

Publication

06/28/2021

Client Alert: EU Adopts New Standards for International Data Transfers

On June 4, 2021, the European Commission ("EC") published its final Implementing Decision adopting new Standard Contractual Clauses ("SCCs") for the transfer of personal data outside the European Economic Area ("EEA"). Businesses and organizations that collect, process, or otherwise handle any EEA personal data (i.e., anything that can be used to directly or indirectly identify a natural person) will need to take steps to ensure that their data transfers are in compliance with the new SCCs and their related requirements. The revisions come into effect on June 27, 2021, but for those currently in compliance, this deadline may extend to December 27, 2022.

SCCs provide a legal basis under the General Data Protection Regulation ("GDPR") to allow the transfer of personal data of individuals in the EEA to countries outside of the EEA that have not been deemed to have an adequate level of data protection. Because the EC has not deemed the United States to have an adequate level of data protection, and because the Court of Justice of the European Union ("CJEU") recently invalidated EU-U.S. Privacy Shield as a self-certification transfer mechanism, the new SCCs will become a critically important personal data transfer mechanism for European and United States businesses and organizations.

CLIENT SERVICES

Intellectual Property
Commercial & Technology Transactions
Cybersecurity & Data Privacy

RELATED PEOPLE

Alfred C. Tam
David A. Wheeler

To comply with this regulation, businesses and organizations who collect, process, or otherwise handle any EEA personal data should:

1. Start mapping known EEA personal data transfers to the U.S. and perform risk assessments based on data types and categories, as well as U.S. data protection laws;
2. Start identifying all data transfers reliant on the original SCCs;
3. Review contract provisions as targets for updating and assess whether contract amendments are required to implement supplementary measures; and
4. Start using the new SCCs and otherwise make relevant agreement updates over the next 18 months or when agreements come up for renewal or renegotiation.

The EC adopted the new SCCs for several reasons. First, the original SCCs were written prior to adoption of the GDPR in 2018 and therefore do not fully address all of the GDPR's data protection requirements. Second, the digital economy has seen significant developments and more complex processing operations involving multiple data importers and exporters, complex processing chains, and evolving business relationships, all of which have resulted in the need for general modernization of the SCCs. Third, and perhaps most significantly, the CJEU issued its *Schrems II* decision on July 16, 2020, which declared as invalid the EU-U.S. Privacy Shield personal data transfer mechanism for data transfers between the U.S. and the EEA. As part of the *Schrems II* decision, the CJEU also called into question the reliability of the original SCCs as a data transfer mechanism unless transfer impact assessments were conducted and "supplementary measures" implemented.



As a result, the new SCCs include substantial updates over the original SCCs. Among the changes, the new SCCs now include:

- modular frameworks to provide increased flexibility for a variety of data transfers among controllers and processors;
- a “docking” clause to permit new parties to be added to previously executed SCCs;
- a significant focus on the compatibility of laws of the data importing country, which requires the parties to assess, on a case-by-case basis, whether the laws of the data importing country, without supplementary measures, will compromise data protections afforded under the SCCs;
- a supplementary requirement that the data importer additionally notify the data exporter of data access requests received from public authorities, assess the legal validity of such requests, and pursue legal remedies against such requests; and
- new obligations with respect to onward data transfers, sub-processors, and cybersecurity.

While the new SCCs come into effect on June 27, 2021, the EC has built in two grace periods whereby (i) the original SCCs can still be executed until September 27, 2021, and (ii) original SCCs that were executed prior to the September 27, 2021 date can still be relied upon as a valid data transfer mechanism until December 27, 2022. After December 27, 2022, the new SCCs must replace the original SCCs as a valid data transfer mechanism.

The NGE Cybersecurity and Data Privacy team stands ready to assist with any and all aspects of compliance relating to the new SCCs. If you have any questions,



please contact David Wheeler, Alfred Tam or your Neal Gerber Eisenberg attorney.

The content above is based on information current at the time of its publication and may not reflect the most recent developments or guidance. Neal Gerber Eisenberg LLP provides this content for general informational purposes only. It does not constitute legal advice, and does not create an attorney-client relationship. You should seek advice from professional advisers with respect to your particular circumstances.