CARTER LEDYARD

our resources

EU-US Transfers of Personal Data in the Wake of the Schrems II Ruling

April 22, 2021

Now that the dust has settled on the Court of Justice of the European Union's ("CJEU") landmark decision in Case C-311/18, *Data Protection Commission v. Facebook Ireland and Maximillian Schrems* ("*Schrems II*"),[1] it is time for many companies to begin the process of adopting recent EU recommendations concerning cross-border personal data transfers, if they have not already done so. In particular, multinational companies, big data and data analytics companies, social media companies, advertising technology companies, app development companies, and companies that gather consumer data, just to name a few, should be taking stock of the post-*Schrems II* recommendations released by the European Data Protection Board ("EDPB") and the European Commission's proposed new standard contractual clauses ("SCCs"), both of which were released in November 2020. Such companies should also consider whether any of the derogations outlined in Article 49 of the EU's General Data Protection Regulation ("GDPR") may provide an alternate method or legal basis for the transfer of data.

The CJEU's July 2020 decision in *Schrems II* significantly impacted the transfer of personal data from EU countries to the US. Most notably, the decision invalidated the Privacy Shield framework, upon which thousands of US companies relied to transfer data to the US in compliance with the GDPR. The decision also signaled that greater scrutiny was required of data transfers being made under other GDPR-compliant methods. This development has caused a great disruption to those companies routinely transferring personal data. Organizations that previously relied on the Privacy Shield must immediately institute an alternative approved transfer mechanism for EU data or risk violating the GDPR, which can carry fines of up to 4% of annual revenue or € 20 million, whichever is greater.

Pre-*Schrems II*: GDPR-Compliant Transfers of Data and the Privacy Shield

The GDPR, which went into effect in 2018, is the comprehensive data protection and privacy law in the EU and the European Economic Area ("EEA").[2] It is intended to protect individuals' personal data and provide individuals with basic rights and control over their personal data. Article 44 of the GDPR prohibits the transfer of personal data from the EU/EEA to recipients in jurisdictions outside the EU/EEA unless specific conditions are met. It prohibits, *inter alia*, the transfer of personal data to a non-EU/EEA country unless such country ensures an "adequate level of protection" for the data. If the European Commission has not issued an adequacy decision pursuant to GDPR Article 45 determining that country to have an adequate level of protection for transferred personal data, the data exporter must conduct the transfer using one of the GDPR's "appropriate safeguard" transfer mechanisms pursuant to Article 46 or one of the GDPR's "derogations for specific situations" under Article 49.

While the EU generally considers the US to have inadequate data protection safeguards, the EU has rendered an adequacy decision for those data transfers to the US covered by the Privacy Shield framework. The Privacy Shield was a program jointly designed by the US Department of Commerce and the European Commission intended to provide companies on both sides of the Atlantic with a mechanism for complying with data protection requirements when transferring personal data between the EEA and the US. It replaced the longstanding EU-US data transfer arrangement, known as the Safe Harbor framework, which the CJEU deemed invalid on October 6, 2015 after an earlier challenge also lodged by Schrems in Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner* ("*Schrems I*").[3]

Since release of the European Commission's Privacy Shield adequacy decision on July 16, 2016, thousands of organizations have relied on the Privacy Shield to receive personal data from organizations in the EEA. To be covered by the Privacy Shield framework, a company was required to self-certify annually to the Department of Commerce that it agreed to adhere to the Privacy Shield Principles, a detailed set of requirements based on privacy principles such as notice, choice, access, and accountability for onward transfer. The Privacy Shield framework, however, has faced criticism from its inception. Principally, critics of the arrangement maintained that it did not resolve the fundamental clash between US surveillance and EU data protection requirements, which received global attention following Edward Snowden's 2013 revelations about mass surveillance by the US National Security Agency.[4]

For data transfers not covered under the Privacy Shield, one of the most common "appropriate safeguard" mechanisms relied upon are SCCs. SCCs were approved and published by the European Commission and intended to be incorporated into agreements governing data transfers from the EU/EEA to countries outside the EU/EEA. Another "appropriate safeguard" mechanism that has been commonly used, especially by multinational companies and groups of related companies, are binding corporate rules ("BCRs"). BCRs are company data protection policies meeting certain criteria that must be submitted to and approved by the competent data protection authority in the EU.

In the absence of a GDPR Article 45 adequacy decision or a GDPR Article 46 appropriate safeguard to legitimize a personal data transfer to a third country, the transfer may still take place in certain situations (referred to as "derogations"), such as when: the data subject provides *explicit consent*; the transfer is necessary for the *performance of certain contracts*; the transfer is necessary for *important reasons of public interest*; the transfer is necessary for the *establishment, exercise or defense of legal claims*; the transfer is necessary in order to protect the *vital interests of the data subject* or of other persons and the data subject is physically or legally incapable of giving consent; or the transfer is necessary for *compelling legitimate interests* pursued by the data controller that are not overridden by the interests or rights and freedoms of the data subject, is not repetitive, concerns a limited number of data subjects, the data controller has assessed the circumstances surrounding the data transfer and on that basis provided suitable safeguards for the protection of the data, and the applicable supervisory authority is informed of the transfer.

Schrems II Invalidates the Privacy Shield and Creates New Obligations

Max Schrems, an Austrian activist and lawyer who had been a user of the Facebook social network for many years, filed a complaint in 2013 whereby he requested, in essence, that Facebook Ireland (through which data of EU Facebook users was transferred to Facebook in the US) be prohibited from transferring his personal data to the US, on the ground that US law and practices did not ensure adequate protection of the personal data held in its territory against the surveillance activities of governmental entities.[5]

In the *Schrems II* decision, the CJEU, siding with Schrems and other critics of the Privacy Shield, determined that the European Commission's adequacy decision for the Privacy Shield was invalid,[6] primarily for two reasons. First, the court determined that US surveillance under Section 702 of the Foreign Intelligence Surveillance Act ("FISA") and Executive Order 12333 did not limit the collection of personal data to what is strictly necessary and proportional, as required by EU law, and therefore did not satisfy the requirements of Article 52 of the EU Charter on Fundamental Rights.[7] Additionally, regarding US surveillance, the court determined that EU data subjects do not have rights actionable in court against US authorities and thus lack an effective remedy, which is required by Article 47 of the EU Charter.[8]

Not only did *Schrems II* invalidate the Privacy Shield, it also made it more difficult to perform cross-border personal data transfers using GDPR Article 46 "appropriate safeguard" transfer mechanisms, such as SCCs. While the *Schrems II* court affirmed the validity of SCCs as a transfer mechanism, it determined that companies are additionally required to assess, on a case-by-case basis, whether the law of the third country ensures adequate protection against access by public authorities to personal data transferred to that country. *Schrems II* requires companies to assess, on a case-by-case basis, whether such transfer mechanisms meet EU standards concerning protection against government access to transferred data, and, if not, whether supplementary measures can be implemented to meet such standards.[9]

Post-*Schrems II* Guidance from the EU

In November 2020, in response to the *Schrems II* decision, the EDPB published recommendations to assist companies in assessing the sufficiency of protections and in implementing supplementary measures when protections are determined to be lacking compared to EU standards (collectively, the "Recommendations").[10] The EDPB's Recommendations provide the following six steps for data exporters to follow:

1. *Know your transfers.* Map all transfers of personal data to third countries, including any onward transfers by data importers in the third country to a different data importer in another third country or the same third country.[11]

2. *Identify the transfer tools relied upon.* Identify the transfer tool or safeguards that a transfer relies upon among those listed in GDPR Chapter V.[12]

3. *Assess whether the third country's law or practice impinges on the transfer tool's effectiveness.* Assess, under the circumstances of the particular transfer, whether the law or practice of the third country may undermine the Article 46 transfer tool's level of protection such that the transferred data would not be afforded a level of protection in the third country that is essentially equivalent to that granted in the EU.[13]

4. *Adopt supplementary measures.* If appropriate, identify and implement supplementary measures to add to the safeguards in order to ensure that the level of protection of the transferred data in the third country is essentially equivalent to that guaranteed in the EU.[14] If no supplementary measures can do so, then the transfer must be terminated.[15] Examples of supplementary technical measures include encryption, pseudonymization, and split or multi-party processing.[16] The Recommendations also contain examples of scenarios where the EDPB has found no supplementary technical measures to be effective.[17] As for supplementary contractual measures, examples include contractual commitments by data importers to put specific technical measures in place and to be transparent, allowing the data exporter to audit whether the importer has provided personal data to public authorities, and contractual commitments by data importers to challenge government requests for access to personal data in court before disclosing the data and to enable data subjects to exercise their rights.[18]

5. *Seek authorization, if required, for the supplementary measure.* Request authorization from a competent data supervisory authority for supplementary measures that contradict SCCs.[19]

6. *Reassess the level of protection of the transferred data at appropriate intervals.* Monitor, on an ongoing basis, developments in the third country to which personal data has been transferred that could impact the data exporter's assessment of the level of protection of personal data in that country and terminate transfers to that country if supplementary measures are no longer effective.[20] Importantly, data exporters are required to document their transfer assessments and supplementary measures, and to make such documentation available to a data protection supervisory authority upon request.[21]

In November 2020, the European Commission also published its draft implementing decision on updated SCCs for the transfer of personal data to third countries along with an accompanying Annex setting forth the new SCCs.[22] As the draft decision explains, these proposed new SCCs reflect the Commission's efforts to update and modernize its previously adopted SCCs to account for recent developments concerning the GDPR and the digital economy.[23] The draft decision and new SCCs were subject to a public consultation period, which closed on December 10, 2020, and it is anticipated that the final SCCs will be adopted in 2021. Once the final version of the new SCCs has been adopted, organizations will have a one-year transition period to implement them.

The July 2020 *Schrems II* decision did not involve any specific rulings on the use of GDPR Article 49 derogations to perform transfers. However, the judge-rapporteur in the *Schrems II* case, Judge Thomas von Danwitz, reportedly stated during a conference in January 2021 that GDPR

derogations are not so narrow and have not been fully explored, thereby suggesting that the ability to rely upon those derogations to perform cross-border personal data transfers may not be as limited as many had previously thought.[24]

On March 25 of this year, the EU Commissioner for Justice and the US Secretary of Commerce announced that the EU and US had agreed to intensify negotiations on an enhanced EU-US Privacy Shield framework that would be compliant with the *Schrems II* decision.[25] Although there is optimism that there will be a new cross-border data transfer pact between the EU and US to replace the Privacy Shield, some have opined that it may take months—if not years—for such an agreement to be reached because of US surveillance laws and the lack of comprehensive data privacy legislation in the US, among other reasons.[26]

US Business Considerations

Businesses that rely on personal data transfers from the EU should review and incorporate the EDPB's Recommendations outlined briefly above. Entities that have relied upon the Privacy Shield framework must explore alternative methods or legal bases for the transfer of data, such as SCCs, BCRs, or derogations.

Companies that have relied upon SCCs in their contracts will need to compare their SCCs to the new SCCs, which will likely be adopted in 2021, and entities should make any required modifications or be prepared to transition to the new SCCs following their adoption. Companies that rely on SCCs will also need to assess whether supplementary procedures must be implemented in order to ensure compliance with the EU requirements. SCCs alone may no longer be sufficient for compliance, and additional safeguards may be required to protect personal data.

Companies, especially those that transfer data internationally amongst related companies or within one company, should reconsider whether any of the GDPR Article 49 derogations apply to their transfers and also should assess whether BCRs are a viable and feasible solution.

Conclusion

The CJEU's decision in *Schrems II* invalidating the Privacy Shield has created much uncertainty and disruption on both sides of the Atlantic. In the aftermath of the court's decision, thousands of companies have been forced to reassess and revise their data transfer mechanisms in the face of an uncertain and evolving legal landscape. In particular, *Schrems II* poses significant questions and concerns for companies and organizations involved in certain types of trans-Atlantic trade, such as large multinationals, big data companies, data analytics companies, social media companies, and companies offering cloud-based services, just to name a few.

Although the EU and the US have agreed to intensify negotiations on an enhanced EU-US Privacy Shield framework, it could be months, or even years, before such an arrangement is in place. Similarly, the EU has not yet approved the revised draft SCCs, but new SCCs are expected to be adopted in 2021. Accordingly, it is essential that companies seek the advice of experienced counsel to help navigate the complex legal issues surrounding cross-border data transfers in light of the evolving law and recommendations from the EU.

* * *

---

[1] Available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en (last visited Apr. 12, 2021).

[2] The EEA includes all EU countries, Iceland, Liechtenstein, and Norway.

[3] Available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=143358 (last visited Apr. 12, 2021).

[4] *See, e.g.*, Natasha Lomas, "EU-US Privacy Shield Is Dead. Long Live Privacy Shield," *TechCrunch.com* (Aug. 11, 2020), https://techcrunch.com/2020/08/11/eu-us-privacy-shield-is-dead-long-live-privacy-shield/; Martin A. Weiss & Kristin Archick, Cong. Research Serv., *U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield* at 1 (May 19, 2016), https://fas.org/sgp/crs/misc/R44257.pdf.

[5] *Schrems I*, ¶¶ *26-28.*

[6] *Schrems II*, ¶ 201.

[7] *Id.* ¶¶ 184-185. In that regard, Article 52 of the EU Charter on Fundamental Rights states: "Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."

[8] *Schrems II*, ¶¶ 191-193. Article 47 of the EU Charter provides in relevant part that "[e]veryone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article."

[9] *Schrems II*, ¶ 134.

[10] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, Nov. 10, 2020 ("Recommendations on Essential Guarantees"), available at https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en (last visited Apr. 12, 2021); EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Nov. 10, 2020 ("Recommendations on Supplementary Measures"), available at https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en (last visited Apr. 12, 2021).

[11] Recommendations on Supplementary Measures, ¶¶ 8-13.

[12] *Id.* ¶¶ 14-26.

[13] *Id.* ¶¶ 28-44.

[14] *Id.* ¶ 45.

[15] *Id.* ¶ 52.

[16] *Id.* ¶¶ 72-86.

[17] *Id.* ¶¶ 87-91.

[18] *Id.* ¶¶ 97-121.

[19] *Id.* ¶¶ 55-57.

[20] *Id.* ¶¶ 62-63.

[21] *Id.* ¶ 7 (citing GDPR Arts. 5(2) and 24(1)).

[22] Both the Draft European Commission Implementing Decision and the Annex containing the revised SCCs are available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries (last visited Apr. 12, 2021).

[23] Draft European Commission Implementing Decision, ¶ 6.

[24] Rob van Eijk & Gabriela Zanfir-Fortuna, "*Schrems II*: Article 49 GDPR Derogations May Not Be So Narrow and Restrictive After All?," *Future of Privacy Forum* (Feb. 4, 2021), https://fpf.org/blog/schrems-ii-article-49-gdpr-derogations-may-not-be-so-narrow-and-restrictive-after-all/.

[25] Press Release, European Commission & U.S. Gov't, Intensifying Negotiations on Transatlantic Data Privacy Flows: A Joint Press Statement by European Comm'r for Justice Didier Reynders and U.S. Sec'y of Commerce Gina Raimondo (Mar. 25, 2021), https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443.

[26] *See* Catherine Stupp, "Surveillance Concerns Could Hold Up European-U.S. Data Agreement for Years," *WSJ Pro* (Mar. 9, 2021), https://www.wsj.com/articles/surveillance-concerns-could-hold-up-european-u-s-data-agreement-for-years-11615285800.

---

related professionals

Matthew D. Dunn / Partner
D 212-238-8706
mdunn@clm.com

Sarah H. Ganley / Associate
D 212-238-8834
ganley@clm.com