through December 10th, 2020.

THE BOTTOM LINE

The Schrems II decision inserted a great deal of uncertainty into data transfers from the EU to the United States. Regulators on both sides of the Atlantic continue to provide guidance, but have not completed negotiations on a new process. Businesses must remain as vigilant and organized as ever in continuously assessing, implementing and monitoring data transfer frameworks and safeguards.

U.S. DEPARTMENT OF COMMERCE — WHITEPAPER

The U.S. Department of Commerce issued a whitepaper in September 2020 which essentially rebutted many of the complaints about the U.S. privacy ecosystem from the Schrems II case. Most telling, they stated:

>> *"[m]ost U.S. companies do not deal in data that is of any interest to U.S. intelligence agencies, and have no grounds to believe they do. They are not engaged in data transfers that present the type of risks to privacy that appear to have concerned the ECJ in Schrems II…"*

>> *"Sharing of FISA 702 information undoubtedly serves important EU public interests by protecting the governments and people of the Member States."*

Despite these statements, EU regulators were not persuaded.

EUROPEAN DATA PROTECTION BOARD — GUIDANCE

The European Data Protection Board (the EDPB) has published its recommendation regarding data transfers, as well as promulgated recommendations regarding the upholding of the *EU Essential Guarantees* (Essential Guarantees), in order to assess whether the legal framework supporting a foreign government's access to data for surveillance purposes is justifiable and proportionate as regards to the rights of data subjects.

The new EDPB-recommended measures require an assessment of the *who*, *what* and *where* in order to manage the security of cross-border transfers of information adequately and sufficiently. Execution of the SCC's by the parties to a data transaction are only one piece of the evaluation, according to the latest from the EDPB.

EDPB RECOMMENDATIONS

The EDPB provided a six-step analysis to assess the sufficiency of security related to cross-border data transactions:

1) Identify Data Transfers

2) Identify Transfer Mechanism

3) Assess the Law of the Third Country

4) Adopt Supplementary Measures

>> continues on next page

5) Formal Procedural Steps

6) Monitor and Evaluate Applicable Data Laws

One component of this assessment, and relevant to the upholding of the Essential Guarantees, is to review whether authorities in the applicable jurisdiction may access data in ways that are contrary to the Essential Guarantees. Since the Court specifically asserted previously that surveillance by the United States government creates vulnerabilities for data subjects, businesses should assume that data transfers from the EU to the U.S. will require additional protections.

As mentioned above, the U.S. Department of Commerce has stated that most data transferred between businesses is of little interest to the government, and thus, there is a low risk of surveillance. Accordingly, the U.S. government's position is that U.S. surveillance laws do not pose a risk to the rights of EU data subjects. However, while transfers in response to the Federal Intelligence Surveillance Act (FISA) orders may arguably be supported under the GDPR's public interest principles and, accordingly, approved by the EDPB, unofficial transfers from the EU to the U.S. outside of any such orders are still likely to be subject to a higher level of scrutiny by the EDPB. Business should, accordingly, assume that additional security measures are necessary.

For more information on these steps, visit here.

REVISED SCC'S

Proposed changes to the SCC's include enhanced data subject protections, including easier enforcement of the agreement against all parties. Data Exporters will be required to document and retain impact assessments. Data Importers will have to notify data exporters and data subjects of surveillance requests, where permissible.

Additionally, whereas the prior SCC's contemplated only one transfer scenario of an EU-based controller to a non-EU-based controller or processor, the updated SCC's will contemplate various additional models, providing for more flexibility which is crucial as the framework underlying data transfers continues to grow more complex with the advent of more sophisticated technological tools.

The updated SCC's also contemplate and provide for transfers by EU-based Processors to Controllers or Processors outside of the EU.

FOR MORE INFORMATION

Gary A. Kibel
Partner
212.468.4918
gkibel@dglaw.com

Oriyan Gitig
Counsel
212.468.4880
ogitig@dglaw.com

or the D&G attorney with whom you have regular contact.

Davis & Gilbert LLP
212.468.4800
1740 Broadway, New York, NY 10019
www.dglaw.com