Technology & Sourcing Alert
September 2020

60 Seconds on Sourcing: Cross-Border Data Transfer Cleanup After *Schrems II*

The European Union's General Data Protection Regulation (GDPR) strictly regulates the privacy and security of personal data, including the transfer of personal data outside of the European Economic Area (EEA). Previously, companies doing business in the EU and U.S. were able to rely on the EU-U.S. Privacy Shield framework as a mechanism to comply with GDPR data transfer requirements when exporting personal data from the EU to the U.S. However, in its recent decision in the Schrems II case, the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. Privacy Shield framework, leaving companies scrambling to evaluate their data transfer mechanisms to ensure they maintain compliance with the GDPR. While the EU-U.S. Privacy Shield framework is now invalid, the CJEU upheld the Standard Contractual Clauses (SCCs) as a data transfer mechanism, but with certain qualifications, which will now require companies to revisit their approach to the SCCs. (Read our alert on the *Schrems II* decision here.)

Key Takeaways

- Companies transferring data from the EU should reevaluate the data transfer mechanisms they rely upon for transferring personal data to the U.S. In particular, EU-based customers need to reconsider their controller-processor relationships to determine which of their data processors, if any, have been relying solely on the Privacy Shield for data transfers from the EU to the U.S. If any processors were relying solely on the Privacy Shield, the SCCs should be put in place.
- Even when the SCCs are already in place, companies should work with their data processors to reassess the data at issue, the processor's data security protocols, and the data protection laws of the data importer to ensure that the laws protect personal data at a level that is "essentially equivalent" to the protections afforded in the EU.
- Given the many uncertainties left by the CJEU's decision regarding use of the SCCs as a tool for complying with the GDPR's cross-border data transfer requirements, companies should carefully review current and updated guidance provided by the European Data Protection Board and local data protection authorities to help inform their decisions regarding compliance with the GDPR and the relative levels of risk involved when exporting personal data from the EU.

Reexamining Cross-Border Transfers

The first step for companies that export personal data from the EU to the U.S. is to inventory all applicable agreements that contemplated cross-border personal data transfers from the EU to the U.S. and identify which agreements relied solely on the Privacy Shield framework for such transfers (and therefore need to be amended to put the SCCs in place), and which agreements already have the SCCs in place.

The exercise does not end there, however. Although the SCCs were upheld generally as a valid tool to protect data

Attorney Advertising

being transferred outside of the EEA, the CJEU noted that companies should review their SCCs on a case-by-case basis to verify whether additional safeguards may be required in order to provide adequate protection for EU personal data, or otherwise suspend transfers of this information.

A key concern of the CJEU when invalidating the Privacy Shield framework was around certain aspects of U.S. domestic law and the inability of the framework to protect EU personal data from U.S. government access and the fact that U.S. laws do not grant data subjects actionable rights before the courts against the U.S. authorities. The court found that U.S. law (i.e., Section 702 FISA and EO 12333) does not ensure an essentially equivalent level of protection for EU personal data. Whether or not companies can transfer personal data on the basis of SCCs will depend on the result of their assessment, taking into account the circumstances of the transfers, and supplementary measures they could put in place. Companies can start by asking processors about their practices and history concerning disclosures to U.S. government authorities, including evaluating whether the data involved is at risk of disclosure. It will be important to understand the processor's policies and practices with respect to responses to government inquiries. Based on this assessment, companies may need to change the type of data being transferred from the EU to the U.S. and/or amend their existing SCCs to address additional technological controls and protections over personal data. Companies and processors both should engage in similar evaluations of subprocessors that may be used to process EU personal data.

The European Data Protection Board has published a Frequently Asked Questions document to provide some initial guidance on the CJEU's judgment, and is continuing to analyze what supplementary measures may provide the sufficient level of guarantees under the GDPR in addition to existing SCC provisions. Companies should continue to monitor developments in this regard to ensure continued compliance for EU-U.S. data transfers.

Related Professionals

Alison Pollock Schwartz . . . . . aschwartz@loeb.com
Monique N. Bhargava. . . . . nbhargava@loeb.com
Ieuan Jolly . . . . . ijolly@loeb.com

6334 REV1 09-15-2020