European Commission Publishes GDPR Decisions that Clarify SCC Issues and Data Transfers From the EU to the U.S.

Related Professionals

Marcel C. Duhamel

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 6.7.2021

On June 4, 2021, the European Commission published a pair of decisions that provided much-needed guidance regarding standard contractual clauses (SCCs) and data transfer from the EU to the U.S. After the *Schrems II* decision, the usefulness of SCCs was very much in doubt, because that decision's rationale for invalidating Privacy Shield—that the Privacy Shield mechanism could not provide adequate protection against access to data by U.S. intelligence services—applied equally to SCCs. The European decisions provide at least a possible means to continue to transfer some forms of data from the EU to the U.S.

Background

The GDPR generally prohibits the transfer of personal data from the EU to countries that have not been deemed to provide adequate levels of data protection. The United States is one such country. GDPR has several "derogations," or exceptions, one of which was the use of an approved certification mechanism that would permit the data importer to receive EU data. In the U.S., Privacy Shield was that certification mechanism, and many U.S. companies relied on Privacy Shield to allow them to receive data from the EU.

In July 2020, the CJEU invalidated Privacy Shield. The primary basis for the decision was that Privacy Shield did not provide an equivalent level of protection to personal data as that data would enjoy in the EU, because there is no avenue for judicial redress in the event a U.S. intelligence service were to access that data. Although the decision did not invalidate SCCs, its rationale would seem to apply to them equally. After all, there is no way an exporter and importer can agree that, if a US intelligence service executes a warrant under the Foreign Intelligence Surveillance Act and accesses an EU resident's personal data in the possession of a US importer, that EU data subject can obtain judicial review. This appeared to be a potential death-knell for EU-US data transfers.

Summary of Decisions

The first of the June 4 commission decisions expands the use of standard contractual clauses to cover processor to controller data transfers. Additionally, processors can now seek sub-processing relationships and utilize a standard contractual clause. This is additional to the controller to controller, and controller to processor situations that may already use a SCC. Entities will now have more SCC selections to ensure compliant data transfers.

The second of the June 4 commission decisions smooths some of the fractures caused by the *Schrems II* decision. The decision now clarifies that use of SCCs to transfer data to the U.S. is not *per se* impermissible merely because of the existence of national security statutes that could lead to access of personal data.

Instead, parties to a SCC can now assess their practical experiences with such laws. Parties to a SCC must review and assess whether laws existing in the importer's country will actually interfere with its obligations under the SCC. This review can include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This diligence review must be thorough, and it must be documented, but in theory it raises at least the possibility that an EU exporter and a U.S. importer can enter SCCs that will permit data transfers even after *Schrems II*.

To be sure, the SCCs themselves impose significant burdens on the importer. Importers are expected to notify the data exporter ***and data subjects*** when they receive a disclosure request; whether this notice is permissible under U.S. law will be, in some cases, a difficult question. Further, importers are compelled to review the legality of the requests. If the party determines the request is unlawful, the importer should exhaust all options to challenge the request. This places the onerous burden on third-country data importers to protect the personal data and advocate for the privacy rights of the data subjects.

Conclusion

These decisions offer some hope for U.S.-based companies hoping to receive data from EU exporters.

Whether they apply to transfer of all forms of data—whether they apply to the transfer of human resource data, for example—may be an open question, as is whether companies will actually be able to provide the requisite level of assurance that access by U.S. intelligence services is, as a practical matter, unlikely. Still, companies facing these issues now have an arrow in a quiver that otherwise seemed to have been emptied entirely by *Schrems II*.

If you have questions about these commission decisions or GDPR generally, please contact Marcel Duhamel, Eva Cuollo or your Vorys attorney.