GIBSON DUNN

July 17, 2020

THE COURT OF JUSTICE OF THE EUROPEAN UNION STRIKES DOWN THE PRIVACY SHIELD BUT UPHOLDS THE STANDARD CONTRACTUAL CLAUSES UNDER CONDITIONS

To Our Clients and Friends:

On July 16, 2020, the Court of Justice of the European Union struck down as legally invalid the U.S.-EU Privacy Shield, which some companies have used to justify transfers of personal data from the EU to the U.S. The Court also ruled that the "Standard Contractual Clauses"("SCCs") approved by the European Commission, another mechanism many companies use to justify such transfers, remain valid with some caveats. The Court's decision will force companies on both sides of the Atlantic to reassess their data transfer mechanisms, as well as the locations in which they store personal data.

This Client Alert lays out the key aspects and implications of the decision.

I. Context of the Decision

As a reminder, under the General Data Protection Regulation ("GDPR"), a transfer of personal data out of the EU may take place only if the third country ensures an adequate level of data protection, as determined by a decision of the European Commission. In the absence of an adequacy decision, the exporter may proceed to such data transfer only if it has put in place appropriate safeguards, which may be provided for by the standard contractual clauses adopted by the Commission. However, in recent years, the validity of these safeguards has been under attack, with the Court's July 16 decision as the most recent significant milestone in that dispute. In large part these attacks have been based on concerns regarding U.S. government access to data on European residents transferred from the EU to the U.S.—concerns that became prominent following reports on government surveillance made public by former U.S. government contractor Edward Snowden.

In June 2013, Maximilian Schrems, a resident of Austria, lodged a complaint with the Irish supervisory authority, the Data Protection Commission ("DPC") in order to prohibit the transfer of his personal data from the European subsidiary of a social media company to the parent corporation in the U.S. Schrems claimed that U.S. laws and practices do not offer sufficient protection against surveillance by U.S. authorities in relation to data transferred to the U.S. That complaint was initially rejected by the DPC on the ground that, in its Safe Harbour Decision 2000/520, the European Commission had found that the U.S. ensured an adequate level of protection. However, in an October 6, 2015 ruling (the so-called "Schrems I case"[i]), the Court declared that the Safe Harbour Decision 2000/520 was invalid.

In response, the European Commission adopted Decision 2016/1250 of July 12, 2016 on the adequacy of the protection provided by the EU-U.S. Privacy Shield ("Privacy Shield") in order to replace the Safe Harbour Decision and to attempt to improve the guarantees afforded to the EU-U.S. data transfers.

In light of the Schrems I case, Schrems reformulated his complaint and sought the suspension/prohibition of data transfers to the U.S. based on the Standard Contractual Clauses, which had been approved by the Commission in 2010[ii].

The DPC took the view that the assessment of that complaint was conditional on the validity of the SCCs. The DPC thus brought proceedings before the Irish High Court, which in turn referred 11 questions to the Court for a preliminary ruling.

Thus, the principal issues before the Court were the viability of the SCCs and the Privacy Shield as mechanisms for the transfer of personal data from the EU to the U.S.

II. Validity of the Standard Contractual Clauses

The Court first confirmed that the GDPR applies to the transfer of personal data to a third country for commercial purposes, even if, at the time of that transfer or thereafter, that data may be processed by the authorities of the third country in question for the purposes of public security, defense and State security.

The Court found that data subjects must be afforded a level of protection essentially equivalent to that guaranteed by the EU's omnibus privacy law, the GDPR, read in light of the EU Charter of Fundamental Rights[iii]. The Court specified that the assessment of that level of protection must take into consideration both the contractual arrangements between the data exporter and the recipient and, as regards any access by the public authorities of that third country to the data transferred, the relevant aspects of the legal system of that third country.

As to the obligations of the local supervisory authorities within the EU (i.e., the data privacy regulators in individual EU Member States) in connection with such transfer, the Court held that, unless there is a valid Commission decision regarding the adequacy of the protections provided by the country to which the personal data is transferred, and where the data exporter established in the EU has not itself suspended or put an end to such a transfer, the relevant regulator must suspend or prohibit a data transfer pursuant to the SCCs if (i) the SCCs cannot be complied with in that country, and (ii) the protection of the data transferred required by EU law cannot be ensured by other means.

Upholding the validity of the SCCs, the Court found that the SCCs make it possible (i) to ensure compliance with the level of protection required by EU law and (ii) to suspend or prohibit transfers of personal data pursuant to such clauses in the event of breach of the clauses themselves or of it being impossible to honor them. The Court's finding hinged, in part, on the fact that the SCCs impose an obligation on both the data exporter and the data recipient to verify, prior to any transfer, whether that level of protection is complied with in the concerned third country. In addition, the SCCs require the data recipient to inform the data exporter of any inability to comply with the SCCs, the exporter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract.

Put simply, then, the Court found that the SCCs remain a valid mechanism for transfer of personal data out of the EU, though there is some uncertainty about the use of such a tool for transferring personal data to the U.S.

III. Invalidity of the Privacy Shield

In contrast to its ruling affirming the validity of the SCCs generally, the Court found that the EU-U.S. Privacy Shield is not compliant with the requirements arising from the GDPR, read in light of the EU Charter of Fundamental Rights.

The Court noted that the Privacy Shield enshrines the position that the requirements of U.S. national security, public interest and law enforcement have primacy, thus condoning interference with the fundamental rights of EU data subjects. In this regard, the Court found that the limitations on the protection of personal data arising from U.S. domestic law fail to meet the requirements of EU law, because U.S. law does not adequately limit the personal data that U.S. public authorities may access and use through surveillance programs.

In addition, the Court indicated that, although U.S. law lays down requirements with which the U.S. intelligence authorities must comply when implementing the surveillance programs in question, the relevant provisions do not grant data subjects actionable rights before the courts against the U.S. authorities. With respect the requirement of judicial protection, the Court held that the Ombudsperson mechanism[iv] referred to in the Privacy Shield does not provide data subjects with any cause of action before a body which offers guarantees essentially equivalent to those required by EU law, such as to ensure both the independence of the Ombudsperson and their power to adopt decisions that are binding on U.S. intelligence services.

Thus, the Court found that Privacy Shield is no longer a justifiable mechanism for transferring personal data from the EU to the U.S.

IV. Consequences

Given the invalidity of the Privacy Shield, companies that have to date used the Privacy Shield as a tool to transfer personal data from the EU to the U.S. should assess whether such transfers may be justified using other means. We hope that the European Data Protection Board ("EDPB")[v] will set a grace period to find an appropriate solution with U.S. authorities and allow companies to come into compliance, as was the case after the Schrems I ruling, when a three-month grace period was put in effect.

As the Court noted, the GDPR does provide for other mechanisms under which transfers of personal data to third countries may take place. However, such mechanisms cannot easily be implemented in practice (e.g., it may be difficult to obtain data subjects' consent).

Many companies have relied to date, and will likely continue to rely on the SCCs for making transfers outside the EU. However, companies must do more than simply adopt the SCCs: the Court specified that the controller established in the EU and the recipient of personal data outside the EU are both required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the relevant third country. In particular, the application of the SCCs to transfer personal data to the U.S. may be in question, as confirmed by the Irish DPC in its statement on the judgment of the Court of Justice of the EU.

It is difficult to predict how local supervisory authorities will respond to this uncertainty regarding the SCCs. One possibility is that supervisory authorities will assess independently the level of protection of data transferred to particular third countries, including the U.S. This would trigger significant legal uncertainty, in particular in the context of the EU-U.S. transfers. Alternatively, there may be a coordinated approach from the European supervisory authorities[vi], which may also, as suggested in the Court ruling, decide to request an opinion from the EDPB, which may adopt a binding decision.

It is also worth noting that the European Commission indicated in its report dated 24 June 2020 that it is currently working, in cooperation with the EDPB, on modernizing the mechanisms for data transfers, including the SCCs. Therefore, an updated version of the SCCs and associated guidance will likely be issued in the near future, adding yet another wrinkle to this issue.

While waiting for these future clarifications and decisions, in light of the above, we recommend companies currently relying on the Privacy Shield or SCCs consult with their data protection officer or counsel to evaluate tailored ways to minimize the risks associated with continued transfers of personal data out of the EU—particularly transfers of such data to the U.S.

---

[i] Judgment of the Court of 6 October 2015 - Maximillian Schrems v Data Protection Commissioner (Case C-362/14).

[ii] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, as amended.

[iii] The Charter of Fundamental Rights brings together all the personal, civic, political, economic and social rights enjoyed by people within the EU in a single text.

[iv] The Privacy Shield Ombudsperson is a Privacy Shield mechanism to facilitate the processing of and response to requests relating to the possible access for national security purposes by U.S. intelligence authorities to personal data transmitted from the EU to the U.S.

[v] It is worth noting that, with respect to the Privacy Shield, in January 2019 the EDPB stated in its second annual joint review of the Privacy Shield that it "*welcomes the efforts made by the US authorities and the Commission to implement the Privacy Shield, […] However, the EDPB still has a number of significant concerns that need to be addressed by both the Commission and the US authorities*".

[vi] The Irish DPC has specified that it looks forward "*to developing a common position with [its] European colleagues to give meaningful and practical effect to today's judgment*". Also, the German Federal Commissioner for Data Protection and Freedom of Information already stated that it will coordinate with its European colleagues. It is also noting the U.S. Secretary of Commerce expressed disappointment but has yet to articulate how the Department will move forward. "*While the Department of Commerce is deeply disappointed that the court appears to have invalidated the European*

Commission's adequacy decision underlying the EU-U.S. Privacy Shield, we are still studying the decision to fully understand its practical impacts," said Secretary Wilbur Ross.

The following Gibson Dunn lawyers prepared this client alert: Ahmed Baladi, Ryan T. Bergsieker, James A. Cox, Patrick Doris, Penny Madden, Alexander H. Southwell, Michael Walther, Kai Gesing, Alejandro Guerrero, Vera Lukic, Sarah Wazen, Adelaide Cassanet, Clemence Pugnet and Selina Grün. Please also feel free to contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the Privacy, Cybersecurity and Consumer Protection Group:

Europe

Ahmed Baladi - Co-Chair, PCCP Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox - London (+44 (0)20 7071 4250, jacox@gibsondunn.com)
Patrick Doris - London (+44 (0)20 7071 4276, pdoris@gibsondunn.com)
Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Alejandro Guerrero - Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic - Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen - London (+44 (0)20 7071 4203, swazen@gibsondunn.com)

Asia

Kelly Austin - Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Jai S. Pathak - Singapore (+65 6507 3683, jpathak@gibsondunn.com)

United States

Alexander H. Southwell - Co-Chair, PCCP Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Debra Wong Yang - Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin - New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Howard S. Hogan - Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen - Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley - San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon - Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson - Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Deborah L. Stein (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner - Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong - San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)