SIDLEY

The End of the Swiss-U.S. Privacy Shield?

William Long and Sabrine Schnyder

Introduction

Following the Court of Justice of the European Union's (CJEU) decision in *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems* (*Schrems II*), the Swiss Federal Data Protection and Information Commissioner (FDPIC) concluded in a position paper published on September 8, 2020, that the Swiss-U.S. Privacy Shield no longer provides a valid mechanism for the transfer of personal data from Switzerland to the United States. With these two decisions, transfer of personal data from Switzerland to the United States is put at jeopardy, and organizations based in Switzerland are well advised to reassess their compliance with Swiss data protection requirements.

I. DATA TRANSFERS ABROAD UNDER SWISS LAW – A BRIEF REMINDER

1. Under the Swiss Data Protection Act (DPA), organizations cannot transfer personal data from Switzerland to countries (including the United States, China, India, and many other non-European countries) that have not yet been deemed by the FDPIC to provide adequate protection for personal data (cf. FDPIC's country list) unless one of the legal transfer mechanisms stipulated in the law (e.g., data transfer agreements or consent) applies to such transfer (cf. Article 6 DPA).

2. To facilitate commercial relationships and the exchange of personal data, the Swiss government enacted the Swiss-U.S. Privacy Shield as a valid legal transfer mechanism to comply with legal requirements when transferring personal data from Switzerland to the United States. To date, more than 3,000 organizations rely on the Swiss-U.S. Privacy Shield.

3. Following the *Schrems II* decision, the FDPIC published its position paper on September 8, 2020, and concluded that the Swiss-U.S. Privacy Shield no longer provides a valid legal transfer mechanism for cross-border exchange of personal data from Switzerland to the United States.

II. SCHREMS II AND THE FDPIC'S POSITION PAPER IN A NUTSHELL

4. On July 16, 2020, the CJEU invalidated the EU-U.S. Privacy Shield (which mirrors the Swiss-U.S. Privacy Shield) with immediate effect so that personal data can no longer be transferred from the EU to the United States based on this legal transfer mechanism.

5. The CJEU based its ruling mainly on the argument that U.S. national security authorities (e.g., National Security Agency, Federal Bureau of Investigation, Central Intelligence Agency) access personal data in bulk without limiting collection to what is "strictly necessary" and thereby disregarding the principle of "proportionality."

6. In addition, the CJEU raised concerns that there is a lack of adequate means of redress for EU citizens to act against the collection of their personal data by these U.S. governmental institutions. In particular, the CJEU deemed the Ombudsman, which had been put in place as a means of redress in the EU-U.S. Privacy Shield, as not sufficient.

7. The FDPIC followed the CJEU's opinion and ruled that Swiss-U.S. Privacy Shield no longer constitutes a valid data transfer mechanism for transfer of personal data from Switzerland to the United States.

8. On a positive note, the CJEU confirmed the validity of the use of standard contractual clauses (SCCs), a form of international data transfer agreements made available for use by the European Commission, as a valid legal transfer mechanism.

9. However, the CJEU also held that organizations are required to put in place additional safeguards where SCCs alone would not guarantee a level of protection of personal data equivalent to the GDPR, for example, because SCCs would not prevent surveillance authorities in the receiving country to access personal data.

10. This basically puts the responsibility on the data controller to verify the law and the level of protection of personal data in the destination country on a case-by-case basis and adapt the SCCs where necessary. Also, according to the CJEU's judgment, the receiving party is obligated to immediately inform the data controller if it can no longer adhere to the contractual obligations under the SCCs.

11. In case such additional contractual measures cannot ensure such protection, or the receiving party breaches the SCCs, the data controller or processor is required to suspend or end the transfer of personal data.

12. Further, while the FDPIC has not yet opined on the validity of the use of SCCs and in particular the need to implement additional safeguards to protect personal data transferred to certain third countries (e.g., China, India, and the U.S.), given the CJEU's judgment in *Schrems II* and the subsequent guidance published by the European Data Protection Board, we expect that this will also become necessary under Swiss law. The FDPIC stated that it will soon publish further guidance.

III. WHAT SHOULD COMPANIES DO?

13. For organizations in the EU and organizations in Switzerland that are subject to GDPR, the *Schrems II* decision is applicable immediately.

14. For organizations in Switzerland that are not subject to GDPR, the *Schrems II* decision has no direct impact. The Swiss-U.S. Privacy Shield remains in force as it has not been formerly invalidated by the Swiss Federal Council. Also, there is to date no court decision confirming the FDPIC's view. However, with the ruling of the FDPIC, transfer of personal data from Switzerland to the United States based on the Swiss-U.S. Privacy Shield brings major legal risks. Hence, organizations in Switzerland are well advised to start looking for alternative transfer mechanisms.

15. In particular, we recommend the following:

- Closely monitor the developments in Switzerland and the EU. More and more regulators are publishing their commentaries and thoughts on *Schrems II*. In fact, the FDPIC stated that it will soon publish further guidance. Also, the European Commission is proposing to release updated versions of SCCs so as to reflect the CJEU's views in *Schrems II* and GDPR requirements. It remains to be seen how long this will take and if these updated SCCs will, in and of themselves, provide the supplementary privacy protections alluded to in *Schrems II*.

- Conduct an assessment of the third countries outside of Switzerland and the EU to which personal data is transferred (through both a factual analysis of personal data flows and analysis of the applicable legal transfer mechanisms) and whether the legal transfer mechanism they use is sufficiently protective under the GDPR and/or Swiss law and in light of the CJEU's decision in *Schrems II* and the FDPIC's position paper.

- Consider alternatives to permit the transfer of personal data to third countries outside of Switzerland and the EU under Article 6(2) of the DPA, for example consent or where the transfer is necessary for performance of a contract.