Lost on the High Seas without a Safe Harbor and a Shield? Navigating Cross-Border Transfers in the Pharma Sector After Schrems II*

Marcelo Corrales Compagnucci, Timo Minssen, Claudia Seitz and Mateo Aboy**

This article analyzes the impact and associated legal challenges of cross-border data transfers in the pharmaceutical sector after the recent Court of Justice of the European Union (CJEU) decision in Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Schrems II). In Schrems II, the CJEU invalidated Decision 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield Framework. That said, the Court also found that the European Commission Decision 2010/87 on standard contractual clauses (SCCs) for the transfer of personal data to processors established in third countries is still valid. The ruling has resulted in significant uncertainty and liability risks for organizations that depend on EU-US cross-border transfers of personal data such as pharmaceutical companies (data controllers) engaged in global clinical trials and their technology providers for endpoint collection and data transfer (processors). In light of these challenges, this paper discusses the need for sustainable practices and a legally sound regulatory environment for data transfer. To mitigate risks and uncertainties, we stress the need for updated SCCs guidelines and argue inter alia for the adoption of contractual frameworks which incorporate SCCs with a robust information security management system (ISMS) and a privacy information management system (PIMS) to ensure an appropriate level of data protection.

* This is a working paper. The final version was submitted to the European Pharmaceutical Law Review and the article is currently under review. This paper could consider developments until 17 August 2020. We will follow up on any new developments in the final version. For further questions please contact: marcelo.c.compagnucci@jur.ku.dk
** Marcelo Corrales Compagnucci, Assoc. Professor, Center for Advanced Studies in Biomedical Innovation Law (CeBIL), University of Copenhagen (UCPH), Founding Director of UCPH’s Center for Advanced Studies in Biomedical Innovation Law (CeBIL), Senior Consultant at X-officio; Claudia Seitz, Visiting Professor of Law at the University of Ghent, Faculty of Law and Criminology, Lecturer at the University of Basel, Faculty of Law, Center for Life Sciences Law (CLSL) and Lecturer at the University of Bonn, Faculty of Law, Centre for the Law of Life Sciences; Mateo Aboy, Principal Research Scholar at the LML (University of Cambridge, UK) and Affiliated Professor & Fellow at the CeBIL, University of Copenhagen (UCPH).
Acknowledgement: The research for this paper was supported by a Novo Nordisk Foundation grant for a scientifically independent Collaborative Research Program in Biomedical Innovation Law (grant agreement number NNF17SA0027784).
1 Introduction

Technological innovations relying in the cloud-based storage and computing such as wearable devices, big data, and artificial intelligence (AI) are emerging in the medical and pharmaceutical sector. They are expected to play an increasingly important role in the future due to the digitalization of clinical outcome assessments (COA) and endpoints. Digital endpoint collection, biomedical signal processing, big data and AI-based technologies often rely on cloud-based architectures for data management, storage and processing power in global clinical trials and clinical research applications. Additionally, the increased need for virtual trials, in part as a consequence of COVID-19, is accelerating the need for technologies capable of being deployed directly at home (e.g., eCOA provisioned devices and wearables) for digital endpoint collection. These virtual trial technologies often leverage cloud-based solutions to upload data from the provision devices deployed at home directly to the cloud for storage, as well as for cloud-computation and trial oversight.

These types of forward-looking technologies result in cloud-based dataflows. In the context of global clinical trials and research, these dataflows often result in cross-border transfers of personal data from the trial participants. Accordingly, the need for an effective and transparent legal framework for cross-border data transfers is increasingly evident. However, due to an inconsistent privacy and data protection regulatory environment, it has been difficult to achieve data transfers at the international level. In the United States for example, largely as a result of the lack of a data protection law at the federal level, the country does not have what is referred to in Article 45 of the GDPR as a general “adequacy decision” from the European Commission which would allow EU-US cross-border data transfers without additional data safeguards under the GDPR.

The failure of the previous Safe Harbor Program was the initiating factor for the creation of a new data transfer regime. This came as a repercussion from the Schrems I Court of Justice of the European Union (CJEU) judgment for apparently violating EU users’ privacy rights in the form of mass surveillance programs in the US. Concisely, the CJEU stated that the fundamental right of

---


4 Timo Minssen, Claudia Seitz, Mateo Aboy and Marcelo Corrales Compagnucci, 2020, The EU-US Privacy Shield Regime for Cross-Border Transfers of Personal Data under the GDPR, EPLR, Vol. 4, Issue 1, p. 34.

natural persons to respect for privacy which is protected under Article 1 of the GDPR is compromised when public authorities are granted access to the content of electronic communications and these authorities are not bound by comparable data protection obligations. Furthermore, the CJEU noticed that the fundamental right to effective judicial protection is also compromised when the US legislation does not make it possible for an individual to take actions in order to have access to his/her personal data, or to rectify or delete such data.\(^6\)

In order to partially alleviate concerns, a “limited adequacy” decision was enacted in 2016 within the context of the transatlantic cross-border transfer mechanism called “EU-US Privacy Shield.”\(^7\) The purpose of this framework lies in the protection of the fundamental rights of EU citizens since the importance of both the fundamental right to respect for private life, guaranteed by Article 7, and the fundamental right to the protection of personal data, guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union (CFR),\(^8\) has been emphasized in the case-law of the Court of Justice.\(^9\) The EU-US Privacy Shield allows the transfer of personal information only in the event that it is certified under the conditions of this framework. Pharmaceutical and healthcare companies extensively use this framework,\(^10\) which allow these firms to legally engage in cross-border data transfers between the EU and US. However, the EU-US Privacy Shield’s status has been challenged at the CJEU in the follow-up Schrems II case.\(^11\)

Since we have already analyzed and discussed the procedural background to the decision in detail in our previous paper in EPLR Vol. 4 Issue 1,\(^12\) (spring 2020), this article starts with a brief summary of the non-binding opinion of the Advocate General (AG)\(^13\) Henrik Saugmandsgaard Øe’s, which was delivered on December 19\(^{th}\), 2020 (section 2). We then examine the outcome and legal essence of the recent CJEU’s Schrems II decision\(^14\) (section 3). This is followed by a discussion of how the decision may impact organizations that deploy cloud-based technologies.

---

6 Timo Minssen, Claudia Seitz, Mateo Aboy and Marcelo Corrales Compagnucci, 2020, The EU-US Privacy Shield Regime for Cross-Border Transfers of Personal Data under the GDPR, EPLR, Vol. 4, Issue 1, p. 36.
9 See, e.g., Case C-553/07 - Rijkeboer, ECLI:EU:C:2009:293, paragraph 47; Joined Cases C-293/12 and C-594/12 - Digital Rights Ireland and Others, ECLI:EU:C:2014:238, paragraph 53; Case C-131/12 - Google Spain and Google, ECLI:EU:C:2014:317, paragraphs 53, 66 and 74.
10 For a list of over 5,300 companies relying on this framework see: https://www.privacyshield.gov/list. Accessed 26 July 2020.
11 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Case C-311/18).
that involve cross border transfers of EU data subjects, how the new legal environment can be navigated (section 4), and concluding remarks (section 5).

2 The Opinion of the Advocate General

By and large, the AG elucidated his concern about the extent of protection of data conveyed from the EU under that system. This concern was particularly expressed in relation to data transferred to the US, which could be accessed by US intelligence agencies and judicial authorities. The AG’s Opinion could be broadly divided into two parts: the first which dealt with the legality of the SCCs and the second which dealt with the EU-US Privacy Shield Framework. The key questions and findings of the AG’s Opinion can be summarized as follows:

The AG took the stance that the SCCs are valid and may offer appropriate safeguards and level of protection, but the AG’s opinion stressed that the aim of the SCCs is to compensate for any deficiencies in the third country data protection legislation where the data exporter and importer are contractually bound. Moreover, the AG considered that the compatibility of the SSCs with the CFR, and in particular, Article 7 (privacy) and Article 8 (data protection), depends on whether there are sufficiently sound mechanisms to ensure that any transfer relying on the SCCs are suspended or prohibited where those clauses are breached or impossible to honor. More specifically, the AG suggested that privacy and data protection complaints must be taken seriously if these clauses cannot be complied with. The AG recommended that the supervisory authorities should examine with all due diligence any complaint filed by organizations and individuals whose data are allegedly transferred to a third country in contravention to the SCCs. If SCCs are violated and appropriate protection cannot be guaranteed, the supervisory authority must suspend or prohibit transfers of personal data.

As for the EU-US Privacy Shield Framework, the AG considered that the subject matter of the main proceedings in the Schrems II case relates to the validity of the SCCs and that any findings relating to the validity of the EU-US Privacy Shield decision could not influence the outcome of the dispute in the main proceedings. The AG therefore recommended that the CJEU should not decide the validity in the Schrems II case since it was not directly contested in the main claim. But, he also raised some concerns whether this Framework met the adequacy threshold. Based on the previous jurisprudence, the AG considered that such surveillance by US authorities was generally justified on the grounds of public interest and that the very essence of Articles 7 and 8 was not compromised. However, the AG noted that the necessity and proportionality principles should be

---

15 Timo Minssen, Claudia Seitz, Mateo Aboy and Marcelo Corrales Compagnucci, 2020, The EU-US Privacy Shield Regime for Cross-Border Transfers of Personal Data under the GDPR, EPLR, Vol. 4, Issue 1, p. 43.
17 Timo Minssen, Claudia Seitz, Mateo Aboy and Marcelo Corrales Compagnucci, 2020, The EU-US Privacy Shield Regime for Cross-Border Transfers of Personal Data under the GDPR, EPLR, Vol. 4, Issue 1, p. 43.
considered on a case by case basis. The AG also raised some doubts with regard to the right to an effective remedy and questioned the effective impact of the introduction of the Ombudsman figure as a mechanism which aims at compensating some of the dearth in the US system. According to the AG, the current Ombudsman mechanism does not ensure independent control of surveillance measures. The Ombudsman must be established by law and should be independent from the executive to effectively address such remedies.¹⁸

3 The Schrems II Judgment

The CJEU finally announced its much awaited Schrems II decision on July 16th, 2020.¹⁹ It delivered a seminal judgment that did not follow all of the AG’s recommendations, since it considered and ultimately invalidated the European Commission’s Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield. In that regard, the CJEU followed a similar approach like almost five years ago when the CJEU rejected the Privacy Shield’s predecessor: the Safe Harbor framework. The Court also held, however, that the European Commission’s Decision 2010/87 on SCC’s²⁰ for the transfer of personal data to processors established in third countries is still valid.

With regard to the SCCs, the CJEU mainly followed the AG’s viewpoint. The CJEU established a heavy burden on data exporters relying on the use of SCCs. Data exporters have an obligation to evaluate the law and practice of the country to which data will be transferred, especially if public authorities may have access to the data. Only when there is not conflicting law and if there is in fact an “adequate level” of protection they can use the SCCs. Moreover, the CJEU underscored that organizations may be required to implement additional safeguards, beyond those contained in the SCCs. With respect to non-EU organizations importing data from the EU based on SCCs, the CJEU noted that they must inform data exporters in the EU if they are unable to comply with the SCCs and where there are no additional safeguards in place. In such case, the data exporter based in the EU must suspend the transfer of data and/or terminate the contract. The CJEU further confirmed the AG’s recommendation with regard to the role of supervisory authorities that should examine and, where necessary, suspend the transfer of personal data to an importing jurisdiction when SCCs are violated and appropriate protection cannot be guaranteed.²¹

Contrary to the approach recommended by the AG’s opinion, the CJEU examined the validity of the EU-US Privacy Shield Framework and decided to strike it down. The CJEU casted doubts

---

¹⁸ Ibid, pp. 43-44.
¹⁹ Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II).
as to whether US law effectively ensures the adequate level of protection prescribed under Article 45 of the GDPR, with regard to the fundamental rights guaranteed by the CFR. The CJEU considered that US law (i.e., Section 602 FISA and EO 12333)\(^\text{22}\) does not grant the necessary limitations and safeguards with regard to the interferences authorized by its national legislation and does not ensure adequate judicial protection against such interferences. With regard to the effective judicial protection, the CJEU concurred with the AG Opinion that the Ombudsman cannot remedy those deficiencies since the figure of the Ombudsman cannot be regarded as a tribunal within the meaning of Art. 47 of the CFR.\(^\text{23}\)

With regard to Articles 7 and 8 of the CFR, access to individual’s personal data with a view to its retention or use breaches the fundamental rights to respect for private life. The CJEU held that the communication of personal data to a third party, including a public authority, represents an interference with the fundamental rights under the scope of the CFR. The same holds true for the retention of personal data and access to that data with the intention of its use by public authorities, regardless of whether the information in question relating to private life is sensitive or not.\(^\text{24}\)

### 4 The Impact on Cross-border Data Transfers

The *Schrems II* judgment covers various important aspects such as commercial and national security issues. Since the CJEU found that the domestic law in the US does not ensure an essentially equivalent level of protection, the EU-US Privacy Shield Framework is no longer valid. SCCs could be used as a substitute, but with the nuance that this would depend on the result of a case by case assessment by the controller established in the EU taking into account the circumstances of the transfer and whether additional measures are in place or not. The supplementary measures along with SCCs, would have to guarantee that US law is not likely to have an adverse effect on the adequate level of protection. If the controller comes to the conclusion that regardless the SCCs and the application of additional safeguards are not going to guarantee the adequate level of protection, the data transfer should be suspended or ended. If the controller, however, considers to keep transferring data notwithstanding this conclusion, he or she should notify the competent supervisory authority. The same assessment and procedure should apply to the Binding Corporate Rules (BCRs) mechanism within companies belonging to the same group.\(^\text{25}\)

Consequently, this decision raises the threshold for international data transfers and puts more pressure on data protection authorities (DPAs) to supervise and take enforcement actions.

\(^{22}\) While Section 702 FISA deals with all “electronic communication service provider”, Executive Order (EO) 12333 organizes electronic surveillance.

\(^{23}\) *Case C-311/18 (Schrems II)* at paragraph 168. See also, CJEU Press Release No. 91/20 (16 July 2020).

\(^{24}\) *Case C-311/18 (Schrems II)* at paragraphs 170 and 171. See also, CJEU Press Release No. 91/20 (16 July 2020).

Additionally, companies should implement “supplementary measures” in order to ensure compliance with adequate level of protection. Some contracts will likely have to be renegotiated to ensure those safeguards mechanisms are in place, especially to ensure compliance with the data protection (SCC Appendix 1) and security (SCC Appendix 2) organizational and technical measures to ensure appropriate safeguards by the organization (in the absence of an “adequacy” decision at the country level).

On July 29th, 2020 the European Data Protection Board (EDPB) adopted a statement during its 34th plenary session on Schrems II. With regard to the Privacy Shield, the EDPB pointed out that the EU and the US should achieve a complete and effective framework guaranteeing that the level of protection granted to personal data in the US is essentially equivalent to that guaranteed within the EU, in line with the judgment. The EDPB intends to continue playing a constructive part in securing a transatlantic transfer of personal data that benefits EU citizens and organizations and stands ready to provide the European Commission with assistance and guidance to help it build, together with the US, a new framework that fully complies with EU data protection law.

With regards to SCCs, the EDPB takes note of the primary responsibility of the exporter and the importer, when considering whether to enter into SCCs, to ensure that these maintain a level of protection that is essentially equivalent to the one guaranteed by the GDPR in light of the CFR. When performing such prior assessment, the exporter (if necessary, with the assistance of the importer) shall take into consideration the content of the SCCs, the specific circumstances of the transfer, as well as the legal regime applicable in the importer’s country. The CJEU underlines that the exporter may have to consider putting in place additional measures to those included in the SCCs.

As a practical implication for reliance on SCCs, the data exporter and importer need to verify whether the destination country’s laws will allow compliance with the GDPR, the SCCs themselves and also the CFR. If the laws of the destination country are likely to prevent compliance, the CJEU suggests it may be necessary to supplement the guarantees contained in the SCCs with other clauses or additional safeguards. Thus, a transfer of personal data to the US can only be justified by SCCs if additional measures are taken that guarantee the same level of data protection as in the EU. The circumstances of the data transfers would have to be considered, according to the EDPB, on a case-by-case basis which also applies to the transfer of personal data of EU citizens to other countries.

In order to ensure compliance, the SCCs should be incorporated in a framework agreement which ensures that any other contractual provisions provide for an adequate level of protection. These safeguards should be documented as part of Appendix 2 of the SCCs, and should include at least the measures to ensure compliance with security of processing to satisfy the Art. 32 GDPR requirements. In the context of clinical trials and clinical research this includes the need to implement a robust information security management system (ISMS) and a privacy information

---

26 Case C-311/18 (Schrems II) at paragraph 133.
management system (PIMS) to ensure an appropriate level of data protection based on the risk. This is also important in order to avoid damage claims since the CJEU held in Schrems II that a breach of SCCs “will result in a right for the person concerned to receive compensation for the damage suffered.”

In the specific case of transfers of personal data to the US it could be possible that a transfer of personal data to a recipient in the US could become a risk if there is any possibility of surveillance of or through the recipient. Thus, it is important to monitor how supervisory authorities take position after Schrems II in order to manage this risk in the near future. As a consequence, the incomplete and apparently insufficient nature of SCCs in the CJEU’s view in Schrems II raises questions in terms of liability and risk management, and may make organizations more hesitant to transfer data under the SCCs. That said, in the context of medical products where the GDPR interplays with the Clinical Trial Regulation (CTR), the risks are lower than in general personal data transfers (e.g., by social media and data aggregation firms) because the trial sponsor is legally obligated by the CTR to carry out a range of processing activities (i.e., the legal basis of processing for the trial is acting under a “legal obligation” under Art. 6(1)(c) and Art. 9(2)(i) “processing is necessary for reasons of public interest in the area of public health, such as […] ensuring high standards of quality and safety of health care and of medicinal products or medical devices…”).

Additionally, the sponsor is already subject to Member States inspections (Article 78 of CTR) and Member States’ GCP inspectors are entitled to have access to clinical trial data, audit the protocol, etc. Accordingly, as long as the sponsor (and the contracted processors) follow the trial protocol authorized under the CTR that defines the purposes and conditions for which the data of clinical trial subjects will be processed and meet the CTR legal obligations (e.g., results reporting, safety reporting, archival of the clinical trial master file for 25 years) while providing an appropriate level of data protection by employing an ISMS such as the ISO27001 and PIMS such as the ISO 27701, SCCs are likely to be considered by the supervisory authorities to provide appropriate safeguards for clinical trial data protection as long as they are employed correctly (e.g., with properly completed Appendix 1 & 2 specifying the organizational and technical measures to ensure an appropriate level of protection based on the risk and audited periodically).

Pharma sponsors (data controllers) and their clinical trial technology/service providers (processors) should review their records of processing activities (Art. 30 GDPR) to determine the specific cross-border transfer mechanism employed for each clinical trial involving EU-US transfers of personal data. In the case that the cross-border transfers have been legitimized solely based on the EU-US Privacy Shield, the pharma data controllers and processors are advised to at least implement European Commission approved SCCs after ensuring they can satisfy their respective obligations as data exporters and importers, including the documentation of the technical and organizational security measures implemented in accordance with SCC Clauses 4(d) and 5(c), audit (SCC Clause 5(f)), and liability (Clause 6). It should be kept in mind that alternative appropriate safeguards – such as ad hoc contractual clauses or BCRs – require approval of the supervisory authority.

28 Case C-311/18 (Schrems II) at paragraph 143.
In addition, Article 49 GDPR sets out conditions under which international transfers of personal data may take place in the absence of an adequacy decision or appropriate safeguards. Companies can rely on the derogations set forth under Article 49 GDPR, provided that the conditions as interpreted by the EDPB in its guidance on Article 49 GDPR are met. When transferring personal data based on individuals’ consent, such consent should be explicit, specific to the particular data transfer(s) and informed, particularly regarding the risks of the transfer(s). Furthermore, transfers of personal data that are necessary for the performance of a contract should only take place occasionally. As a consequence, the referral to Article 49 GDPR does not offer a general solution since it is limited to cases under exceptional circumstances.

Finally, not all the cross-border dataflows are possible to be legitimized employing SCCs. The current SCCs enable cross-border transfers from a 1) EU/EEA Controller to a non-EU/EEA Controller, or 2) EU/EEA Controller to a non-EU/EEA processor. The European Commission approved SCCs are not designed for use by non-EU Controllers or by processors as data exporters. Accordingly, they cannot be used by a non-EU/EEA Controller to transfer data or for processor-to-processor transfers.

5 Outlook and Conclusions

The Schrems II ruling will result in significant uncertainty for organizations involved in EU-US cross-border transfers such as pharmaceutical companies, contract research organizations (CROs), and their technology providers engaged in global clinical trials. In light of the complexity of the situation, swift cross-Atlantic negotiations, grace periods and updated SCCs guidelines are now needed to establish sustainable, user-friendly practices and a legally sound regulatory environment for data transfer in the pharmaceutical sector, as well as in other sectors. This has become particularly important since it is clear that many entities that depended on the Privacy Shield will now swiftly switch to the use of SCCs, whereas those vendors that have already operated with SCCs will have to ascertain and confirm the legality of their SCCs in compliance with Schrems II vis-à-vis concerned business partners and customers. The proposed contractual framework attempts to mitigate some of the risks and fills the gaps in the current legal framework. It will also provide a broader scope of value-added services and imbue a privacy and information security management culture among organizations to ensure an appropriate level of data protection based on the risk and audit systems.

That said, it is clear that Schrems II will not turn off the Internet and much EU data will still be transferred to the US on many levels and in both “everyday life” and sector-specific situations. Individual rights, data protection, data integrity and EU data interests must thus be reconciled with the necessary support for international business, innovation and trade on many levels.
Last but not least, we would like to stress that *Schrems II*, is clearly also a constitutional judgment with important constitutional implications for the European public order.\(^{29}\) While these implications were not at the focus of this paper, it is clear that *Schrems II* will keep the European legal discourses and lawyers busy on many levels.