November 18, 2020

Client Alert

Cross-Border Data Transfers Following the *Schrems II* Judgment

Four months ago, the Court of Justice of the European Union (the "CJEU") wreaked havoc when it invalidated the Privacy Shield program for personal data transfers from the EU to the US. Known as the *Schrems II* decision, the CJEU's judgment also conditionally upheld the Standard Contractual Clauses ("SCCs") as a valid mechanism for transfers of personal data to jurisdictions outside the EU.

The CJEU emphasized that before using the SCCs, parties should assess the laws of the destination country and consider reinforcing the SCCs with additional safeguards. Yet the CJEU did not provide detailed guidance on how the assessment should be conducted or what additional safeguards should be used.

With the CJEU's conditions for SCCs validity uncertain, the court left the global data economy puzzled on what needs to be done to lawfully transfer personal data from the EU to other countries. Now, the European Data Protection Board ("EDPB") finally published its draft guidelines,[1] which are not easy to follow and are far from workable for many organizations. These guidelines are open to public comments through November 30, 2020.

The EDPB's Six-Step Recommendations for Supplementary Measures to the SCCs

Step 1: Map Your Data Transfers

Any organization exporting GDPR-governed personal data should map all its data transfers and ensure that the data that it transfers to countries outside the EU (referred to as "third countries") is relevant and limited to what is necessary, considering the purpose of the transfer. The data exporter should also take into account any onward transfers to sub-processors in another third country.

Step 2: Determine which GDPR Transfer Tool to Use

If a data exporter transfers personal data to a country that has been declared by the EU Commission as providing an adequate level of protection of personal data (through an "Adequacy Decision"), no additional steps need to be taken other than monitoring that the Adequacy Decision remains valid.

At this time, the EU Commission recognizes 12 countries as adequate, including Israel, Switzerland, Japan, and Canada (commercial organizations). The EU Commission is currently re-evaluating most of its Adequacy Decisions. Absent an Adequacy Decision, a data exporter will have to rely on one of the other cross-border data transfer tools provided by the GDPR, the most notable being the SCCs.

Shortly after the EDPB issued its draft guidance, the EU Commission published for public comments a draft of an updated version of the SCCs.[2] Once formally adopted by the EU Commission over the next few months, the

[1] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, available at: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en

[2] Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries, available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries . This draft decision is open to public comments through December 10, 2020.

existing version of the SCCs will be repealed. Organizations will then be given a grace period of up to one year to replace their existing SCCs with the new version.

The new SCCs provide coverage for all possible types of transfers. They also enhance the obligations imposed on the parties across various topics, including response to government data access requests, transparency toward the data subjects, and mutual indemnity.

Step 3: Assess the Laws Affecting Data Protection in the Third Country

The data exporter is required to conduct an assessment of the laws in the third country that may affect the level of protection of personal data, to ensure that the personal data transferred benefits from an "essentially equivalent" level of protection as the GDPR provides.

The assessment should focus on laws that affect the exercise of data subject rights and access to data by public authorities for surveillance purposes. The assessment needs to be properly documented.

A major hurdle is the requirement to conduct an assessment of the laws in a third country, which undoubtedly is a resource-intensive task. Another hurdle found in the guidelines is the requirement to assess only objective factors, such as the existence and scope of public authorities' right to access personal data, with no ability to rely on subjective factors such as the likelihood that authorities will access personal data given the specific circumstances of the data exporter.

To assist with the assessment, the EDPB also issued a European Essential Guarantees ("EEG") document[3]. It explains what the EDPB views as the essential guarantees necessary in the laws of a third country that allow public authorities access to personal data for surveillance purposes. If these guarantees are not satisfied, the laws of a third country cannot be considered "essentially equivalent" to the laws of the EU.

The EEG poses another hurdle, making it questionable whether third countries that often attract data transfers can satisfy the EEG criteria. Notably, the CJEU and the EDPB have already determined that the United States, in the current state of its laws, does not meet the EEG criteria.

Step 4: Identify and Adopt Supplementary Measures

In the probable scenario that step 3 reveals that the third country does not provide an essentially equivalent level of protection as the EU, the data exporter must identify and adopt supplementary measures on a case-by-case basis. The purpose of these measures is to elevate the protection afforded to the data so that it rises to the appropriate level of protection under the EU standards. The selection of measures also needs to be properly documented to comply with the GDPR's accountability principle.

The supplementary measures at issue may be contractual, technical, and organizational. The data exporter may have to combine several measures to ensure the appropriate level of protection. Yet, the EDPB clarifies that contractual and organizational measures alone will generally not safeguard against access to personal data by the authorities of a third country. In these situations, sufficiently protective technical measures must also be used. If the data exporter finds that no additional measures can ensure an essentially equivalent level of protection, it may not transfer personal data to that third country.

[3] Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

The EDPB provides a non-exhaustive list of suggested measures, including encryption as a technical measure where the recipient in the third country is exposed only to encrypted data. However, encryption is not a workable solution for cloud processing in third countries (including the United States), because cloud processing usually requires a clear-text (unencrypted) copy of the data.

Step 5: Formal Procedural Steps with EU Data Protection Authorities

In some cases, the data exporter will need to approve its supplementary measures with the relevant EU supervisory authority. For example, where the additional measures proposed may directly or indirectly conflict with the original provisions of the SCCs.

Step 6: Periodically Re-Evaluate and Follow Developments in the Third Country's Laws

The data exporter should periodically re-evaluate the level of protection afforded to personal data in the third country and follow any developments in that third country's law that may affect its initial assessment. The data exporter should also establish appropriate mechanisms to ensure that it can promptly suspend or discontinue transfers. This could be the case where the data importer has breached or is unable to honor, the commitments it has taken regarding the protection of the personal data, or where the supplementary measures are no longer effective in that third country.

Recommendations

The EDPB's draft recommendations on supplementary measures, together with the European Essential Guarantees document and the EU Commission's draft update to the SCCs, would introduce significant practical difficulties for many organizations that engage in cross-border transfers of GDPR-governed data. This is particularly true with transfers to U.S. cloud service providers.

We recommend that organizations take advantage of the remaining period for public comments to submit their concerns and feedback to the EDPB and the EU Commission. Also, given the likelihood that the final guidelines will not change dramatically, we recommend that organizations evaluate their data transfer posture in light of these rules, and consider viable alternatives to their data transfers to third countries, where necessary.

Haim Ravia
HRavia@PearlCohen.com

Dotan Hammer
DHammer@PearlCohen.com

The Internet, Cyber and Copyright Group
Pearl Cohen Zedek Latzer Baratz