Overview

Schrems II Update and Data Transfer Assessment

David Dumont
Anna Pateraki
Hunton Andrews Kurth

Bloomberg Law

Become a Contributor

Schrems II Update and Data Transfer Assessment

Contributed by David Dumont and Anna Pateraki, both in the Brussels office of Hunton Andrews Kurth.

On July 16, 2020, the Court of Justice of the European Union (CJEU) issued a landmark ruling invalidating the EU-U.S. Privacy Shield Framework, but affirming the ongoing validity of the EU Standard Contractual Clauses (SCCs) as a data transfer mechanism, subject to an additional assessment of the transfer.

Overview of the Judgment

In Data Protection Comm'r v. Facebook Ireland Ltd., Case C311/18 (often referred to as "*Schrems II*"), the CJEU invalidated the European Commission's adequacy decision underlying the EU-U.S. Privacy Shield Framework on grounds that it does not provide an adequate level of protection for the transfer of personal data from the EU to the U.S. due to concerns related to public authorities' access to EU personal data under U.S. law.

In particular, the CJEU took the view that the limitations on the protection of personal data arising from U.S. domestic law on the access and use of the transferred EU personal data by U.S. public authorities are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law (in particular under the principle of proportionality), in so far as the U.S. government surveillance programs include provisions that are not limited to what is strictly necessary. Notably, the CJEU focused, among others, on Section 702 of the US Foreign Intelligence Surveillance Act of 1978 (FISA) that applies to data collection from "electronic communication service providers".

In addition, according to the CJEU, the EU-U.S. Privacy Shield Framework does not grant EU individuals actionable rights before an independent body offering guarantees that are substantially equivalent to those required under EU law. On those grounds, the CJEU declared the EU-U.S. Privacy Shield invalid. Therefore, organizations that relied on the EU-U.S. Privacy Shield Framework to legitimize transfers of EU personal data to the U.S. should transition to alternative data transfer mechanisms such as the SCCs or Binding Corporate Rules.

As for the validity of the SCCs, the CJEU stated that the SCCs provide sufficient protection for EU personal data, but imposed an obligation on organizations relying on them to assess, prior to the transfer, whether there is in fact an "adequate level of protection" for personal data in the importing jurisdiction (see below).

In addition, the CJEU concluded in its judgment that a competent supervisory authority may suspend or prohibit a transfer of personal data pursuant to SCCs under certain circumstances, in particular where the SCCs cannot be complied with in the destination country.

Notwithstanding the CJEU judgment, the U.S. Department of Commerce issued a press release on July 16, 2020, indicating that it will continue to administer the Privacy Shield program and that the CJEU's judgment does not relieve participating organizations of their Privacy Shield obligations.

New Obligations for Organizations

Schrems II marks a new era for cross-border data transfers, whereby reliance on a data transfer mechanism alone is no longer sufficient. A company's data transfer mechanism must now be backed up by a data transfer assessment for accountability purposes.

With respect to conducting a data transfer assessment, the CJEU held that both the data exporter and the data importer should:

- Assess on a case-by-case basis the law of the destination country, in particular laws regarding access by public authorities to EU personal data transferred, to determine whether the relevant legal framework allows the data importer to comply with its obligations under the relevant data transfer mechanism (i.e., the SCCs for the purpose of the judgment); and
- Implement "supplementary measures" to those offered by the SCCs, *if necessary* to ensure an appropriate level of data protection in the destination country.

Where a data importer is unable to comply with the terms of the SCCs, or there is otherwise an inadequate level of protection for EU personal data transferred, the data exporter must cease the transfer of personal data and require the data importer to delete or return any personal data already transferred.

EDPB Recommendations on Supplementary Measures

On November 11, 2020, the European Data Protection Board (EDPB), the body of EU data protection authorities, published recommendations following *Schrems II* regarding measures that supplement data transfer tools under the GDPR (Recommendations on Supplementary Measures). The Recommendations were subject to public consultation and the final version is expected in early 2021.

The Recommendations include six steps that organizations should follow to identify and implement effective supplementary measures post *Schrems II*:

- Know your transfers and map the transfers that the organization carries out;
- Identify the data transfer mechanism(s) under the GDPR on which the organization relies;
- Assess the legal system of the destination country (see EEG Guarantees below) to determine whether it undermines the protection under the relevant data transfer mechanism (i.e., whether the chosen data transfer mechanism continues to be effective in light of the circumstances of the transfer);
- Consider implementing technical, contractual and organizational supplementary measures if the legal assessment concludes that the legislation of the destination country "impinges" on the effectiveness of the chosen data transfer mechanism;
- Take any formal procedural steps required for the adoption of the supplementary measures (e.g., seek approval from a supervisory authority if there is intention to modify the substance of the SCCs); and
- Monitor developments and re-evaluate the transfer assessment at appropriate intervals.

EDPB Recommendations on European Essential Guarantees

In addition, the EDPB published recommendations on the European Essential Guarantees for surveillance measures (EEG Recommendations), which organizations should take into account when conducting the relevant assessment of a third country's laws for *Schrems II* purposes.

The EEG Recommendations provide that laws which intend to make limitations to the data protection rights recognized by the EU Charter of Fundamental Rights (such as measures that allow access to personal data by public authorities) should require that:

- The processing of personal data in connection with government access and surveillance measures is based on clear, precise and accessible rules;
- The data processing demonstrably takes into account the principles of necessity and proportionality with regard to the legitimate objectives pursued;
- An independent oversight mechanism exists; and
- Effective remedies are available to the individuals whose personal data is processed.

Conducting a Data Transfer Assessment

A data transfer assessment should consider the EEG Recommendations, as discussed above. As part such assessment, an organization should collect information (where needed with the help of the data importer) and evaluate issues such as:

- Does the destination country have a data protection regime that generally provides the same protections for individuals as the GDPR?
- Do the laws in the destination country allow public authorities to carry out bulk government surveillance or can government surveillance be carried out in a proportionate manner?

- Are such government surveillance laws ambiguous or not publicly available?

In addition, a data transfer assessment should take into account the GDPR's risk-based approach. Accordingly, the assessment should also consider whether there is "high" or "limited" risk that government surveillance laws in the destination country are likely to "impinge" on the effectiveness of a data transfer mechanism in the context of a specific type of transfer. That said, it would be useful to assess (i) the data importer's exposure to government surveillance (for example, by taking into account criteria such as the data importer's sector of business, the types of data transferred and the data importer's history in relation to being subject to government surveillance or not), and (ii) the data importer's ability to oversee, minimize or challenge data disclosure requests made by public authorities.

There is no one-size-fits-all solution of what supplementary measures may be required in a given data transfer scenario. Depending on the circumstances of the transfers (e.g., intra-group transfers, transfers to vendors), an organization may consider implementing:

- *Technical* supplementary safeguards such as encryption (e.g., in transit/at rest), pseudonymization or other obfuscation method;
- *Contractual* supplementary safeguards (e.g., addendum to data transfer agreement); and/or
- *Organizational* supplementary safeguards (e.g., internal governance policies and procedures regarding how to handle data access requests by public authorities).

Of course, the more supplementary measures an organization is able to implement, the more the risk is mitigated.