EU DATA PROTECTION: PRIVACY SHIELD SHATTERED BY THE SWORD OF EUROPEAN JUSTICE - WHAT COMES NEXT FOR TRANSATLANTIC DATAFLOWS?

Date: 17 July 2020

Data Protection, Privacy, and Security Alert

By: Claude-Étienne Armingaud, Natali Adison, Dr. Thomas Nietsch, Martin Fokken

In a highly anticipated *Schrems II* decision,[1] the Court of Justice of the European Union (CJEU) invalidated the Privacy Shield, the legal framework allowing transatlantic exchanges of personal data for commercial purposes between the European Union and the United States, mainly citing U.S. surveillance practices and inadequate recourse to EU individuals. On the other hand, the CJEU upheld the Commission Decision 2010/87 on Standard Contractual Clauses (SCCs) for the transfer of personal data to processors established in third countries (see our alert here).

THE SCHREMS SAGA

Max Schrems, the Austrian “datactivist” whose name is already associated to the CJEU decision (*Schrems I*) which invalidated the Safe Harbour mechanism on 06 October 2015 (see our coverage here), had filed a complaint to the Irish Data Protection Authority, the Data Protection Commissioner (DPC), regarding Standard Contractual Clauses and the Privacy Shield mechanism.

In a surprising procedural move, further to its investigation, the DPC filed a lawsuit in order to call upon the Irish High Court to issue another reference to the CJEU. The Irish High Court summarized the factual findings, highlighting that the United States were implementing "mass processing" of personal data and referred eleven interpretive questions to the CJEU on 13 April 2018.

On 19 December 2019, the Advocate General (AG) of the CJEU, issued a non-binding advisory opinion on the matter, advising the CJEU to declare the SCCs valid and, while dedicating a dozen pages of its opinion to criticizing the Privacy Shield, he concluded that there was no need to examine its validity.

THE CJEU DECISION INVALIDATING THE PRIVACY SHIELD

The CJEU only partly followed the AG's opinion; by finding that the limitations on the protection of personal data arising from the domestic law of the United States, more in particular the U.S. public authorities' use and access of EU data, are not circumscribed in accordance with the proportionality principle, bearing in mind that the surveillance programs based on those provisions are not limited to what would be deemed “strictly necessary.” In simple terms, this means that the CJEU found that the United States were engaging in overreaching surveillance, incompatible with the European level of data protection.

Furthermore, the CJEU reiterated the importance of the availability of an effective administrative and judicial redress for data subjects whose personal data is being transferred. Consequently, the CJEU found the legal procedures available to Europeans, regarding the processing of their data once transferred to the United States, were insufficient, on the basis that there was no such procedure available to non-U.S. citizens.

In addition, as to the requirement of judicial protection, the CJEU found that the Ombudsperson mechanism, referred to in the Privacy Shield and implemented further to complex negotiations between the United States and the EU, did not guarantee the independence of the Ombudsperson nor indicated that the Ombudsperson had the power to adopt decisions which would be binding on the U.S. intelligence services. Consequently, the Privacy Shield did not mention any legal safeguards providing data subjects with any cause of action before a body which offers guarantees essentially equivalent to those required by EU law.

The immediate consequence of the Schrems II decision is the immediate need for the nearly 5,000 U.S.-based companies relying on Privacy Shield to transfer personal data from the EU to the United States to amend their existing data protection process and rely on another instrument, such as the SCCs (see here) or Codes of Conducts (see here).

THE REACTION OF THE EU INSTITUTIONS

The European Commission (EC) promptly reacted to the decision of the CJEU. In a press conference on the same day of the ruling, the Vice-President of the EC, Věra Jourová, and the Commissioner for Justice Didier Reynders, explained how the EC was already planning to ensure the continuity of safe data flows.

In particular, they clarified that the EC was now following three priorities:

1. guaranteeing that the data of EU individuals were protected when transferred across the Atlantic;
2. ensuring the continuation of personal data flows, while working constructively with their American counterparts; and
3. working with the European Data Protection Board (EDPB) and each of the Member States Supervisory Authorities, to ensure the adequacy of the international data transfer toolbox.

According to Commissioner Jourová, the transatlantic data flow can continue, based on the broad toolbox for International transfers provided by the GDPR (e.g. Binding Corporate Rules or SCCs).

The EC is planning to work with the EDPB as well as the remaining 27 EU Member States, in order to update the SCCs as soon as possible. However, the EC still needs to assess the consequences of the invalidation of the Privacy Shield. In the meantime, transatlantic dataflows between companies may take place, based on the other mechanisms for International data transfers of personal data, available under the GDPR.

THE REACTION OF THE UNITED STATES DEPARTMENT OF COMMERCE

The Secretary of the U.S. Department of Commerce, Wilbur Ross, promptly released a press release in response to the *Schrems II* decision, expressing its deep disappointment with the decision. The statement indicates that the decision creates significant negative consequences to the transatlantic economic relationship that is vital for businesses of all sizes and sectors.

It further states that the Department of Commerce will continue to administer the Privacy Shield program, including processing submissions for self-certification and re-certification to the Privacy Shield framework and maintaining the Privacy Shield List as the Schrems II decision does not relieve participating organizations of their Privacy Shield obligations.

THE IMMEDIATE IMPACTS AND NEXT STEPS

The first political impact is that, less than five years after the invalidation of Safe Habor, the U.S. Government and the EU Commission will again need to engage in new negotiations eventually leading to a new agreement.

However, given that the Privacy Shield is no longer a suitable guarantee to legitimize data transfers to the United States within the meaning of the GDPR, companies which used to rely on it, or on business partners that relied on it, will need to find another legal ground to render such international data transfer lawful, or face potential fines up to EUR 20 million or 4% of their global annual turnover.

Ultimately, it remains to be seen how the EDPB and Member States Supervisory Authority will react: will they grant a grace period for companies relying on the Privacy Shield to move toward alternative mechanism or directly enforce GDPR due to lack of legal basis for data transfers for the US? Will they will provide guidance with regard to countries where the Standard Contractual Clauses are not sufficiently honored and thus cannot serve as means to justify data transfers to these countries? In any case, companies will want to review available options without waiting for such positions to be published.

Such other mechanisms may include, *inter alia*:

- Relying on one of the derogations provided under Art. 49 GDPR, namely
  - Consent of the data subject to the transfer, with a consent compliant with GDPR requirements;
  - Necessity for the performance of a contract executed with or in the interest of the data subject;
  - Necessity for important reasons of public interest;
  - Necessity for the establishment, exercise or defence of legal claims; and
  - Necessity to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.
- Adopting binding Corporate Rules, which would require substantial investments in time, human resources and costs and only address data transfers within the same corporate group;
- Executing Standard Contractual Clauses, which were also affected by the Schrems II decision (see our alert here); or
- Developing Codes of Conduct with a given industry (see our alert here), which may become the unlikely beneficiary of the Schrems II decision.

K&L Gates global data protection team (including in each of our European offices) remains available to assist you in achieving the compliance of your data transfers at global levels.

FOOTNOTES

[1] Court of Justice of the European Union - Grand Chamber - 16 July 2020 - C-311/18 - *Schrems II*

KEY CONTACTS

CLAUDE E. ARMINGAUD
PARTNER
PARIS
+33.(0)1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM

NATALI ADISON
ASSOCIATE
BRUSSELS
+32.(0)2.336.1934
NATALI.ADISON@KLGATES.COM

THOMAS NIETSCH
SENIOR ASSOCIATE
BERLIN
+49.(0)30.220.029.408
THOMAS.NIETSCH@KLGATES.COM

MARTIN FOKKEN
ASSOCIATE
BERLIN
+49.(0)30.220.029.405
MARTIN.FOKKEN@KLGATES.COM

