wiley

NEWSLETTER

Post-*Schrems II*: The European Union Provides Guidance on Data Transfers

December 2020

Privacy in Focus®

In the wake of the *Schrems II* decision (explained here) that upended the transfer of personal data from the European Union (EU) to countries without an adequacy decision, such as the United States, companies have requested guidance from European authorities on compliant methods to transfer data outside of the EU. In November, the European Data Protection Board (EDPB) and the European Commission (EC) delivered, with guidance to assist companies seeking to create compliant data transfer models.

Specifically, on November 10, 2020, the EDPB released its recommendations on supplemental transfer tools to ensure compliance with the EU level of protection of personal data (Recommendations). The next day, on November 11, 2020, the EC released long-awaited proposed updates to Standard Contractual Clauses (SCC). SCCs, in general, create a contractual obligation between parties to safeguard data transferred outside of the EU that is "essentially equivalent" to the protection requirements of the GDPR, and – subject to certain additional considerations – are recognized as a valid data transfer mechanism.

The newly released guidance provides a helpful roadmap for companies; however, it is also clear that in this evolving and complex area, companies will have to carefully evaluate the risk associated with the transfer of certain types of data to some countries.

Below is a high-level review of the Recommendations and the updated SCCs. For a more comprehensive summary or analysis – or to consider how these developments impact your company's cross-

Authors

Joan Stewart
Of Counsel
202.719.7438
jstewart@wiley.law

Practice Areas

GDPR and Global Privacy
Privacy, Cyber & Data Governance

border data transfers – do not hesitate to reach out to a member of our team.

The Recommendations

Schrems II acknowledged that SCCs could be a valid transfer mechanism but expressed concern that the local laws of the importing country could negate the safeguards meant to be provided by SCCs. Specifically, the *Schrems II* court cautioned entities that rely on SCCs to transfer data to these countries that they may need to take "supplemental measures" on a case-by-case basis to ensure the individual data subject's rights are honored. The court did not provide additional guidance on the use of supplemental measures, but rather delegated that task to the EDPB.

The Recommendations, among other things, provide the first concrete insight into what "supplemental measures" businesses should consider. The Recommendations advise that an exporter or importer must determine if the country receiving the data has laws or practices that could compromise the individual rights meant to be protected by the SCCs. Most commonly, this will be laws that allow for government surveillance of certain types of data.

If the receiving country has laws or regulations that may leave an individual's data without protection that is "essentially equivalent" to those provided by the GDPR, the businesses should consider supplementary measures. These measures should be customized for the type of data being transferred and the type of law or regulation that triggered the need for supplemental measures. The Recommendations caution that businesses should consider these measures on a case-by-case basis, not a one-size-fits-all approach.

Recommended supplemental measures include, but are not limited to:

- **Technical measures**, such as encryption, transferring pseudonymized data only, transfer to a protected recipient, and additional contractual measures.
- **Organizational steps**, such as internal policies and standards adopted voluntarily between contracting parties.
- **Internal Policies**, likely best suited to transfer between commonly owned companies, such as procedures to handle government requests for access to data and extensive training of relevant employees.
- **Transparency and Accountability**, such as by committing to document and record the government requests with the company's response and provide this information to the individual whose data was accessed.
- **Adoption of Standards and Best Practices**, such as adopting data security and privacy policy practices that follow EU certification methods or other international standards.

Importantly, the use of any supplemental measure must be evaluated by its effectiveness. For example, if a country prohibits a business from disclosing that it has received a government request for access to data – the transparency and accountability measures outlined above would not be effective. Accordingly, if your company is considering using a supplemental measure, it is important to perform a fact-specific analysis for

effectiveness.

The Updated SCCs

The day after the release of the Recommendations, the EC released its proposed updates to the SCCs. The updated SCCs modify the existing clauses in several important respects. First, the updated SCCs are structured to support a wider range of data transfer relationships. Currently, there are two versions of the SCCs: one for Controller to Controller transfers and another for Controller to Processor transfers. In contrast, the updated SCCs follow a modular format allowing the contracting parties to select the clauses that best apply to the transfer relationship. The four modules are: Controller to Controller, Controller to Processor, Processor to Processor, and Processor to Controller.

Second, the updated SCCs give careful treatment to the issue at the center of the *Schrems II* decision – government access to data. The updated SCCs set out requirements for the data importer in the event local laws impact its ability to comply with the terms of the SCCs. Specifically, the updated SCCs incorporate many of the recommendations of the EDPB, such as to notify the exporter of the legally binding request from the government entity and committing to challenge the request under certain circumstances.

The EC accepted comments to the proposed updates through December 10. For businesses that rely on SCCs, keep a close watch for release of the final updated SCCs as this will trigger a one-year deadline to amend contracts that currently include the older version to the new and improved version of the clauses.

For businesses that transfer data from the EU to the United States (or other countries without adequacy decisions), the Recommendations and updated SCCs will be crucial to creating a compliant transfer protocol. Businesses should carefully consider what data they are exporting from the EU and which laws could compromise the "essentially equivalent" protection of that data in the importing country, and look to the Recommendations for guidance on what supplemental measures are appropriate on a case-by-case basis to transfer data consistent with the terms of the updated SCCs.

Our team has helped entities of all sizes from various sectors parse through complicated GDPR issues – from determining whether the GDPR applies to developing compliance programs. If your organization has questions about the GDPR or the potential impact of this regulation on your business, do not hesitate to reach out.