Lost on the High Seas without a Safe Harbor or a Shield? Navigating Cross-Border Transfers in the Pharmaceutical Sector After Schrems II Invalidation of the EU-US Privacy Shield

Corrales Compagnucci, Marcelo; Minssen, Timo; Seitz, Claudia; Aboy, Mateo

Published in:
European Pharmaceutical Law Review

Publication date:
2020

Document version
Peer reviewed version

Citation for published version (APA):
Corrales Compagnucci, M., Minssen, T., Seitz, C., & Aboy, M. (2020). Lost on the High Seas without a Safe Harbor or a Shield? Navigating Cross-Border Transfers in the Pharmaceutical Sector After Schrems II Invalidation of the EU-US Privacy Shield. *European Pharmaceutical Law Review*, *4*(3), 153-160.

Lost on the High Seas without a Safe Harbor or a Shield? Navigating Cross-Border Transfers in the Pharmaceutical Sector After *Schrems II* Invalidation of the EU-US Privacy Shield

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

This paper 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, including 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 a legally sound regulatory environment for data transfer. To mitigate risks and uncertainties, we stress the need for updated GDPR-compliant SCCs and SCC guidelines and argue, inter alia, for the adoption of data protection 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, as well as for sector specific transfer mechanisms including health data adequacy decisions and the need for GDPR certification and codes of conduct for cross-border transfers of clinical trial data.

* Marcelo Corrales Compagnucci, Assoc. Professor, Center for Advanced Studies in Biomedical Innovation Law (CeBIL), University of Copenhagen (UCPH); Timo Minssen, Professor of Law at the 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). This paper could consider developments until 17 October 2020. For correspondence: <marcelo.c.compagnucci@jur.ku.dk>

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).

I. Introduction

Technological innovations relying on cloud-based storage and computing such as wearable devices, big data, and artificial intelligence (AI) are emerging in the medical and pharmaceutical sector.[1] 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 international clinical trials and clinical research applications. Additionally, the increased need for virtual trials, in part as a consequence of COVID-19,[2] has accelerated 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 for remote patient and side monitoring 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.[3]

These types of forward-looking technologies lead often to cloud-based data flows. In the context of global clinical trials and research, these data flows generally result in cross-border transfers of personal data from the trial participants. Accordingly, the need for an effective 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 legally-compliant personal data transfers at the international level. The United States, for example, largely as a result of the lack of a data protection law at the federal level, does not have what is referred to in Article 45 of the General Data Protection Regulation (GDPR)[4] as a general "adequacy

[1] Marcelo Corrales Compagnucci, Janos Meszaros, Timo Minssen, Aras Arasilango, Talal Ous and Muttukrshnan Rajarajan, 2019, Homomorphic Encryption: The 'Holy Grail' for Big Data Analytics & Legal Compliance in the Pharmaceutical Sector? *EPLR*, Vol. 3, Issue 4, pp. 144-145.

[2] See, e.g., European Commission, Guidance on the Management of Clinical Trials during the COVID-19 (Coronavirus) Pandemic. Version 3 (28 April 2020), available at: https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-10/guidanceclinicaltrials_covid19_en.pdf. Accessed 17 October 2020.

[3] US FDA, 'FDA Guidance on Conduct of Clinical Trials of Medical Products during COVID-19 Public Health Emergency: Guidance for Industry, Investigators, and Institutional Review Boards' (21 September 2020), available at: https://www.fda.gov/media/136238/download. Accessed 17 October 2020; Sophie Porter, 'The Impact of COVID-19 on Virtual Trials' (12 June 2020), available at: https://www.mobihealthnews.com/news/europe/impact-covid-19-virtual-trials. Accessed 17 October 2020; Simon Erridge, Azeem Majeed and Mikael Sodergren, 'Virtual Trials: Looking Beyond COVID-19' (6 July 2020), available at: https://blogs.bmj.com/bmj/2020/07/06/virtual-trials-looking-beyond-covid-19/. Accessed 17October 2020.

[4] Regulation (EU) 2016/679 of the EP and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ 2016 L 119, p. 1 (General Data Protection Regulation, GDPR).

decision" from the European Commission which would allow EU-US cross-border data transfers without additional data safeguards under the GDPR.[5]

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 consequence of the *Schrems I*[6] judgment of the CJEU 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 natural persons to privacy, which is protected under Article 8(1) of the Charter of Fundamental Rights of the European Union (CFR)[7] and accordingly in Article 1 of the GDPR for the protection of personal data 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 according to Article 47 CFR 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.[8]

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 the "EU-US Privacy Shield."[9] The purpose of this framework was the protection of the fundamental rights of EU data subjects. The importance of both the fundamental right to respect for private life, guaranteed by Article 7 CFR, and the fundamental right to the protection of personal data, guaranteed by Article 8 CFR, has been emphasized in the case-law of the CJEU.[10] The EU-US Privacy Shield allowed the transfer of personal data only in the event that it is certified under the conditions of this framework. Pharmaceutical and healthcare companies extensively used this framework,[11] which allowed 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.[12]

Since we have already analyzed and discussed the procedural background to the decision in detail in our previous paper,[13] (Spring 2020), this paper starts with a brief summary of the non-

---

[5] 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, pp. 34-50.

[6] CJEU, Case C-362/14 - *Maximiliam Schrems v Data Protection Commissioner* of 6 October 2016, ECLI:EU:C:2015:650 (*Schrems I*). See also, CJEU Press Release No. 117/15 (6 October 2015).

[7] Charter of Fundamental Rights of the European Union (EU CRF), OJ C 326, 26.10.2012, pp. 391-407.

[8] 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, pp. 34-50.

[9] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (OJ 2016 L 207, p. 1).

[10] See, e.g., CJEU, 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.

[11] For a list of over 5,300 companies relying on this framework see: https://www.privacyshield.gov/list. Accessed 17 October 2020.

[12] CJEU, Case C-311/18 – Data Protection Commissioner v. Facebook Ireland Limited, Maxilimian Schrems (*Schrems II*), ECLI: EU:C:2020:559.

[13] 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, pp. 34-50.

binding opinion of the Advocate General (AG)[14] Henrik Saugmandsgaard Øe, which was delivered on 19 December 2020 (section 2). We then examine the outcome and legal essence of the recent CJEU's *Schrems II* decision[15] (section 3). This is followed by a discussion of how the decision may impact organizations which deploy cloud-based technologies that involve cross border transfers of data on EU data subjects, how the new legal environment can be navigated (section 4), and concluding remarks (section 5).

II. 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.[16] 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.[17]

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.[18]

---

[14] Opinion of the Advocate General Saugmandsgaard Øe, delivered on 19 December 2019 in Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems, ECLI:EU:C:2019:1145; see also CJEU Press Release No. 165/19 (19 December 2019), available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=49246 . Accessed 17 October 2020.

[15] CJEU, Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, ECLI:EU:C:2020:559 (*Schrems II*), available at: http://curia.europa.eu/juris/document/document_print.jsf?docid=228677&text=&dir=&doclang=EN&part=1&occ=first&mode=lst&pageIndex=0&cid=9710274 . Accessed 17 October 2020.

[16] 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, pp. 34-50.

[17] Cynthia O'Donoghue and Daniel Millard, 'Advocate General Gives Opinion on Schrems II: An Early Christmas Present? (19 December 2019), available at: https://www.technologylawdispatch.com/2019/12/in-the-courts/advocate-general-gives-opinion-on-schrems-ii-an-early-christmas-present/. Accessed 17 October 2020.

[18] 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, pp. 43-50.

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 of the EU-US Privacy Shield Framework 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 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.[19]

III. The *Schrems II* Judgment

The CJEU finally announced its much awaited *Schrems II* decision on 16 July 2020.[20] 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 on 6 October 2015 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's[21] 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 heavy burden on data exporters who rely 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 where the law of the third country allows its public authorities to interfere with the rights of the data subject to which the data relates. In these situations the CJEU underscored that organizations may need to implement supplementary measures beyond those contained in the SCCs in order to guarantee the necessary level of protection. The overarching goal is for the exporter and importer to compensate for any gaps in data protection in a third country (e.g., lack of an adequacy decision pursuant to

[19] Ibid, pp. 43-44.
[20] CJEU, Case C-311/18 - *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems,* ECLI:EU:C:2020:559 (*Schrems II*).
[21] Commission Decision 2010/87 of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593), OJ L 39, 12.2.2010, pp. 5-18.

Article 45 GDPR) by implementing the approved SCCs as well as the necessary supplementary measures to ensure a level of protection essentially equivalent to that guarantee under GDPR. 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. 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.[22]

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 doubt as to whether US law effectively ensures the adequate level of protection prescribed under Article 45 GDPR, with regard to the fundamental rights guaranteed by the CFR. The CJEU considered that US law (i.e., Section 702 FISA and EO 12333)[23] 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 Article 47 CFR.[24]

With regard to Articles 7 and 8 CFR, access to 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.[25]

IV. The Impact on Cross-border Data Transfers

1. General Considerations

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.

---

[22] Hunton Andrews Kurth, 'Breaking: Unexpected Outcome of the Schrems II case: CJEU Invalidates EU-US Privacy Shield Framework but Standard Contractual Clauses Remain Valid' (16 July 2020), available at: https://www.huntonprivacyblog.com/2020/07/16/breaking-unexpected-outcome-of-schrems-ii-case-cjeu-invalidates-eu-u-s-privacy-shield-framework-but-standard-contractual-clauses-remain-valid/. Accessed 17 October 2020.

[23] While Section 702 FISA deals with all "electronic communication service provider", Executive Order (EO) 12333 organizes electronic surveillance.

[24] Case C-311/18 (*Schrems II*) at paragraph 168. See also, CJEU Press Release No. 91/20 (16 July 2020).

[25] Case C-311/18 (*Schrems II*) at paragraphs 170 and 171. See also, CJEU Press Release No. 91/20 (16 July 2020).

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. If the controller comes to the conclusion that the SCCs and the application of supplementary measures cannot guarantee a level of protection essentially equivalent to that guaranteed withing the EU by GDPR, the data transfer should be suspended or ended. The same assessment and procedure should apply to the Binding Corporate Rules (BCRs) mechanism within companies belonging to the same group.[26] Consequently, this decision raises the threshold for international data transfers and puts more pressure on data controllers and data protection authorities (DPAs) to supervise and take enforcement actions. Additionally, companies should implement "supplementary measures"[27] in order to ensure compliance with adequate level of protection. Some contracts will likely have to be renegotiated to ensure those safeguard mechanisms are in place, especially to ensure compliance with the data protection (SCC Appendix 1) and security (SCC Appendix 2), including an assessment of the organizational and technical measures to ensure appropriate safeguards by the organization (in the absence of an "adequacy" decision at the country level).

The European Data Protection Board (EDPB) takes note of the primary responsibility of the exporter and the importer to ensure that the SCCs 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 transfer impact 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 supplementary 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 (when complemented with the SCCs obligations), the SCCs themselves and also the CFR. Thus, a transfer of personal data to a non-EU or EEA country can only be justified by SCCs when the result of the transfer impact assessment indicates that the law of third country when complemented with SCCs (as well as any required supplementary measures needed to compensate for the circumstances involving the particular transfer) guarantee an essentially equivalent level of data protection as in the EU.

In order to ensure compliance, the SCCs should be incorporated in as part of an overarching privacy and data protection framework to ensure overall GDPR compliance, including the implementation of organizational and technical measures to ensure security of processing (Article 32 GDPR) in light of the result of the Data Protection Impact Assessment (DPIA, Article 35). 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 Article 32 GDPR

[26] European Data Protection Board (EDPB), Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* adopted on 23 July 2020, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf. Accessed 17 October 2020.
[27] Case C-311/18 (*Schrems II*) at paragraph 133.

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 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."[28]

2. Pharmaceutical Section Considerations

In the context of medical products where the GDPR interplays with the Clinical Trial Regulation (CTR),[29] 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 Article 6(1)(c) and Article 9(2)(i) CTR "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 State inspections (Article 78 CTR) and Member State GCP inspectors are entitled to have access to clinical trial data, audit the protocol, etc. The sponsor and the contracted processors are obliged to follow the trial protocol authorized under the CTR legal obligations. This protocol defines the purposes and conditions for which the data of clinical trial subjects will be processed to ensure safety and reliability under CTR, including results reporting, safety reporting, and archival of the clinical trial master file for 25 years. Accordingly, given the stringent regulatory obligations regarding ICH/GxP, nature of the processing and oversight from regulatory authorities 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, especially when the companies implement a robust ISMS (e.g., ISO 27001) and PIMS (e.g., ISO 27701) properly complete the SCC's Appendix 1 & 2 specifying the organizational and technical measures to ensure an appropriate level of protection based on the risk and audited periodically. The IS0 27701 (the PIMS extension to the ISO 27001 ISMS) is well suited to become an approved GDPR "certification mechanism" under Article 40, which would create another "appropriate safeguards" cross-border transfer mechanism under Article 46(f).

Pharma sponsors (data controllers) and their clinical trial technology/service providers (processors) should review their records of processing activities (Article 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 pharmaceutical data controllers and processors are advised

[28] Case C-311/18 (*Schrems II*) at paragraph 143.

[29] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC, OJ L 158, pp. 1-76 (Clinical Trials Regulation), available at: https://ec.europa.eu/health/human-use/clinical-trials/regulation_en. Accessed 17 October 2020.

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.

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.

V. Outlook and Conclusions

There have been several new developments in the immediate aftermath of the *Schrems II* ruling. Among these, Max Schrems' NGO, "none of your business" (noyb) filed 101[30] identical complaints with multiple EU/EEA data protection authorities against major companies in 30 EU/EEA Member States. The complaints relate to the fact that many companies still use Google Analytics or Facebook Connect. According to Mr. Schrems, both companies (Google and Facebook) admit that they transfer data of European citizens to the US for processing. Neither of these services are essential to run the companies' websites. Thus, they could have been replaced or at least deactivated by now.[31] In response, on 4 September 2020, during its 37th plenary session,

[30] The link to the list of the 101 companies is available at: https://noyb.eu/en/eu-us-transfers-complaint-overview. Accessed 17 October 2020.

[31] The noyb website states that the reason for this is that: "A quick analysis of the HTML source code of major EU webpages shows that many companies still use Google Analytics or Facebook Connect one month after a major judgment by the Court of Justice of the European Union (CJEU) - despite both companies clearly falling under US surveillance laws, such as FISA 702. Neither Facebook nor Google seem to have a legal basis for the data transfers. Google still claims to rely on the "Privacy Shield" a month after it was invalidated, while Facebook continues to use the 'SCCs', despite the Court finding that US surveillance laws violate the essence of EU fundamental rights." See: '101 Complaints on EU-US transfers filed', available at: https://noyb.eu/en/101-complaints-eu-us-transfers-filed (17 August 2020). Accessed 17 October 2020.

the EDPB has created a task force to respond these complaints and a task force committed to prepare recommendations to aid data controllers and processors with their duty to identify and implement the supplementary measures that data exporters and importers can be required to take to ensure adequate protection when transferring data. In addition, the EDPB adopted new Guidelines to clarify the concepts of controller and processor, in particular the concept of joint controllership, and Guidelines on the targeting of social media users.[32]

On July 29th, 2020 the EDPB adopted a statement during its 34th plenary session on *Schrems II*.[33] 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. Given the legal issues associated the EU-US Privacy Shield under EU and US law (beyond the concerns of US government surveillance), the European Commission and the US could also consider a sector-specific adequacy decision under Article 45 GDPR for international transfers of health data based on the existing US health privacy law, the Health Insurance Portability and Accountability Act (HIPAA).[34]

Unfortunately, the *Schrems II* judgment is far from illuminating and the ruling has resulted 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 and updated SCC guidelines are now needed to establish 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* as part of their cross-border transfer impact assessment. Especially problematic is the fact that the CJEU did not specify the nature or types of "supplementary measures" beyond the SCC safeguards already included as part of the SCC clauses and SCC Appendix 2 (i.e., the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c)). Since the controller/processor are subject to GDPR when processing

---

[32] European Data Protection Board (EDPB) – Thirty-Seventh Plenary Session: Guidelines controller-processor, Guidelines targeting social media users, taskforce complaints CJEU Schrems II judgement, taskforce supplementary measures. Available at: https://edpb.europa.eu/news/news/2020/european-data-protection-board-thirty-seventh-plenary-session-guidelines-controller_en (14. Accessed 17 October 2020.

[33] European Data Protection Board (EDPB), statement during the 34th plenary session, available at: https://edpb.europa.eu/news/news/2020/european-data-protection-board-thirty-fourth-plenary-session-schrems-ii-interplay_sv. Accessed 17 October 2020.

[34] Laura Bradford, Mateo Aboy and Kathleen Liddell, 2020, International transfers of health data between the EU and USA: a sector-specific approach for the USA to ensure an 'adequate' level of protection, *Journal of Law and the Biosciences,* October 2020, pp. 1-33.

data from EU subjects, these measures (documented as part of the SCC Appendix 2) should already include the controls to ensure a level of security appropriate to the risk (documented as part of the Article 35 DPIA) such pseudonymization and encryption of personal data, as well as the information security controls designed to satisfy the security of processing (Article 32 GDPR) and other GDPR requirements. Accordingly, it is particularly important for the EDPB to clarify and provide illustrative examples of the types of "supplementary measures" needed in addition to SCC's to complement any Article 45(2) data protection gaps in the non-EEA third country that need to be compensated by SCCs and the associated "supplementary measures" to afford a level of protection essentially equivalent to that guaranteed within the EU.

In the specific context of pharmaceutical clinical trials, the required compliance with strict legal and regulatory requirements such as the EU CTR, as well as the implementation of GxP controls and guidelines from the International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use (ICH) helps provide additional safeguards for clinical trial data. GDPR contemplates several "appropriate safeguards" mechanism under Article 46, including GDPR-compliant SCCs, Codes of Conduct and Certification Mechanisms. Unfortunately, despite the explicit GDPR mandate to the EDPB and European Commission (e.g., Board and the Commission shall encourage the establishment of data protection certification mechanisms) these mechanisms are still not available for controllers and processors. That said, the ICH is unique in bringing together the international regulatory authorities and pharmaceutical industry to evaluate scientific and technical aspects of pharmaceutical trials and develop ICH guidelines. Accordingly, the ICH is specially well positioned to propose an Article 40 "Code of Conduct for Data Protection in International Clinical Trials" in order to ensure an appropriate level of data protection and provide a sector-specific "appropriate safeguards" mechanism for cross-border transfers of clinical trial data under Article 46(e) GDPR. Pursuant to Article 40(1), the EDBP and the Commission should encourage the drawing up of Codes of Conduct intended to contribute to the proper application of GDPR taking account of the specific features of the various processing sectors. Similarly, the development of an Article 42 GDPR "Certification" mechanism is needed in order to enable cross-border transfers pursuant to adequate safeguards under Article 46(f).