Strategic Perspectives

Wolters Kluwer

July 18, 2018

Cross Border Transfers of Personal Data: Options to Privacy Shield

By Cynthia J. Cole and Neil Coulson, Baker Botts LLP*

This is the second in a two-part article series by Cynthia J. Cole and Neil Coulson on the future of cross border transfers of personal data under the General Data Protection Regulation if Privacy Shield disappears from the adequacy landscape for cross-border transfers.

The European Union ("EU") imposes strict requirements on entities that collect personal data from individuals residing in the European Economic Area ("EEA") and then transfer that data to a non-EEA country. In particular, the General Data Protection Regulation ("GDPR" or "Regulation"), adopted in 2016 and effective on May 25, 2018, only permits such cross-border transfers to countries or territories with legal regimes that provide an "adequate" level of personal data protection, as determined by the European Commission ("EC").

The United States is not deemed as having "adequate" laws and practices in place for the protection of personal data and thus, multinationals that transfer data to the United States must rely on alternative options. One such mechanism has been the Privacy Shield. However, the future of Privacy Shield is now uncertain, given recent activity by the European Parliament and the European Commission.

If the Privacy Shield is suspended, U.S. companies looking to conduct cross-border transfers must enact Binding Corporate Rules or adopt the EU's Model Clauses. The two alternatives to Privacy Shield that are currently available to U.S. companies are Binding Corporate Rules ("BCRs") and "Model Clauses" (also called "standard contractual clauses"). BCRs are internal regulations that a company enacts globally, which then bind the entire entity. The GDPR expressly included BCRs in the Regulation, which confirms the commitment by the EU to the strength of intra-group global privacy programs and their importance in ensuring compliance. Model Clauses are contractual clauses that the EC has blessed as providing sufficient protections for the transferred personal data. These options have existed simultaneously with Safe Harbor and then Privacy Shield under European data protection regimes but are more cumbersome to implement. Companies that have shunned these options may now no longer have any choice.

Option 1: Binding Corporate Rules ("BCRs") must be internally enacted by a company and externally reviewed and accepted. Binding Corporate Rules allow a company to conduct systematic cro*ss-border transfers of personal data within the same corporate group to a country or countries

* Baker Botts partner **Neil Coulson** is the Department Chair – Intellectual Property in London and Moscow. **Cynthia J. Cole** is Special Counsel in Palo Alto in Baker Botts' corporate, technology and privacy and data security practice groups.

that do not provide an adequate level of protection (as determined by the European Commission)[1]. BCRs are available to both controllers and processors. BCRs ensure that the company, across all geographies, adheres to the required level of protection even if the country into which the data is being transferred does not itself provide the same protections. To enact BCRs, a company must go through the following steps:

1. The company must choose and designate a lead supervisory authority. This is a Data Protection Authority ("DPA") responsible for coordinating EU procedure with other European DPAs. The DPAs are located in each EU member state. The supervisory authority also coordinates any investigations into the company's data transfer or processing activities, handles complaints from data subjects, and is a point of contact regarding compliance. The lead supervisory authority depends on the location of a company's main establishment. Guidelines on designating a lead supervisory authority include deciding whether the company has a centralized establishment which makes decisions about processing activities. If not, the company and the supervisory authority will attempt to determine where the effective and real exercise of management activities takes place, including where the power to have decisions effectively implemented lies, and where the company is registered.

2. The company must draft the BCRs and submit them to the lead supervisory authority for approval. The BCRs must include particular items as enumerated in Article 47 of the GDPR and must also meet the requirements of the Article 29 Working Party (the Working Party and related guidelines have been succeeded by the European Data Protection Board ("EDPB"), which is responsible for implementing the GDPR). The EDPB has acknowledged and endorsed many of the guidelines provided by the Article 29 Working Party. The draft BCRs must be submitted along with (1) application form WP133, (2) a list of entities bound by the rules, (3) an element showing that the rules are binding, and (4) any documentation that shows that the commitments in the rules are being respected. The lead supervisory authority will then review the draft BCRs and provide comments.

3. The BCRs must include, among other items: (1) the structure and contact details of the corporate group and each of its members, (2) the categories of personal data, (3) the type of processing, (4) the type of data subjects affected, (5) the identification of the third country or countries in question, (6) the application of the data privacy principles, in particular, purpose limitation, data minimization, data storage by design and default, (7) the mechanisms for ensuring verification of compliance with the BCRs and (8) the appropriate data protection training to personnel having permanent or regular access to personal data (this list is not exhaustive).

4. The lead supervisory authority will circulate the BCRs to any other relevant DPAs, located wherever the company's personal data transfer or transfers occur.

---

1 Currently the countries deemed to provide an adequate level of protection are: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay.

5. The relevant DPAs receive, review, and accept the BCRs as compliant. To speed up the process of reviewing BCRs, mutual recognition of BCRs was agreed upon by at least 21 member countries. Under mutual recognition, once the lead supervisory authority determines that a company's BCRs are sufficient, DPAs in other countries accept that determination as a valid basis for authorizing the BCRs for their own countries.

6. After the Binding Corporate Rules are considered final and accepted, the company may request authorization for data transfers.

Option 2: Model Clauses (also called "standard contractual clauses") are issued by the European Commission (EC) and may be enacted by a U.S. company depending on the entities involved in the transfer of data.

The EC decides whether a contractual clause includes sufficient safeguards such that a company enacting the clause is legally bound to protect personal data at a level that is deemed adequate. The EC has adopted two sets of clauses that relate to data transfer from a data controller within the EU to a data controller outside of the EEA and the wording of these clauses can either be used as they stand, or the wording can be incorporated into commercial contracts where the transfer of personal data out of the EEA is contemplated. A data controller as defined by the GDPR is an entity that exerts control over the purpose and means for processing personal data. The EC has also adopted a separate set of clauses that relate to data transfer between a data controller in the EU and a data processor outside of the EEA. A data processor as defined by the GDPR is an entity that processes personal data on the behalf of a data controller. It is important to note, however, that the Model Clauses issued by the EC have not been updated since the passage of the GDPR and there is currently a reference from the Irish High Court pending before the Court of Justice of the European Union (CJEU) to rule on their adequacy.

The EC approved sets of standard contractual clauses, namely: (1) the 2001 controller to controller clauses, (2) the 2004 alternative controller to controller clauses and (3) the 2010 controller to processor clauses. These will all remain valid until they are replaced or amended by new versions that match the framework under the GDPR or the CJEU rules that they are inadequate. In addition, some prominent technology companies have already pioneered the idea of obtaining the approval of DPAs for their own versions of data transfer agreements. This is a time-consuming process, but the advantage of this approach is that companies may enjoy greater flexibility in the way they contractually commit to the protection of personal data.

In anticipation of the October 2018 European Commission's annual review of the Privacy Shield, and its possible suspension, currently-certified U.S. companies should investigate Binding Corporate Rules or Model Clauses to ensure no or minimal interruption in any cross-border data transfers of personal data originating in the EEA.