SULLIVAN & CROMWELL LLP

July 20, 2020

European Court of Justice Further Restricts Data Transfers in *Schrems II*

EU-US Privacy Shield Invalidated and Adequacy of Standard Contractual Clauses Must be Assessed on a Case-by-Case Basis

SUMMARY

In the recent decision of *Data Protection Commissioner* v. *Facebook Ireland Limited, Maximillian Schrems* (Case C-311/18) ("*Schrems II*"), the European Court of Justice for the European Union ("CJEU") has affirmed the validity of Standard Contractual Clauses ("SCCs") as a mechanism to effect lawful transfers of personal data from the European Economic Area ("EEA") to third countries under the European Union's General Data Protection Regulation ("GDPR") but has specified that SCCs must offer an adequate level of protection of personal data, based on a case-by-case assessment of the circumstances of the transfer. The CJEU has also invalidated the EU-US Privacy Shield mechanism for transfer, striking a major blow to the thousands of U.S.-based organizations that rely on the shield to receive data transfers from the EU.

BACKGROUND

Max Schrems (an Austrian citizen and privacy advocate) is notable for having previously successfully challenged the transfer of his data (and the data of EU citizens generally) to the U.S. by Facebook Ireland Ltd to its U.S.-based parent company, Facebook Inc. (C-362/14 of October 6, 2015, "*Schrems I*"). *Schrems I* led to the CJEU invalidating the Safe Harbour Privacy Principles, which governed transfers of data and resulted in the implementation of the EU-U.S. Privacy Shield (discussed below) under which U.S.-based companies may, following certification, receive data for commercial purposes from the EU. Following the decision in *Schrems I*, the Irish High Court (which had referred the case to the CJEU) referred the decision back to the Irish Data Protection Commission ("DPC") for assessment. The DPC opened an investigation and requested that Mr. Schrems reformulate his complaint having regard to the declaration in *Schrems I* that the Safe Harbour Privacy Principles were invalid.

Mr. Schrems subsequently requested that Facebook Ireland identify the legal bases for the transfer of personal data of users of the Facebook social network from the EU to the U.S. In response, Facebook Ireland referred to a data transfer processing agreement between it and Facebook Inc., modelled on Standard Contractual Clauses ("SCCs") adopted by the European Commission pursuant to Decision 2010/87, which, under GDPR, create a legal basis for transfer of data from the European Economic Area ("EEA") to third countries (including the U.S.). In his reformulated complaint to the DPC, Mr. Schrems claimed first that the clauses in that agreement were not consistent with the SCCs adopted pursuant to Decision 2010/87. Second, Mr. Schrems asserted that SCCs could not in any event justify the transfer of his personal data to the U.S. because, under U.S. law, Facebook Inc. is required to make the personal data of its users available to U.S. authorities, such as the National Security Agency and Federal Bureau of Investigation. Mr. Schrems claimed that there was no remedy that would adequately protect EU data subjects' rights to respect for private life and protection of personal data in these circumstances, and that the DPC should suspend the data transfers.

The DPC considered that it was impossible to adjudicate on Mr. Schrem's complaint unless the Court examined the validity of the SCCs and therefore brought proceedings before the Irish High Court. Sharing the DPC's doubts, the Irish High Court referred a number of questions to the CJEU for preliminary ruling. In summary those questions concerned:

- The applicability of EU law when data transferred is processed in third countries for national security reasons.
- The level of protection required for transfers.
- The impact of the non-binding nature of SCCs on third country public authorities.
- The validity of the SCCs adopted pursuant to Decision 2010/87, including their validity in light of the EU Charter of Fundamental Rights (the "EU Charter") which protect EU citizens' rights to private life and right to the protection of personal data concerning him or her.
- An assessment of the EU-U.S. Privacy Shield.

DATA TRANSFERS UNDER GDPR

As well as regulating the processing of personal data, GDPR places restrictions on transfers of personal data from the European Economic Area ("EEA") to a third country or international organizations. The restrictions are designed to ensure that the protections that personal data are afforded within the Union are not lost as a result of a transfer outside of it.

Pursuant to Article 45, GDPR, the European Commission has the ability to grant an "adequacy decision" in respect of any non-EU jurisdiction. Transfers to countries that have been determined adequate by the Commission do not require any further specific authorization. The Commission has so far recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay as providing adequate protection of personal data. The U.S. was also recognized but only in so far as the EU-U.S. Privacy Shield framework (adopted on 12 July 2016 following *Schrems I*) applied. Companies in the U.S. could certify under that framework for the purposes of receiving data from the EU for commercial purposes. The

Shield subjected certified companies to strong data protection obligations, and required safeguards on U.S. government access to data, effective protection and redress for individuals, and an annual joint review by the EU and U.S. to monitor the correct application of the arrangement.

In the absence of an adequacy decision, transfers of personal data to a third country or international organization may take place subject to "appropriate safeguards" being implemented, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available. Such safeguards are listed at Article 47 GDPR and include binding and enforceable instruments between public authorities, binding corporate rules, SCCs, and approved codes of conduct or certification mechanisms. If an "appropriate safeguard" is not in place then any transfer must fall within one of the Article 49 derogations, which apply in limited circumstances only (*e.g.*, with the informed consent of the data subject, or to exercise a legal right or defence), and are designed as a last resort means of effecting "occasional" and "necessary" transfers.

SCCs have become one of the most frequently relied upon safeguards for transferring data from the EEA to third countries and international organizations, and are commonly used where data is transferred from the EEA to the United States in the absence of a Privacy-Shield certification. SCCs can be entered into between two data controllers or between a controller and a processor (*Schrems II* concerned Controller-Processor SCCs adopted pursuant to Decision 2010/87). SCCs may also be adopted by a Member State data supervisory authority and subsequently approved by the Commission. SCCs are standard form and may not be modified by the parties save that they are required when executing their agreement to add details of the categories of affected data subjects, the purpose of the transfer, the categories of data (including categories of sensitive data), recipients of the data, and, in the case of controller-processor transfers, details of the data processing activities that the data will be subject to.

DECISION

In a comprehensive judgment, the CJEU dealt with a number of issues arising in connection with data transfers, before concluding that: (i) SCCs were a valid mechanism for effecting transfer of personal data from the EEA to third countries but that their adequacy must be assessed on a case-by-case basis; and (ii) the EU-U.S. Privacy Shield was invalid as a means of effecting data transfers from the EU to the U.S.

The Court held that EU law applies to transfers of personal data to a third country where those transfers form part of commercial activity, even though the transferred data may then undergo processing by the public authorities of the third country for the purposes of national security. In other words, data processing by the authorities of a third country cannot exclude such a transfer from the scope of GDPR.

On the level of protection required in respect of transfers to third countries, the Court held that the requirements laid down in GDPR concerning appropriate safeguards, enforceable rights, and effective legal remedies, must be interpreted as meaning that data subjects whose personal data is transferred to a third country pursuant to SCCs, will be afforded a level of protection essentially equivalent to that

guaranteed within the EU by GDPR, read in light of the EU Charter (which guarantees in particular, respect for private and family life, personal data protection and the right to effective judicial protection). The Court specified that the level of protection provided when transferring data pursuant to an SCC must be assessed on a case-by-case basis. That assessment must take into consideration both the contractual obligations entered into by the data exporter and data importer, and the relevant aspects of the legal system of the third country, in particular access by the public authorities of that third country to the data transferred.

The Court also clarified the role of EU Member State data supervisory authorities ("DPAs"), in connection with data transfers to third countries. Unless there is an adequacy decision issued by the Commission with respect to the destination country, DPAs must suspend or prohibit a transfer of personal data if they take the view that SCCs being relied upon to effect the transfer are not or cannot be complied with in that country, and that the protection that is required by EU law of the data transferred, cannot be ensured by other means.

Having made these findings, the Court turned to the key issue of the validity of Decision 2010/87 (pursuant to which the Commission has approved Controller-Processor SCCs). The Court found that the fact that SCCs are contractual in nature, and thus do not bind public authorities of third countries, does not affect their validity. That said, their validity must depend on whether there are effective mechanisms to ensure the same level of protection as required by EU law in connection with the data. In addition, there should be mechanisms that allow for suspension or prohibition of transfers of personal data in the event of a breach of the SCCs, or if honoring the terms of the clauses becomes impossible. The Court found that the SCCs do establish such mechanisms, pointing in particular to the fact that the SCCs adopted pursuant to Decision 2010/87 impose obligations on both the exporter and importer of data to verify, prior to any transfer, whether the level of protection afforded to the data in the EU is respected in the third country concerned. Data importers are also required to inform data exporters of any inability to comply with SCCs, following which, the data exporter is required to suspend the transfer of data and/or terminate the contractual arrangement with the importer.

Finally, the Court examined the validity of the EU-U.S. Privacy Shield in light of the requirements arising under the GDPR, and the relevant provisions of the EU Charter. The Court noted that the Shield enshrines the primacy of U.S. national security, public interest, and law enforcement, thus condoning interference with the fundamental rights of persons whose data is transferred to the U.S. The Court highlighted limitations on the protection of personal data arising from U.S. domestic law on the access to and use by U.S. public authorities. It found that those features of the U.S. legal system are not circumscribed in a way that satisfies the data protection requirements to those under EU law. In particular, U.S. surveillance programmes are not adequately restricted by the principle of proportionality in so far as they are not limited, in accessing data, to what is strictly necessary. Further, the CJEU found that the EU-U.S. Privacy Shield framework does not grant EU individuals actionable rights before a 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.

COMMENT

While SCCs remain a valid means of effecting data transfers outside of the EEA, organizations that currently rely on them must carefully consider whether the data will be adequately protected in the country of destination, not only as a matter of contractual obligation, but also taking into account the relevant aspects of the third country's legal system, in particular the ability of public authorities to access and use the data being transferred. Organizations must not rely blindly on SCCs to effect transfers but must carefully assess each transfer on a case-by-case basis and adopt supplementary measures if required. If supplementary measures are required, and cannot be put in place which ensure adequate protection of the data, then the transfer will only be able to take place pursuant to one of the narrowly drawn derogations provided for in Article 49, GDPR. Supervisory authorities will also be expected to play a more active role in monitoring data transfers.

With regards to the EU-U.S. Privacy Shield, the Court did not stipulate any grace period with respect to its invalidation, therefore organizations that currently rely on the Shield for effecting data transfers must urgently identify an alternative transfer mechanism. Organizations may be able to rely upon derogations for certain transfers. SCCs, or alternative approved safeguards (such as binding corporate rules) should also be considered. At the same time, the U.S. Department of Commerce, expressing its disappointment at the CJEU's decision, has stated that the CJEU's decision does not relieve participating U.S. organizations of their Privacy Shield obligations.

Both aspects of the CJEU's decision in *Schrems II* create potentially significant challenges for companies wishing to transfer data from the EU to the U.S. The removal of the EU-U.S. Privacy Shield threatens some 5,000 U.S.-based companies' ability to receive data from the EU. In addition, the assessments required prior to the use of SCCs to effect transfers will likely have a particular impact on transfers to U.S.-based organizations. The Irish DPC has already highlighted, in a statement issued in response to the judgment, that the application of the SCC mechanism to transfers of personal data to the U.S. is now questionable, and that this is an issue that will require further and careful examination, not least because assessments will need to be made on a case-by-case basis. More generally, organizations may want to review whether sending personal data outside the EU or a jurisdiction that has been determined adequate, is the best course for their business in light of alternatives available to them.

* * *

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York		
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Nicole Friedlander	+1-212-558-4332	friedlandern@sullcrom.com
Nader A. Mousavi	+1-212-558-1624	mousavin@sullcrom.com
Palo Alto		
Nader A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com
London		
Craig Jones	+44-20-7959-8488	jonescra@sullcrom.com
Paris		
Gauthier Blanluet	+33-1-7304-6810	blanluetg@sullcrom.com
Frankfurt		
Carsten Berrar	+49-69-4272-5506	berrarc@sullcrom.com
Krystian Czerniecki	+49-69-4272-5525	czernieckik@sullcrom.com
Michael Rosenthal	+49-69-4272-5533	rosenthalm@sullcrom.com
Brussels		
Michael Rosenthal	+32-2896-8001	rosenthalm@sullcrom.com