Hughes Hubbard & Reed

The EU-U.S. Privacy Shield Is Invalid: What Now?

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

July 27, 2020 - On July 16, 2020, the Court of Justice of the European Union ("CJEU") issued its long-awaited judgment in Case C-311/18 ("*Schrems II*"). The CJEU held that transfers to non-EU countries must afford EU data subjects a level of protection essentially equivalent to that guaranteed within the EU. The court found that the European Commission's standard contractual clauses ("SCCs") meet this standard, even though they do not bind the authorities of the non-EU country. However, the CJEU invalidated the EU-U.S. Privacy Shield on the ground that the United States failed to ensure equivalent protections. In particular, the court considered that certain U.S. government surveillance programs fail to limit themselves to what is strictly necessary or grant EU data subjects actionable rights.

What Schrems II Changes for EU-U.S. Data Transfers

The Privacy Shield Is No Longer Valid

Following the CJEU's judgment, the Privacy Shield is no longer a basis for EU-U.S. transfers. The CJEU's judgment is effective immediately, and there is no grace period. The European Commission has announced that it is already speaking with U.S. authorities "to develop a strengthened and durable transfer mechanism," but there is no telling how long this might take.

The Use of Standard Contractual Clauses Is Unclear

In the absence of the Privacy Shield, the first instinct of many companies may be to enter into SCCs or binding corporate rules for EU-U.S. transfers. However, the use of these safeguards is presently unclear pending further guidance from the European Commission and the national data protection authorities in the EU. The CJEU found that the SCCs are valid in principle, but its decision raises questions about whether companies can comply with their requirements in the context of EU-U.S. transfers.

Initial Guidance from EU Authorities

The European Commission has expressed support for the continuing use of SCCs. At a press conference following the CJEU judgment, Vice-President Vera Jourová, stated, "The Court of Justice declared the Privacy Shield decision invalid, but also confirmed that the standard contractual clauses remain a valid tool for the transfer of personal data to processors established in third countries. This means that the transatlantic data flows can continue, based on the broad toolbox for international transfers provided by the GDPR, for instance binding corporate rules or Standard Contractual Clauses."

The reaction of the national data protection authorities has been mixed. The data protection authorities in France, the UK, the Netherlands and Denmark released press statements to the effect that they are still analyzing the full consequences of the *Schrems II* judgment. The Irish Data Protection Commissioner noted that, "in practice, the application of the SCCs transfer mechanism to transfers of personal data to the United States is now questionable. 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."

In Germany, the Federal Commissioner for Data Protection announced that transfers to the United States are still possible but require additional safeguards. The Berlin data protection authority stated that transfers to the United States are currently not possible and encouraged controllers to use service providers within the EU. The Hamburg data protection authority appears to take a similar position, noting that the CJEU's reasons for invalidating the Privacy Shield also apply to the SCCs, and that the SCCs are, therefore, equally unsuitable to protect those affected.

On July 23, 2020, the European Data Protection Board (EDPB) published FAQs. With respect to the use of SCCs for EU-U.S. transfers, the EDPB noted that the CJEU found that U.S. law does not ensure an essentially equivalent level of protection. The EDPB advised, "Whether or not you can transfer personal data on the basis of SCCs will depend on the result of your assessment, taking into account the circumstances of the transfers, and supplementary measures you could put in place. The supplementary measures along with SCCs, following a case-by-case analysis of the circumstances surrounding the transfer, would have to ensure that U.S. law does not impinge on the adequate level of protection they guarantee."

Pending further guidance, the situation in the EU is presently unclear. The CJEU judgment has thrown EU-U.S. data transfers into a state of confusion, and both EU and U.S. authorities are studying the situation. Meanwhile, companies on both sides of the Atlantic are wondering what, if anything, they should be doing. We have provided some recommendations below.

What Can Be Done

1. Do Not Wait

Companies transferring the personal data of EU residents to the United States should review the legal basis for those transfers in light of the CJEU's reasoning in *Schrems II* and the guidance referred to above. This is particularly important for companies that have been relying on the EU-U.S. Privacy Shield. The Privacy Shield is no longer a basis for EU-U.S. transfers.

Given the current confusion, companies may be tempted to wait until there is more clarity. Indeed, there are many who think that the national data protection authorities in the EU will refrain from enforcement activities until there is a new transatlantic mechanism in place. However, there is no guarantee that these data protection

authorities will wait and the Federal Commissioner for Data Protection in Germany has already stated that it will "urge rapid implementation [of the *Schrems II* decision] in particularly relevant cases."

In the absence of clear guidance from the European authorities, waiting for the next compromise between the European Commission and the United States may carry significant risk. The data protection authorities in the EU are empowered to prevent ongoing transfers, require transferred information to be destroyed or returned, and/or impose monetary sanctions or fines.

2. Add Supplementary Protections to SCCs

In the absence of the Privacy Shield, many companies may turn to SCCs. In *Schrems II*, the CJEU noted that it may be necessary to supplement the SCCs to ensure an adequate level of protection. As the CJEU stated, "It is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection . . . by providing, where necessary, additional safeguards to those offered by those clauses."

Given the uncertainty regarding the SCCs, EU data exporters and U.S. importers should consider adding supplemental protections to them. There may be little, if anything, a U.S. importer can do to protect the transferred data from U.S. government surveillance programs, but any protections that can be added may help the parties in the event that a supervisory authority questions a particular transfer. It is not clear what protections need to be added, but *Schrems II* indicates that, in appropriate cases, a U.S. importer might be able to:

- declare that it has no reason to believe that any EU data subjects affected by the transfer are subject to U.S. government surveillance programs;
- declare that it has no reason to believe its national law would prevent it from fulfilling its obligations under the SCCs as amended;
- undertake to implement additional technical and organizational measures to ensure the security of the data (such as the use of encryption or token transmission);
- undertake to verify and to inform the EU data exporter of the existence of local laws that may compromise the security of the data;
- undertake to immediately inform the EU data exporter if it becomes aware of any changes in legislation or regulations that may have negative consequences for the guarantees and obligations offered by the SCCs as amended; and/or
- if it is compelled to disclose personal data to governmental authorities, undertake to inform the EU data exporter of its inability to comply with the SCCs as amended.

3. Use Article 49 Derogations Whenever Possible

Companies making EU-U.S. transfers should also consider whether they can rely on one of the derogations contained in Article 49 of the GDPR. The *Schrems II* decision does not affect these derogations, which permit the transfer of data regardless of whether there is an adequate level of protection. Indeed, the CJEU noted that it was not necessary to stay the effects of its decision "in view of Article 49 of the GDPR." The Article 49 derogations may be available for, among others, transfers made with explicit consent or transfers that are necessary for the performance of contracts, for important reasons of public interest, or for the establishment, exercise or defense of legal claims.

4. U.S. Data Recipients Should Continue to Follow the Privacy Shield Principles

The U.S. Department of Commerce has stated that it will continue to administer the Privacy Shield program in the United States. It is not clear what this means, but both the Commerce Department and the U.S. Federal Trade

Commission have indicated that the *Schrems II* ruling does not release U.S. Privacy Shield participants from their existing obligations.

With respect to data already transferred to the United States, U.S. data recipients should continue to adhere to the Privacy Shield Principles. Among other things, this means maintaining reasonable and appropriate security measures, as well as policies and procedures that respect the rights of EU data subjects and ensure accountability for onward transfers. U.S. data recipients should also maintain their Privacy Shield website notices, subject to any adjustments that may be needed to reflect the *Schrems II* ruling.

5. Document Efforts to Ensure Adequate Protections

Companies engaged in EU-U.S. data transfers should document their efforts to ensure that they are providing EU data subjects with protections that are essentially equivalent to those guaranteed by EU law. This applies to the transfers themselves and to other aspects of GDPR compliance. We could be heading into a period of increased regulatory scrutiny and NGO activism, and well-documented compliance efforts will be invaluable in the event of legal action by data protection authorities in the EU and/or interested parties such as NGOs.

6. Monitor the Data Protection Authorities

The situation in the EU remains fluid, and there will be further guidance on EU-U.S. data transfers. The European Commission, the EDPB, and the national data protection authorities in the EU are expected to make further statements regarding the impact of the *Schrems II* ruling. There could also be further questions referred to the CJEU for rulings that may clarify *Schrems II*. EU data exporters and U.S. data importers need to monitor further developments and adjust their compliance programs accordingly.

This client advisory and our recommendations are not intended as legal advice. Our recommendations reflect what we believe to be best practices, based on the currently existing guidance from EU and U.S. authorities. Companies involved in EU-U.S. data transfers should consider their responsibilities and obligations on a case-by-case basis, taking into account the specific circumstances and guidance from the relevant data protection authorities.

For assistance with EU-U.S. data transfers, please contact any of the Hughes Hubbard attorneys listed below.

Stefan Naumann | Partner
Hughes Hubbard & Reed LLP
4 rue Cambacérès | 75008 Paris, France
Office +33 (0) 1 44 05 80 60 | Cell +33 (0) 6 64 10 33 06
stefan.naumann@hugheshubbard.com | bio

Seth D. Rothman | Partner
Hughes Hubbard & Reed LLP
One Battery Park Plaza | New York, NY 10004-1482
Office +1 (212) 837-6872 | Cell +1 (917) 697-8093
seth.rothman@hugheshubbard.com | bio

Elsa Malaty | Associate
Hughes Hubbard & Reed LLP
4 rue Cambacérès | 75008 Paris, France
Office +33 (0) 1 44 05 80 18 | Cell +1 (929) 253-5120
elsa.malaty@hugheshubbard.com | bio

Related People

Stefan Naumann

Seth D. Rothman

Elsa Malaty

Related Areas of Focus

Data Privacy & Cybersecurity