EU Privacy Earthquake:

Can U.S. Companies Comply With GDPR After "Schrems II"?

By David S. Greber, **CIPP/E, CIPP/US, CIPM**

August 2020

Every United States business that uses personal data of European data subjects would do well to revisit *immediately* its strategy for complying with European privacy law.

On July 16, 2020, the Court of Justice of the European Union ("CJEU") issued its decision in Data Protection Commission vs. Facebook Ireland, Max Schrems (Case C-311/18) ("Schrems II"), invalidating one of the primary legal grounds for importing European data into the United States and leaving the viability of the other two primary methods in some doubt. Here's what happened and what I think U.S. businesses should consider doing about it.

Pre-Shrems II Basis for Transfer of Personal Data to the U.S.

Europe's General Data Protection Regulation (the "GDPR") is one of several laws, charters, conventions, directives, and regulations that protect the privacy of European data subjects. In Europe, privacy is considered a fundamental human right. In general, Chapter V of the GDPR only allows transfers of European personal data outside the European Union ("EU") to countries determined by the European Commission (the "Commission") to provide adequate legal protection "to ensure that the level of protection of natural persons guaranteed by . . . [GDPR] is not undermined." GDPR Article 44.

Before Schrems II, one or more of three mechanisms approved by the Commission were usually used by U.S. businesses to meet the requirements of Article V (under appropriate circumstances):

1. EU-U.S. Privacy Shield ("Privacy Shield"). In 2016, the Commission determined[1] that a program established by the U.S. Department of Commerce called the EU-U.S. Privacy Shield program would, together with other safeguards present in the American legal system, provide adequate safeguards to guarantee EU data subjects privacy protections, judicial remedies, and access to independent judicial review that were essentially

[1] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 (the "Privacy Shield Decision"), p. 32.

equivalent[2] to what was then provided to them under EU law.[3] U.S. businesses participating in the program would be permitted to import EU personal data into the United States.

2. Standard Contractual Clauses ("SCC"). U.S. businesses could receive EU personal data under approved contract terms known as "Standard Contractual Clauses" through which the U.S. businesses would agree, among other things and in essence, to handle the EU data in a manner consistent with the rights and protections afforded the data subject under the GDPR. If U.S. legislation is likely to have a substantial adverse effect on the warranties and obligations provided in the SCC, then the SCC and the GDPR require the suspension or termination of data transfer (unless another lawful basis of personal data export can be found).

3. Binding Corporate Rules ("BCR"). U.S. businesses that have affiliated companies, some of which are established in the EU and some of which are not, may transfer data between those companies if the companies transferring and receiving the data adopt approved internal data protection policies called Binding Corporate Rules. The BCR must:

    a. Include all EU general data protection principles and enforceable rights to ensure appropriate safeguards for the EU personal data transfers;

    b. Contain the elements required by GDPR Article 47.2;

    c. Be approved by the appropriate EU supervisory authority;

    d. Be legally binding on the companies;

    e. Expressly confer rights on the data subjects to enforce the BCR by complaint to the competent supervisory authority and to the courts; and

    f. Include a mechanism for reporting to the competent supervisory authority any legal requirements to which a member of the group of businesses is

[2] At the time the Commission was concerned about the privacy implications of U.S. government interference with the rights of EU data subjects through U.S. surveillance of European personal data under Section 702 of the U.S. Foreign Intelligence Surveillance Act ("FISA"), Presidential Policy Directive 28 ("PPD-28"), and Presidential Executive Order 12333. It resolved these concerns in part by allowing a U.S. "Privacy Shield Ombudsperson" to serve as an intermediary and conduit for EU privacy complaints and by accepting certain assurances from the U.S. government concerning its processing of EU personal data.

[3] The decision was issued before the effective date of the GDPR. It continued in force under the GDPR until Schrems II. The EU privacy law that controlled at the time the decision was originally issued was Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (the "Directive).

subject in a third country that are likely to have a substantial adverse effect on the guarantees provided by the BCR.

If the third country (e.g. the United States) has laws that make it impossible to fulfill the privacy protection promises made in the BCR, then BCR cannot be used as a basis for transfer of EU personal data to the United States.

Background to the Schrems II Decision

Schrems II represents the second difficult judicial round in the Commission's efforts to construct a viable adequacy determination that would allow the transfer of EU personal data to the United States. The United States' comparatively weak protections of personal data privacy and U.S. government surveillance programs make this a challenge. So has the determined opposition of EU data subject Maximillian Schrems ("Schrems"). Schrems has complained twice that the Commission's adequacy determinations concerning transfers of personal data to the U.S. violate European privacy law. The CJEU has agreed with Schrems both times.

Both of the Schrems complaints were made initially to the Data Protection Commissioner for Ireland (the "DPC") about the transfer of Schrems' Facebook data from Facebook Ireland Limited to Facebook, Inc. in the United States.

In Schrems I,[4] Facebook had transferred personal data in reliance on the Commission's 15-year-old "Safe Harbour Decision," [5] in which the Commission had determined that U.S. privacy protections under the U.S. Department of Commerce's "Safe Harbour" program—the predecessor to the current Privacy Shield program—were adequate for the purpose of allowing EU personal data to be transferred to the U.S. Following the disclosure in June 2013 by former U.S. National Security Agency contractor Edward Snowden of U.S. surveillance activities, Schrems complained to the DPC that his Facebook data transferred to the U.S. would be exposed to these surveillance activities, which could not be legitimized by the Safe Harbour Decision. Although the DPC refused to investigate, the Irish High Court and the CJEU essentially agreed with Schrems, resulting in the CJEU's invalidation of the Commission's Safe Harbour Decision. Front and center in the CJEU's Schrems I decision were concerns that U.S. government surveillance activities endangered the privacy rights of EU data subjects whose data were transferred to the United States.

After Schrems I, several important events occurred in fairly quick succession, which contribute to my belief that SCC and BCR are not far behind the Privacy Shield in

[4] Judgment of the Court of Justice of the European Union dated October 6, 2015, Data Protection Commission vs. Facebook Ireland, Max Schrems (Case C-362/14)("Schrems I").
[5] Commission Decision of 26 July 2000 (2000/520/EC)(the "Safe Harbour Decision").

being rendered useless to U.S. businesses (although still technically valid under European law):

- **October 6, 2015**: Schrems I decided by CJEU.

- **October 20, 2015**: Irish High Court quashed the DPC's refusal to investigate the Schrems complaint and remitted the complaint to the DPC for investigation.

- The DPC immediately opened a Schrems investigation.

- **November 1, 2015**: Facebook was notified of the DPC investigation. Facebook subsequently justified its continued transfer of data after Schrems I based on the use of SCC in an agreement between Facebook Ireland Limited and Facebook, Inc. of November 2016.

- **December 1, 2015**: At the invitation of the DPC, Schrems submitted a revised complaint to the DPC, requesting that the DPC suspend Facebook Ireland's transfer of data to the United States.

- **May 24, 2016**: The DPC issued a draft decision in the Schrems II matter, tentatively finding Facebook's data transfer unlawful based on the threat to EU data privacy posed by U.S. government surveillance activity. The DPC stated that the SCC Decision should arguably be held invalid in light of these considerations. The DPC also announced her immediate referral of the Schrems case to the Irish High Court to determine the validity of SCC as a basis for transfer of EU personal data to the U.S. The DPC considered the draft Privacy Shield Decision circulated by the Commission in forming her opinion in her draft decision.

- **July 12, 2016**: The Commission issued its new adequacy determination in its Privacy Shield Decision.

- **December 16, 2016**: The Commission amended its SCC Decision in light of the holding in Schrems I.

- **October 3, 2017**: The Irish High Court issued a 153-page decision tending to agree with the positions of the DPC in her draft decision and referring 11 questions to the CJEU for decision, including whether the SCC Decision remains valid.

The arguments of Maximillian Schrems, and the findings of the DPC and the Irish High Court, are at least implicitly founded on their convictions that the dangers posed by U.S. surveillance activity are pervasive and cannot be adequately mitigated to conform to EU

privacy standards in the current U.S. legal environment. Not by Privacy Shield, nor by SCC, nor by BCR. For example, in her draft decision in Schrems II, the DPC said:[6]

> It is also my view that the safeguards purportedly constituted by the standard contract clauses set out in the Annexes to the SCC Decisions do not address the CJEU's objections concerning the absence of an effective remedy compatible with the requirements of Article 47 of the Charter, as outlined in Schrems. **Nor could they.** On their terms, the standard contract clauses in question do no more than establish a right in contract, in favour of data subjects, to a remedy against either or both of the data exporter and importer. Importantly for current purposes, there is no question but that the SCC Decisions are not binding on any US government agency or other US public body; nor do they purport to be so binding. It follows that they make no provision whatsoever for a right in favour of data subjects to access an effective remedy in the event that their data is (or may be) the subject of interference by a US public authority, whether acting on national security grounds, or otherwise.

It is not obvious how supplemental measures by the data controller and the data processor could cure these problems.

Similarly, in referring the case to the CJEU, Justice Costello of the High Court Commercial of Ireland said:[7]

> [I]t is arguable that the limitations on the exercise of the right to an effective remedy before an independent tribunal, as required by Article 47, for EU citizens whose data privacy rights are infringed by the intelligence agencies are not proportionate or necessary or needed to protect the rights and freedoms of others. Neither the introduction of the Privacy Shield Ombudsperson mechanism nor the provisions of Article 4 of the SCC decisions eliminate the well-founded concerns raised by the DPC in relation to the adequacy of the protection afforded to EU data subjects whose personal data is wrongfully interfered with by the intelligence services of the United States once their personal data has been transferred for processing to the United States.

U.S. federal statutory reform may be required to address these concerns satisfactorily.

The Schrems II Decision

[6] Draft Decision of the Data Protection Commissioner of Ireland dated May 24, 2016, Mag. Maximillian Schrems v. Facebook Ireland Limited (Ref. 3/15/766), pp. 29-30, para. 61 (emphasis added).

[7] Judgment of the High Court Commercial of Ireland dated October 3, 2017, Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (2016 No. 4809 P.)(Ms. Justice Costello), p. 152, para 334.

Following are the CJEU holdings in Schrems II and some of the implications of the holdings:

1. The Privacy Shield Decision is invalid.[8]

   Implications: Under the GDPR, businesses that relied on the Privacy Shield Decision as the legal basis for transfer of EU personal data into the United States must either stop the transfers immediately or find another lawful basis for the transfer. If transfer continues or resumes after suspension, the data controller may have to notify the applicable supervisory authority of the continued transfer. The supervisory authority might conduct an audit to determine whether the proposed transfer should be suspended or prohibited in order to ensure an adequate level of protection.[9]

2. Althought SCC's remain valid,[10] they are not necessarily sufficient to transfer personal data to a third country, particularly "where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates."[11]

   The decision affirms the obligations of the controller and processor to address the problem. Under Article 46(1) of the GDPR, controllers and processors must "compensate for the lack of data protection in a third country" in order to "ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union."[12] The level of protection must take into account not only the SCC but also "the relevant aspects of the legal system of the third country" set out in a non-exhaustive manner in Article 25(2) of the GDPR.[13] "Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses."[14] Whether the supplemental protections will be sufficient to provide the level of protection required by EU law must be assessed on a case-by-case basis.[15]

   Implications: When it comes to proving adequate protections under GDPR, controllers and processors who transfer EU personal data to the United States

[8] Judgment of the Court of Justice of the European Union dated 16 July 2020, Data Protection Commission vs. Facebook Ireland, Max Schrems (Case C-311/18) ("Schrems II"), p. 44, para. 5
[9] Id., p. 35, para 145.
[10] Id., p. 44, para. 4.
[11] Id., p. 32, para. 126.
[12] Id., p. 28, para. 95, citing GDPR Article 46(1) and Recital 108.
[13] Id., p. 29, para. 104, citing GDPR Articles 45(2) and 46.
[14] Id., p. 33, para. 132, citing GDPR Recital 109.
[15] Id., p. 33, para. 134.

face a difficult problem, because they cannot change U.S. surveillance laws or practices that could compromise the rights of EU data subjects to privacy protections. In light of the DPC's past statements, it is not obvious what supplemental measures could be taken by controllers and processors that would convince the DPC that EU personal data transfers to the United States comply with the GDPR.

3. Inadequate Protections Compell Supervisory Authorities to Suspend or Prohibit Data Transfer. EU Privacy Supervisory Authorities, including the Irish DPC, are *obligated* to suspend data transfer to a third country pursuant to SCCs "if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of that regulation [the GDPR] and by the Charter of Fundamental Rights, cannot be ensured by other means . . . ."[16]

   Implications: The Irish DPC and other competent supervisory authorities in the EU likely have reasonable grounds to suspend or prohibit transfers of personal data from the EU to the United States, if the transfers are justified based solely on the Privacy Shield Decision, or if they are based on SCC without supplemental measures that address the DPC's concerns. On July 28, 2020, the German Data Protection Conference issued a written statement that all data transfers based on the EU-U.S. Privacy Shield Decision must stop. Although BCR were not addressed in the Schrems II decision, there is no persuasive reason why the systemic dangers that were referenced in invalidating the Privacy Shield Decision, and that challenge the usefulness of the SCC Decision, will not also make the BCR of little value in justifying transfers of EU personal data to the U.S.

Steps U.S. Businesses Should Consider Taking.

While each U.S. business that is required to comply with the GDPR has a unique set of circumstances and considerations, I suggest these potential action items for discussion:

1. Deliberate and Plan Promptly. Call a meeting of the business's privacy and data protection decision makers to discuss the implications of Schrems II, including obligations to notify under existing SCC and reasonable supplemental measures that can be taken. Include knowledgeable attorneys in your discussion. Involve outside parties after the internal team has decided the game plan.

[16] Id., p. 44, para. 3, citing GDPR Article 58(2)(f) and (g).

2. Continue to Comply With Privacy Shield Obligations. Continue to comply with the EU-U.S. Privacy Shield. If the business wants to terminate its participation in Privacy Shield, the formal requirements for termination should be considered.

3. Consider Hosting EU Personal Data in the EU. The hosting country could be chosen for its data protection and regulatory characteristics. The data might still be processed in the U.S. in the meaning of GDPR Article 4(2), but it is worth evaluating whether the receipt, storage, and processing of EU personal data using EU servers would make the data less accessible to the U.S. government under U.S. law (and therefore better protected from a privacy perspective).

4. Consider Other Grounds for Import of EU Personal Data. Although the business should continue to abide by its SCC and BCR, it should consider whether the dangers of U.S. government surveillance recognized in Shrems II also represent a lack of legal protection of EU personal data in the United States that renders SCC and BCR legally unsupportable as a basis for EU data transfer. Discuss the possible use of GDPR Article 49 grounds for import of the data into the United States. One such ground is "explicit consent." GDPR Article 49(1)(a) permits a transfer of EU personal data without an adequacy decision if "the data subject has **explicitly consented** to the proposed transfer, after having been **informed** of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards" (emphasis in original). The EU Data Protection Board has issued guidelines and requirements for the use of explicit consent, which should be followed carefully.

5. Review Fair Processing Notice, Cookie Notice, and Cookie Policy. Disclosures to website visitors, cookie notices, and cookie policies may need to be revised in light of the decision in Schrems II. Particularly if relying on the "explicit consent" approach, the quality of all disclosures should be strong.

6. Improve GDPR Compliance In General. The invalidation of the Privacy Shield Decision may prompt EU supervisory authorities to audit the GDPR compliance of U.S. businesses that import EU personal data into the United States—starting with Privacy Shield participants. Improving the business's degree of GDPR compliance would appear to be a good risk mitigation decision. For example, the business should consider taking a hard look at the types of data it gathers from EU data subjects to determine whether it truly needs the data. Under the principle of data minimization (GDPR Article 25(1)), it may be best for the business not to gather, for example, geolocation data or browser analytics data from EU data subjects if the gathering is not necessary to

complete a contract with or fulfill the delivery of goods or services to EU customers.

Conclusion

Schrems II has badly shaken the ground that supports GDPR compliance by U.S. businesses. This would be a good time for U.S. businesses to take stock of the damage and to attempt to reinforce the structure of their European privacy law compliance strategy.

About the Author

Mr. Greber advises clients on how to comply with federal and state privacy laws governing the collection, use, retention, disclosure, and destruction of personal information gathered from customers. He assists his clients in establishing privacy and data security programs, and drafts privacy policies and terms of use for websites and mobile apps. He has assisted clients in responding to data breaches. Mr. Greber is a member of the International Association of Privacy Professionals (IAPP), the largest and most comprehensive global information privacy community. The IAPP developed and launched the only globally-recognized credentialing programs in information privacy. Mr. Greber holds the following IAPP certifications: CIPM (Certified Information Privacy Manager), CIPP/US (Certified Information Privacy Professional / US law), and CIPP/E (Certified Information Privacy Professional / European law).

Contact Information

David S. Greber, Esq.
Offit Kurman, P.A.
50 Carroll Creek Way, Suite 340
Frederick, MD 21701, USA
240.772.5137
dgreber@offitkurman.com
www.offitkurman.com
View Website Bio
LinkedIn: David Greber

4838-7803-8222, v. 1