rjgaito
LAW FIRM

The Business of Data

RJ Gaito's Data Protection and Cyber Update

Date: September 1st, 2020

International data transfers

Highlights:

The Court of Justice of the European Union (CJEU) on July 16, 2020, delivered its latest judgment in Max Schrems' case against Facebook Ireland Ltd. and Data Protection Commissioner (Ireland) (Max Schrems II). In a landmark decision, the CJEU struck down the European Union-United States of America (EU-US) Privacy Shield scheme as a mechanism allowing US commercial companies to transfer and store EU personal data in the US.

The CJEU validated the Standard Contractual Clauses (SCCs) which Facebook had been using, however, it invalidated the Privacy Shield and the "adequacy decision" of the European Commission's decision (EU) 2016/1250 of July 2016, relating to the Privacy Shield mechanism.

The CJEU decision makes EU-US data transfer contentious and, consequently, requires scrutiny of any data transfer from the EU to any third country, irrespective of the implementation of the SCC or a so-called EU "adequacy decision".

The judgment provided critical guidance for transfer of data of EU data subjects outside the EU.

General Guiding Principles:

- The SCCs, as a mechanism for maintaining General Data Protection Regulation (GDPR) compliance, is valid but they do not in themselves validate data transfers. The prevailing and critical element for a valid transfer of data is whether the third country provides, in a continuous manner, adequate safeguards to EU data subjects. This essentially means protection which is equivalent to that guaranteed by the EU. In this context, judicial redress for data subjects in the third country is an essential element to consider.
- Even where the SCCs are implemented, the analysis that should be undertaken is whether any third country provides adequate protection for personal data and data subject. Any such analysis must consider actionable judicial redress for data subjects that is of critical importance.
- SCCs and "adequacy" decisions are no longer a compliance guarantee with EU GDPR.

Recommendations:

- Parties should consider if they are using data importers that are relying on the EU-US Privacy Shield for validating data transfers and consider how to strengthen their data transfer mechanisms.
- Data exporters and importers now need to assess the level of data protection in the data recipient's country and to suspend transfers if deemed inadequate. Failure to do so could result in legal liabilities.
- Data protection authorities need to assess whether transfers to third countries provide adequate protection.
- Any laws or practices in third countries that could detract from the SCCs contractual guarantees of adequate protection should indicate that such country's approach to data protection is incompatible with GDPR. Countries that use extensive surveillance practices should be of particular concern.
- Organizations should consider resorting to European Economic Area (EEA) service providers for data processing services.

Background

When Personal data is transferred outside the EEA, special safeguards are foreseen to ensure that the protections travel with the data. The 2016 GDPR reform offers a toolkit of mechanisms to transfer data to third countries in the form of the EU Commission adequacy decision mechanism, binding corporate rules, as well as derogations for specific situations.

One such scheme was the Privacy Shield put in place for EU-US data transfers which received a so called "adequacy decision" by virtue of the EU Commission implementing decision (EU) 2016/1250. Notwithstanding that the adequacy decision, by its decision rendered on July 16, 2020, the CJEU invalidates the Privacy Shield.

Under the Privacy Shield, US companies wishing to process EU personal data were required to be registered under the Privacy Shield list, each year explaining which data they are collecting and how they apply the Privacy Shield principles.

In Schrems II, the CJEU determined that the US is not providing an equivalent level of protection for data subjects, and more specifically, because of access and use of the transferred data by US public authorities.

The key considerations that the CJEU applied to invalidate the Privacy Shield was on the basis that under US law there are insufficient guarantees to data subjects and that it was lacking in the required judicial redress and actionable rights before courts for non-US persons against the US authorities.

In Schrems II, the CJEU recognized SCCs as valid, being another transfer safeguard for international data transfer, however, only to the extent that data is transferred to a jurisdiction which offers equivalent protection to the one granted within the EU.

The implementation of SCCs is now insufficient to ensure the lawfulness of the transfer under the GDPR and it is necessary to analyse and ensure a level of protection substantially equivalent to that guaranteed within the Union.

Resulting legal uncertainty

It is our view that transfer of data to the US, based exclusively on the Privacy Shield, is currently not permissible and supplementing existing SCCs is a task entailing a highly uncertain outcome.

The European Data Protection Board (EDPB) is now working to determine which kind of supplementary measures can be taken to ensure the necessary protections for achieving the required EU standard.

We note that, the EDPB's position (FAQ taken of July 23, 2020), is that the CJEU assessment applies, notwithstanding an adequacy decision or the implementation of binding corporate rules. The EDPB reiterates the view that, the exporters and importers of data are responsible for analysing the adequacy of protection in that third country of destination to enable the data importer to comply with the standard data protection clauses or the binding corporate rule, before transferring personal data to that third country.

Therefore the exporters and importers of data are responsible for illegal or otherwise invalid data transfers and consequently it is essential to make an analysis of the situation and to ensure that the third country offers an equivalent level of protection.

Henceforth, the transfer of data from EU to US can no longer be justified and legitimate by the Privacy Shield.

Each transfer made on that basis is illegal and the controller or processor, in their capacity as importers or exporters of data, must find another way to comply with GDPR.

Where do matters stand now?

The CJEU argued that its judgment does not create a legal vacuum and makes reference to Article 49 of GDPR, whereby in the absence of an adequacy decision or appropriate safeguards, certain exemptions permit data transfers where the data subjects have given their consent, and those transfers are necessary for the conclusion or performance of a contract between the data subject and the controller.

In its FAQ adopted on July 23, 2020, the EDPB underlined that, recourse to the Article 49 exemptions shall remain for occasional transfers and could not be a permanent basis for validating recurring transfers.

In the light of the EDPB response, we believe that Schrems II has created significant legal uncertainties for EU-US data transfers, as well as is the case of other non-EEA countries.