Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Court of Justice of the European Union Rules Privacy Shield Invalid and Standard Contractual Clauses Can Remain But Only in Certain Circumstances

July 17, 2020

On July 16, 2020, the Grand Chamber of the Court of Justice of the European Union (CJEU) in Luxembourg handed down its highly anticipated judgment in a case brought by privacy activist Max Schrems (C-311/18, Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems ("Schrems II")). The seminal judgment upholds the use of Standard Contractual Clauses (SCCs) but only in certain circumstances, and, significantly, finds that the EU-U.S. Privacy Shield is an invalid mechanism for transferring personal data from the EU to the U.S. under the General Data Protection Regulation (GDPR). The judgment follows a hearing in the case on July 9, 2019, and publication of the legal opinion of Advocate General Henrik Saugmandsgaard Øe on December 19, 2019. We set out below the key features of this judgment and the implications for international data transfers.

I. Background to Schrems II

In June 2013, Schrems challenged the validity of the so-called Safe Harbor agreement between the EU and the U.S. before the Irish Data Protection Commissioner ("Irish DPC"), where he requested that Facebook Ireland be prohibited from transferring his personal data to the U.S. Although his complaint was initially rejected by the Irish DPC, the High Court of Ireland made a request to the CJEU for a preliminary ruling on the validity of Safe Harbor. In its landmark ruling on October 6, 2015, the CJEU struck down Safe Harbor on the basis that it violated fundamental rights to privacy in not affording a level of protection for personal data equivalent to that which is afforded under EU law (Maximillian Schrems v. Data Protection Commissioner (C-362/14) ("Schrems I")). The invalidated Safe Harbor was replaced by the EU-U.S. Privacy Shield ("Privacy Shield"), a framework arrangement which allowed the transmission of personal data from EU entities to registered U.S. entities, following the European Commission's ("Commission") decision that the Privacy Shield provided adequate protections ("Privacy Shield Decision").[1]

Following Schrems I, the vast majority of EU controllers and processors entered into SCCs with their U.S. counterparties (and counterparties in other countries, for which

Contact Information

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Jenny Arlington (nee Grozdanova)
Counsel
jarlington@akingump.com
London
+44 20.7012.9631

Rachel Claire Kurzweil
Associate
rkurzweil@akingump.com
Washington, D.C.
+1 202.887.4253

Sahar Abas
Trainee Solicitor
(not admitted to practice)
sahar.abas@akingump.com
London
+44 20.7012.9859

there is currently no adequacy decision[2] by the Commission) in order to transfer personal data lawfully out of the EU. Schrems then challenged the use of SCCs by Facebook Ireland. He maintained that U.S. law required Facebook Inc., to whom Facebook Ireland transferred personal data of EU based users, to make such data available to certain U.S. authorities, including the National Security Agency (NSA) and Federal Bureau of Investigation (FBI), which Schrems asserted was incompatible with his data privacy and other fundamental rights.

The Irish High Court subsequently made a reference to the CJEU (a procedure under EU law where national courts may seek clarifications on questions of EU law) with 11 questions broadly concerning whether personal data transfers of data from the EU to the U.S. and the access, use and retention of data by U.S. authorities transferred from the EU to the U.S. is contrary to the level of data protection and privacy guaranteed as a fundamental right under EU law.

II. Key Features of the CJEU Judgment

The judgment considers all 11 questions referred by the Irish High Court, but the most significant part of the decision relates to the questions on SCCs and the Privacy Shield.[3]

1. Standard Contractual Clauses: Valid, But Only in Certain Circumstances

After Schrems I and the annulment of Safe Harbor, the Irish DPC continued the investigation into the mechanisms under which Facebook Ireland transferred data to Facebook Inc. in the U.S. In that investigation, Facebook Ireland explained that a large part of personal data was transferred to Facebook Inc. pursuant to SCCs. The Irish DPC then issued a draft decision, stating that the investigation is ongoing, but provisionally found it likely that the personal data of EU citizens would be processed by the U.S. authorities in a manner incompatible with Articles 7 (Respect for private and family life) and 8 (Protection of personal data) of the Charter of Fundamental Rights of the European Union ("Charter"). Further, the Irish DPC's preliminary view was that U.S. law did not provide EU citizens with legal remedies compatible with Article 47 of the Charter.

In light of that, the CJEU was asked whether a data protection authority (DPA) is required to suspend or prohibit a transfer of personal data to a third country pursuant to SCCs, if the DPA's view is that the SCCs cannot be complied with in that third country, or whether the power to suspend or prohibit transfers should be limited to exceptional cases. The CJEU explained that if the Commission has made an adequacy decision (currently issued to only 12 jurisdictions[4]) which is still in place, a DPA cannot validly conclude that a jurisdiction does not offer adequate protection. However, for all the other third countries where no Commission adequacy decision is in place, a DPA is allowed to take a view that the SCCs are not, or cannot be, complied with, and that EU law requirements for the protection of the data transferred cannot be ensured by other means. The CJEU ruled that, in such cases, the DPA **must** suspend or prohibit the transfer, unless the controller or the processor have already done so. Further, faced with the risk that the DPAs in each Member State can adopt divergent decisions, the CJEU reminded DPAs of the possibility to refer the matter to the European Data Protection Board (EDPB), so that the EDPB can adopt a binding decision applicable to all Member States.

The CJEU also examined whether SCCs should be invalidated, given that they are in place where there is no Commission adequacy decision and, by their contractual nature, they do not bind the authorities in third countries. The CJEU, like the Advocate General, found that there is nothing to affect the validity of the legal instrument with which the SCCs were put in place.[5] However, the CJEU emphasized that their validity depends on whether **in practice** the SCCs make it possible to ensure compliance with the level of protection required by EU law, as envisaged by the various rights and obligations in the wording of the SCCs. In the event of a breach of the SCCs or impossibility to honor them, the transfer should be suspended or prohibited. The CJEU pointed out the EU data exporter's obligation to suspend the data transfer or terminate the contract where the recipient outside the EU is not, or no longer able, to comply with the obligations under the SCCs, as well as the duty of that recipient to tell the EU counterparty about any inability to comply.

2. EU-U.S. Privacy Shield Invalid

In 2016, the Commission found that the Privacy Shield ensured an adequate level of protection of personal data transferred from the EU to the U.S. In Schrems II, the CJEU ruled that the Privacy Shield was invalid, broadly for two reasons.

First, the Commission had acknowledged that the Privacy Shield Framework Principles (issued by the U.S. Department of Commerce) ought to be adhered to "the extent necessary to meet national security, public interest, or law enforcement requirements." The CJEU found that this derogation enabled interference with personal data based on national security, public interest or on the basis of U.S. domestic legislation. Those limitations on the protection of personal data arising under domestic U.S. law were not equivalent to the limitations allowed under EU law. In particular, the CJEU found that:

- Section 702 of the Foreign Intelligence Services Act (FISA) did not contain any limitations on the power to implement surveillance programs for the purposes of foreign intelligence, and did not contain guarantees for non-U.S. persons potentially affected by such programs. Under EU law, interference with fundamental rights must satisfy the requirements of the principle of proportionality, be clearly defined in scope and be subject to minimum safeguards, which were not features the CJEU could identify in FISA.
- Both surveillance programs under Section 702 of FISA and monitoring programs based on Executive Order 12333 ("E.O. 12333") did not confer rights that were enforceable against U.S. authorities in courts.
- Presidential Policy Directive 28 ("PPD-28"), with which the surveillance programs under FISA and monitoring programs under E.O. 12333 must comply, allowed for bulk collection of large volumes of data and permitted access to data in transit to the U.S. without that access being subject to any judicial review. Consequently, the CJEU held that neither Section 207 of FISA nor E.O. 12333 (read together with PPD-28) provide the minimum safeguards required to meet the principle of proportionality and the surveillance programs established "cannot be regarded as limited to what is strictly necessary."

Second, the CJEU explained that Article 47 of the Charter required data subjects whose rights and freedoms were guaranteed by EU law to have an effective remedy before a tribunal. Data subjects were not granted rights actionable in the courts

against U.S. authorities and thus had no right to an effective remedy in relation to surveillance programs based on Section 702 of FISA or E.O. 12333. The CJEU further held that the introduction of a Privacy Shield Ombudsperson "cannot remedy the deficiencies" in relation to the judicial protection of persons whose personal data were transferred to the U.S. In particular, this was because:

- the Privacy Shield Ombudspersons' independence from the executive was undermined by the fact that the position was appointed by the Secretary of State, reported directly to the Secretary of State, and was an integral part of the U.S. State Department; and
- there was nothing in the Privacy Shield Decision that indicated the Ombudsperson had the power to adopt decisions that were binding on intelligence services and therefore did not ensure a cause of action before a body which offered data subjects' guarantees equivalent to those required under the Charter.

III. Implications For Organizations

The invalidation of the Privacy Shield and the qualifications of when SCCs can be relied upon have significant implications for controllers and processors who transfer data from the EU to third countries, in particular to the U.S.

First, companies relying exclusively on the Privacy Shield for transfers of data from the EU to the U.S. should examine their position and consider what alternative mechanisms they could rely on in order to transfer personal data lawfully to the U.S. The CJEU ruling does not have a grace period so its effect is immediate. In light of the reasons identified by the CJEU as to why the Privacy Shield (and previously Safe Harbor) is invalid, we suspect that a further version of a similar framework will be met with some skepticism by the relevant EU institutions and hence there are doubts as to the possibility of its implementation.

Second, in light of the Irish DPC's preliminary finding that the U.S. does not offer an adequate level of protection, and the CJEU's ruling that in circumstances where such finding exist the transfer must be suspended or terminated, we anticipate challenges for companies wishing to rely on SCCs for transfer of personal data from Ireland to the U.S. Transfers to other third countries under the SCCs should be examined on a case-by-case basis, preferably by the exporters of data (before the relevant DPA starts an investigation). Other transfer mechanisms should be considered and to the extent that SCCs must be relied upon, at a minimum, companies should be prepared to show that the provisions of the SCCs are being adhered to.

Third, we anticipate that the EDPB will be asked to harmonize the approach in relation to transfers of data to the U.S. Currently there is a real risk (and opportunity) that different EU Member States take a different view as to the validity of SCCs in relation to transfers to the U.S. We anticipate that any divergence will be short lived. The U.K.'s position will be closely watched once it leaves the EU at the end of this year.

1 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46 on the adequacy of the protection provided by the EU-U.S. Privacy Shield.

2 Note that an "adequacy decision" is a decision adopted by the Commission on the basis of the GDPR, which establishes that a non-EU country ensures an adequate level of protection of personal data by reason of its domestic law or the international commitments it has entered into.

3 For the other questions, the two high-level points are as follows. First, even though national security matters are outside the scope of EU law, the GDPR applies in certain circumstances where national security matters of

a third country are in play. Specifically, where personal data are transferred for commercial purposes from the EU to the U.S., the GDPR will apply to that transfer even if data could be processed for the purposes of public security, defense and state security by the authorities of the third country (rather than by the direct recipient of the data). Second, the CJEU provided guidance as to the factors to be taken into consideration by the relevant data protection authority (DPA) for the purposes of assessing whether that country ensures an adequate level of protection. Those factors should broadly correspond to the factors that the Commission needs to take into account when considering making an adequacy decision.

4 Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay. The Privacy Shield was also on the list prior to this judgment.

5 Commission Decision 2010/87/EU of 5 February 2010, on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016.