PUBLICATION

New Compliance Obligations for Cross-Border Data Transfers

Authors: Vivien F. Peaden
September 27, 2021

For several years, cross-border data transfers functioned similar to airport security checks for international travel, with the Privacy Shield operating as a fast check-in lane. After the European Union (EU) Court invalidated the Privacy Shield in July 2020 (*Schrems II* decision), EU-U.S. data transfers faced greater uncertainties. While other mechanisms existed, Privacy Shield was a common compliance tool. Given the inability to utilize the Privacy Shield concept, the EU introduced an update to an alternative mechanism, new standard contractual clauses (New SCC), which replace the 2010 version and facilitate post-*Schrems II* cross-border data transfers. Beginning September 27, 2021, most organizations will need to amend their commercial agreements with the New SCC for transatlantic data transfer. These new processes will add significant compliance obligations for customers and vendors to assess, document, and implement to ensure additional safeguards for protecting EU personal data.

Why the EU Invalidated the Privacy Shield

Before July 2020, more than 5,000 companies transferred EU personal data to the U.S. through the Privacy Shield framework approved by the U.S. and the EU. For 15 months following the *Schrems II* decision, companies have been struggling with this "Suez Canal moment" that places severe hurdles for transatlantic data transfer. Similar to the Evergreen container ship's accidental blockage of the Suez Canal in 2021, the impasse in cross-border data transfer jeopardizes EU-U.S. trade at an estimated $1 trillion per year.

The EU-U.S. friction over cross-border data transfer arises because of their differing approaches in privacy and data protection: while the U.S. considers data privacy important, the EU sees it as inalienable and sacred. Edward Snowden's revelation about U.S. surveillance programs further demonstrated that the U.S. federal government can compel companies such as Facebook to turn over EU residents' data. In response, the EU court found that U.S. laws undermine the protections of the General Data Protection Regulation (GDPR). The court noted in its opinion that U.S. national security laws do not afford individuals sufficient rights when their personal data is intercepted by U.S. intelligence agencies.

Options for Cross-Border Data Transfers

U.S. organizations must undergo a thorough case-by-case assessment of cross-border data transfers, known as a transfer impact assessment (TIA). Other options are binding corporate rules (BCR), however these are generally not favored by most organizations.

When to Amend Existing Agreements with the New SCC

For contracts signed before September 27, 2021 under the old SCC, companies have until December 27, 2022 to amend with the New SCC. The New SCC comes in one document with four separate cross-border transfer scenarios or modules:

1. Controller to controller,
2. Controller to processor,
3. Processor to processor, and
4. Processor to controller.

A business must select the applicable module before initiating the transfer based on the executed New SCC. A key step for the TIA outlined below is that the business must also adopt supplementary measures, in addition to the New SCC, to provide GDPR-equivalent data protection to EU residents.

The Six Steps for a Transfer Impact Assessment

The European Data Protection Board (EDPB), the EU body responsible for GDPR implementation, directed businesses exporting EU personal data to the U.S. perform the following six-step assessment:

Step 1: Perform data mapping for cross-border data transfer.

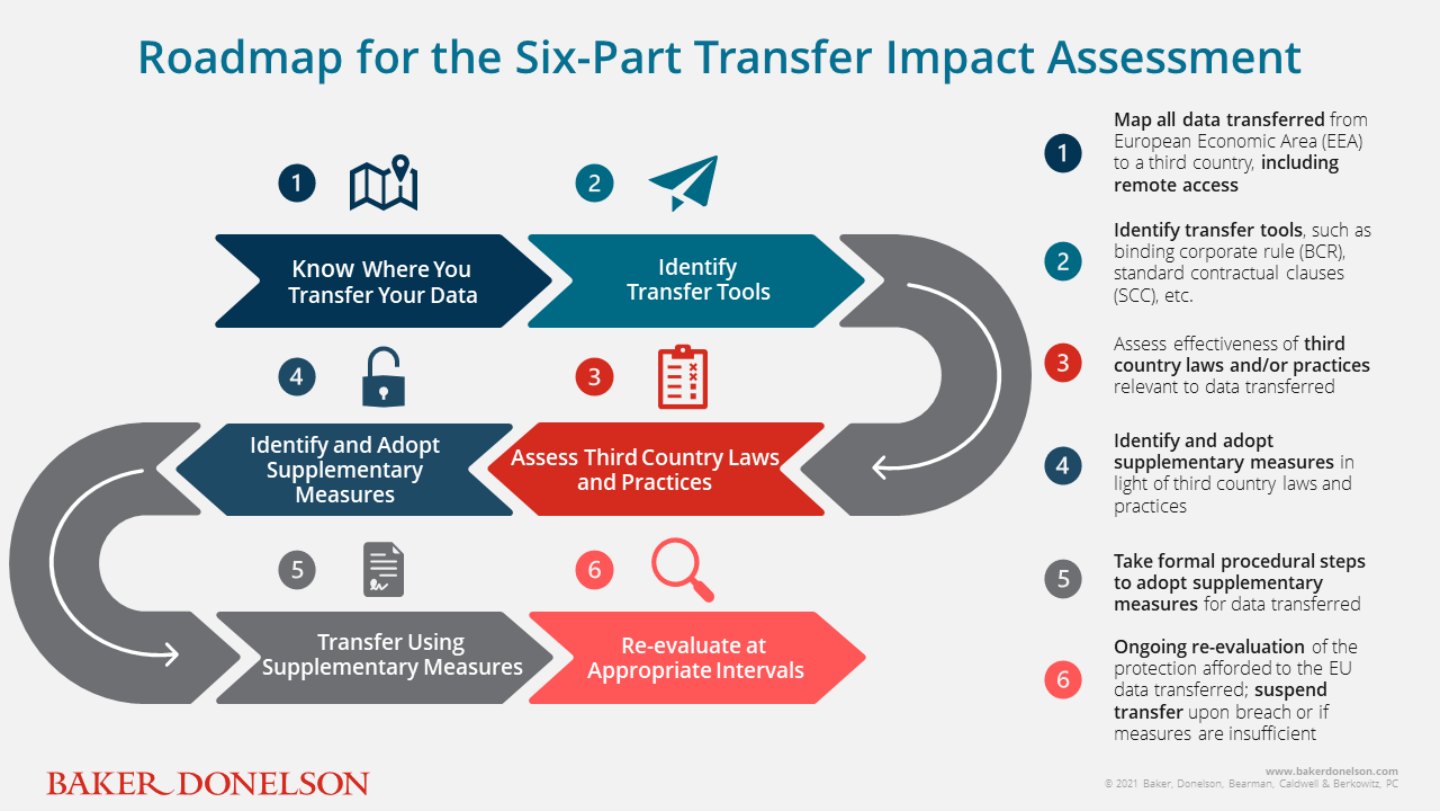
Step 2: Identify appropriate transfer tools, i.e., the New SCC or a few other mechanisms.

Step 3: Assess whether the GDPR will be undermined under any laws and/or practices in the third country (i.e., the U.S.) that are applicable to the specific data being transferred based on relevant, objective, and publicly available information.

Step 4: Identify and adopt appropriate contractual, technical, and organizational measures (supplementary measures) if the third country's laws lack GDPR-equivalent protection.

Step 5: Take formal procedural steps to adopt supplementary measures.

Step 6: Re-evaluate at appropriate intervals the protection afforded to the EU personal data transferred.



Whether organizations choose the New SCC or other transfer tools for cross-border transfers, they should involve their data privacy counsel to conduct the six-step TIA mandated by the EDPB.

The good news is an organization does not need to repeat the assessment every time it transfers the same specific categories of personal data to the same country outside the EU. For example, if a company regularly transfers to the U.S. a dataset with EU residents' names, emails, and job titles, the company must complete and document a TIA specific to transferring this type of dataset to the U.S. in order to comply with the EDPB guidelines. For this specific scenario, the company can rely on the documented TIA without repeating the same process each time it transfers the data, subject to the following conditions:

- The transfer involves the same specific type of data from the EU to the same third party, i.e., the U.S. in this case,
- It continues to implement the necessary supplementary measures, and
- It re-evaluates and monitors the level of data protection afforded to this specific dataset by keeping continuous vigilance of the third country laws and practices.

Conclusion

Similar to the 2021 Suez Canal blockage that disrupted global trade, companies will feel the rippling impacts of the *Schrems II* decision as they operationalize and implement the New SCC. Most U.S. organizations will now need to rely on the New SCC as the primary tool for cross-border transfers. The New SCC provides a mechanism to facilitate trade, while imposing complex, ongoing contractual obligations for data protection. All organizations should thoroughly review the terms and implement supplementary measures, or risk cross-border data transfers on tenuous grounds.

If you have any questions about cross-border transfers or any other privacy matters, please contact Vivien F. Peaden, CIPP/US, CIPP/E, CIPM or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Practice Team.