The EU-US Privacy Shield Regime for Cross-Border Transfers of Personal Data under the GDPR

What are the legal challenges and how might these affect cloud-based technologies, big data, and AI in the medical sector?

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

Cloud-based technologies, big data, statistical signal processing algorithms, and Artificial Intelligence (AI) technologies are expected to play an increasingly important role in the medical field. Big data and AI-technologies rely on the cloud for data storage as well as for computational power and thus need effective and robust legal frameworks for international data transfer. Because of inconsistent data protection regulations, this is not always simple to achieve as it can be illustrated in the United States (US)-European Union (EU) context. Due to the lack of general data protection law at the federal level, the US currently does not have a general 'adequacy decision' from the European Commission to enable EU-US cross-border data transfers without the need for additional data protection safeguards under the General Data Protection Regulation. As a fallback, a 'limited adequacy' decision was adopted in 2016 on the so-called 'EU-US Privacy Shield Framework'. This framework protects the fundamental rights of natural persons in the EU and allows the free transfer of personal data to companies that are certified under the EU-US Privacy Shield. However, the EU-US Privacy Shield has been recently contested at the Court of Justice of the European Union (CJEU). This paper analyses the EU-US Privacy Shield Framework, the associated legal challenges, and how these might affect organisations deploying or implementing cloud-based medical technologies relying on cross-border data transfers from EU data subjects.

I. Introduction

The extraordinary expansion and upsurge of cutting-edge information technologies over the last decade has created opportunities for companies and research organisations to collect, process, transfer, and share enormous volumes of data across multinational borders. Among these technologies, big data algorithms, artificial intelligence (AI), and machine learning (ML) systems are predicted to have a significant impact on the digital transformation of the healthcare and pharma sectors, especially for the development and application of medical devices, novel drugs, and precision medicine. The application of advanced algorithms, big data techniques, and AI technologies has several potential advantages such as more efficient diagnosis and drug development programs. The general aim of these computer and data intensive methods in the medical field is to use algorithms to uncover relevant information from data and to assist

DOI: 10.21552/eplr/2020/1/6

* 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). 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, Senior Research Scholar at the LML (University of Cambridge, UK), affiliated Professor & Fellow at the CeBIL (University of Copenhagen), and Visiting Scholar at the Petrie-Flom Center (Harvard Law School). Marcelo Corrales Compagnucci, Post Doc, Center for Advanced Studies in Biomedical Innovation Law (CeBIL). For Correspondence: <timo.minssen@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)

clinical decision-making in order to perform a wide array of functions, such as aiding in diagnosis generation and therapy selection, making risk predictions and stratifying disease, reducing medical errors, and improving productivity.[1] Yet, some of the underlying principles of EU General Data Protection Regulation (GDPR) including data limitation (Art 5.1.(c)) and purpose limitation (Art 5.1.(b)) are fundamentally misaligned with some of the underlying principles of big data and AI. For example, a foundational principle of big data, statistical learning algorithms and AI is to collect as much data as possible (ie, data maximization) and allow the algorithms to 'discover' previously unknown relationships (ie, purpose extension).

Additionally, the GDPR limits cross-border data flows of personal data (Art. 44 GDPR). This impacts computational intensive big-data technologies, such as medical AI/ML that rely heavily on cloud-based solutions for 1) data storage and 2) computational power. Cloud computing offers the underlying IT infrastructure to enable these advanced algorithms to operate on medical big data[2] with the ultimate objective of improving precision medicine, clinical trials, medical records, medical devices, and the overall experience and engagement with patients.[3] The pervasive and dynamic nature of the cloud often results in cross-border data transfers through a flexible distributed network of infrastructure and service providers.[4] This enables organisations to deploy a broad spectrum of digital technologies such as wearables, implantable medical devices or ingestible electronics.[5] Examples of this abound and several projects have demonstrated the benefits of AI/ML in medical cloud-based applications. For instance, the EU funded OPTIMIS project[6] ran a use case scenario, which tested how a cloud-based application could perform the processing of big data analytics in genomic sequencing. Consider then a scenario where several hospitals and medical research institutions attempt to make use of secondary data to detect the DNA sequencing of a particular disease. The cloud-genomic application enabled a workflow that performed automatic gene detection considering a specific genome analysis (Genewise) which was able to identify the gene patterns. The whole process involved a supple network of cloud-accessible databases based on algorithms that could analyse and predict the gene structure.[7] Such projects, and the use of wearables and AI, often results in intrinsic cross-border data flows due to the use of cloud-computing. Another example are clinical trials where pharmaceutical and medical device companies conducting trials in the EU need to transfer the data to the US FDA for regulatory and supervision purposes. Moreover, having multi-site trials is a necessity in many clinical trials, such as clinical trials on rare diseases where globally distributed trials are the norm in order to have enough subjects to conduct the trials.[8]

The recent digital medicine transformation thus offers the healthcare and pharmaceutical sector new opportunities, but also challenges data protection laws to adapt. Exchange of patient data in international collaborations and international multi-site clinical trials result in cross-border data-flows, which often raise complex legal issues, including the way the law is interpreted and applied in the fields of data ownership, privacy, and data protection law.

As indicated before, the GDPR[9] does not only protect personal data from EU data subjects within the EU but also imposes stringent rules for transfers of personal data outside of the EU and the European Economic Area (EEA) Member States (Norway, Liechtenstein and Iceland). The EU Commission has

1 Jianxing He, Sally L Baxter, Jie Xu, Jiming Xu, Xingtao Zhou and Kang Zang, 'The Practical Implication of Artificial Intelligence Technologies in Medicine' (2019) Nature Medicine 25, 30-26.

2 Min Chen, *Big Data: Related Technologies, Challenges and Future Prospects* (Springer, 2014) 12.

3 Claudia Rijcken, 'Sequoias of Artificial Intelligence' in Claudia Rijcken (ed) *Pharmaceutical Care in Digital Revolution: Insights Towards Circular Innovation* (Elsevier, 2019) 127.

4 Kijpokin Kasemsap, *The Role of Cloud Computing Adoption in Global Business*, in: Victor Chang, Robert Walters and Gary Wills (eds) *Delivery and Adoption of Cloud Computing Services in Contemporary Organizations* (IGI Global, 2015), 31.

5 See S Gerke, T Minssen, H Yu et al, 'Ethical and Legal Issues of Ingestible Electronic Sensors' (2019) Nat Electron 2, 329-334; Supriya Biswas, *Relationship Marketing: Concepts, Theories and Cases* (2nd ed., Learning Private Ltd., 2014), 333.

6 Optimized Infrastructure Services (OPTIMIS) was an EU funded project within the 7th Framework Program under contract ICT-257115.

7 Marcelo Corrales Compagnucci, Big Data, Databases and 'Ownership' Rights in the Cloud (Springer 2019), 231.

8 Cf. Mulberg, A.E., Bucci-Rechtweg, C., Giuliano, J. *et al.* Regulatory strategies for rare diseases under current global regulatory statutes: a discussion with stakeholders. *Orphanet J Rare Dis* 14, 36 (2019). https://doi.org/10.1186/s13023-019-1017-5; Day S, Jonker AH, Lau LPL, et al. Recommendations for the design of small population clinical trials. Orphanet J Rare Dis. 2018;13(1):195. Published 2018 Nov 6. doi:10.1186/s13023-018-0931-2.

9 Regulation (EU) 2016/679 of the European Parliament 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, 1 (General Data Protection Regulation, GDPR).

the power to determine, on the basis of Article 45 GDPR whether a country outside the EU offers an adequate level of data protection.[10] Because of the high data protection standards of the GDPR any intended data transfer to third countries needs to be permitted according to the regulations of the GDPR. The EU Commission differentiates between adequate and non-adequate third countries: Adequate third countries are those for which the EU Commission has confirmed a suitable level of data protection on the basis of an adequacy decision which declares that the level of protection in the third country is comparable to those of the GDPR.

The EU does not consider the US as one of the countries outside the EU and the EEA that provides an adequate level of *general* data protection to permit transfer without additional safeguards such as in the case of Switzerland[11] or Japan.[12] In these cases, the adequacy decision expressly permits data transfer to these third countries. In order to permit transfer of personal data without additional safeguards, a *limited* 'adequacy decision' on the EU-US Privacy Shield Framework[13] was adopted on 12 July 2016, which came into force on 1 August 2016. This Framework allows the free transfer of personal data to companies that are certified in the US under the EU-US Privacy Shield.[14] As one of the few possible legal mechanisms that companies can employ to lawfully engage in cross-border data transfers between the EU and US, the Framework is being widely used by companies in the healthcare and pharmaceutical sector.

The EU-US Privacy Shield Framework was designed after the failure of the Safe Harbour Program as a consequence of the *Schrems* I Court of Justice of the European Union (CJEU) judgment, for allegedly violating EU user's privacy rights due to, *inter alia*, mass surveillance programs in the US. In summary, the CJEU ruled that legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life under the GDPR. In addition, the CJEU observed that the US legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection, the existence of such a possibility being inherent in the existence of the rule of law.

However, the EU-US Privacy Shield Framework has been recently contested in a follow-up case now pending before the CJEU (*Schrems* II). The Advocate General (AG) *Henrik Saugmandsgaard Øe's* Opinion in this case is that the subject matter of the main proceedings does not relate directly to the EU-US Privacy Shield Framework. Yet, the AG casted doubt with regard to the adequate level of protection of data transferred from the EU under such a system, in particular where data transferred to the US could be accessed by US intelligence agencies and judicial authorities. The AG's Opinion may be influential, however, it is not legally binding. Therefore, the CJEU could still potentially invalidate the EU-US Privacy Shield Framework, resulting in transfers of personal data between the EU and US no longer lawful.

Given that the EU-US Privacy Shield Framework is already the major mechanism employed by pharmaceutical companies to legally transfer clinical trial data between the EU and the US, the potential invalidation of the Privacy Shield could lead to significant disruptions. Since it is the only Art. 45 GDPR mechanism available by adequacy decision to legally transfer data between the EU and the US, the robustness of this system and legal certainty is crucial for multi-site international clinical trials in the context of drug approvals. The ongoing legal challenge therefore poses great legal risk to companies currently relying on the adequacy of this cross-border mechanism and may affect, in particular, the deployment of cloud-based big data and AI technologies relying on cross-border data transfers between the EU and the US.

---

10 The adoption of an adequacy decision involves a proposal from the EU Commission,an opinion of the EU Data Protection Board, an approval from representatives of EU Member States and the adoption of the decision by the European Commission

11 Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, OJ L 215 [2000] 1.

12 Commission Implementing Decision (EU) of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, OJ L 76, [2019] 1.

13 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 (notified under document C(2016) 4176). <https://ec.europa.eu/info/sites/info/files/celex_32016d1250_en_txt.pdf> accessed 10 November 2019.

14 Robert Walters, Leon Trakman and Bruno Zeller, *Data Protection Law: A Comparative Analysis of Asia-Pacific and European* (Springer, 2009) 281.

In light of this complex background, *section 2* starts out by explaining various cross-border transfer mechanisms and the EU-US Privacy Shield Framework. Next, *section 3* provides a historical overview and contextual background to the recent legal developments that have resulted in the current legal uncertainty, including the recent AG's Opinion in the *Schrems II* case. *Section 4*, follows-up with an overview on recent US developments and litigations that might be relevant for the ongoing European litigation. *Section 5* then provides a summary of the European Commission's most recent annual evaluation of the Privacy Shield Agreement. *Section 6* discusses the impact and potential effects of the pending litigations and uncertainties, as well as potential ways how to address these or alternative routes. This will provide the basis for our conclusions in *section 7*.

II. Cross-Border Transfer Mechanisms and the EU-US Privacy Shield Framework

The GDPR lays down rules relating the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Pursuant to Art. 1 GDPR it protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. Personal data means any information relating to a 'data subject' who is an identified or identifiable natural person that can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Art. 4(1) GDPR).

Transfers of personal data to countries outside the EU and EEA are only lawful if the conditions specified in Chapter 5 of the GDPR are complied with by the controller and processor. Pursuant to Art. 44 GDPR 'All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.' Art. 45-50 GDPR detail the available legal instruments and associated conditions for lawful cross-border transfers. These include:

1. Transfers on the basis of an 'adequacy decision' by the European Commission (Art. 45);
2. Transfers subject to 'appropriate safeguards' by the controller/processor on condition that enforceable data subject rights and effective legal remedies for data subjects are available (Art. 46, Art. 47); and
3. Derogations for specific situations (Art. 49).

In effect, these mechanisms are intended to ensure that either 1) the country (adequacy decision) or 2) the organisation safeguards with appropriate standard contract clauses ('SCCs') and binding corporate rules ('BCRs') ensure an appropriate level of data protection to the data subject. In this paper, we focus on transfers on the basis of an adequacy decision (Art. 45 GDPR) in the context of EU-US data transfers.

1. Transfers on the Basis of an 'Adequacy Decision'

Pursuant to Art. 45 GDPR, the EU Commission has the power to determine whether a country outside the EU offers an adequate level of data protection. The adoption of an adequacy decision involves several steps, namely: 1) a proposal from the EU Commission, 2) an opinion of the European Data Protection Board (EDPB), 3) an approval from representatives of EU Member States, and 4) the adoption of the decision by the EU Commission.

The effect of these adequacy decisions is that personal data of the subject data can be transferred from the EU and the EEA to that third country without any further safeguards such as a special authorisation for each specific case. At the time of this writing, the EU Commission has recognised Andorra, Argentina, Canada (for commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay as providing adequate protection. Discussions are ongoing with South Korea.[15]

The general adequacy determination for the US is complicated by the fact that the US does not have Federal general data protection legislation. Instead, the US has sector specific privacy and data protection regimes at the federal level (eg, HIPAA, FERPA)

15 An overview of the adequacy decisions and the non-EU Member States with an adequate level of data protection is available at <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 10 November 2019.

and state privacy and data protection laws (eg, CCPA). That said, Art. 45(1) GDPR states that:

> 'A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.'

Accordingly, adequacy decisions can be limited to a territory or specific sectors within a third country. This enabled the International Trade Administration (ITA) within the US Department of Commerce (DOC) and the EC to provide organisations with a mechanism to comply with data protection requirements when transferring personal data from the EU or EEA to the US on the basis of a 'limited adequacy decision' ('United States *limited to* Privacy Shield Framework' adequacy) for companies that *voluntarily* choose to adopt this privacy framework. US-based companies subject to the jurisdiction of the US Federal Trade Commission or the Department of Transportation can join the EU-US Privacy Shield Framework in order to benefit from the 'adequacy determination'.

2. Practical Aspects of the EU-US Privacy Shield Framework

US-based organisations may join the Privacy Shield Frameworks (EU-US & Swiss-US Frameworks) by 1) publicly committing to complying with the Framework's requirements and 2) submitting a self-certification to the DOC. These commitments are enforceable under US law.

To join either Privacy Shield Framework (US or Swiss), a US-based organisation will be required to self-certify to the DOC and publicly commit to comply with the Framework's requirements. Once an eligible organisation makes the public commitment to comply with the Framework's requirements, the commitment becomes enforceable under US law. The requirements include: 1) informing individuals about data processing, 2) providing free and accessible dispute resolution, 3) cooperating with the DOC, 4) maintaining data integrity and purpose limitation, 5) ensuring accountability for data transferred to third parties, 6) transparency related to enforcement actions, and 7) ensuring commitments are kept as long as data is held. With regards to the transparency requirements, the company must adopt a privacy policy that contains 13 specified details about its privacy practices and must provide the DOC with a draft privacy policy at the time that it submits its first self-certification.

This privacy policy must comply with the Privacy Shield Framework(s) principles (7 main principles and 16 supplementary principles), and include a link to the DOC Privacy Shield website[16] as well as a link to the 'complaint submission form of the independent recourse mechanisms that is available to investigate individual complaints'. If the company does not follow the requirements of the Privacy Shield Framework and violates one of the data protection obligations, data subjects have the right to complain and obtain a remedy. Privacy Shield companies are required to provide an independent recourse mechanism to investigate unresolved complaints (eg, an alternative dispute resolution (ADR) or submit to the oversight of an EEA national DPA). In summary, the Framework requires greater transparency, oversight, and redress mechanisms which include the involvement of DPAs, DOC, and FTC to ensure unresolved complaints by European data subjects are investigated and resolved.

III. Historical Context and the Legal Developments

As it turns out, however, the current EU-US Privacy Shield Framework is facing considerable legal challenges. These are partially founded in the complex history of cross-national US-EU data transfer regimes, and partially in recent events and developments. The background of fundamental legal challenges can be found in the different standards for the protection of personal data as well as in the different regulations for online privacy and data transfers in the US and the EU.[17]

---

16 <https://www.privacyshield.gov/welcome> accessed 10 November 2019.

17 Sherri J Deckelboim, 'Consumer Privacy on an International Scale: Conflicting Viewpoints underlying the EU-US Privacy Shield Framework and how the Framework will impact Privacy Advocates, National Security, and Businesses' (2016 - 2017) 48 Geo J Int'l L, 263.

Data Protection Regulations in the US are fragmented. The US follows a different approach to data protection compared to the GDPR as a general standard of the protection of personal data in the EU. There is no Federal legislation on US data protection. Instead of formulating one all-encompassing regulation such as the GDPR, the US system implements sector specific data protection laws and regulations. As a consequence, US data protection legislation may partly be up to GDPR standards, while other parts may not.

In addition to this fundamental different approach in protecting personal data there have been several recent events and data protection scandals. One of the most recent event was the *Facebook – Cambridge Analytica* data scandal in early 2018 where *Cambridge Analytica* had misused the personal data of millions of peoples' *Facebook* profiles without their consent and used it for political advertising purposes.[18] This scandal has led to an ongoing discussion on the potential misuse of personal data by tech companies collecting a huge amount of personal data. Although the data misuse in the context of the *Cambridge Analytica* scandal happened before the application of the GDPR, the scandal has led to a Motion for a Resolution by the European Parliament (EU Parliament) on 10 October 2018. The purpose of this Motion was to wind up the debate on the statement by the EU Commission on the use of *Facebook* users' data by *Cambridge Analytica* and the impact on data protection.[19] In this motion the EU Parliament stated that it:

> 'Expects all online platforms to ensure full compliance with EU data protection law, namely the GDPR and Directive 2002/58/EC (e-Privacy), and to help users understand how their personal information is processed in the targeted advertising model, and that effective controls are available, which includes ensuring that separate consents are used for different purposes of processing, and that greater transparency is in place in relation to the privacy settings, and to the design and prominence of privacy notices.'

In addition, the European Parliament noted that:

> 'Notes that the misuse of personal data affects the fundamental rights of billions of people around the globe; considers that the GDPR and the e-Privacy Directive provide the highest standards of protection; regrets that Facebook decided to move 1.5 billion non-EU users out of the reach of the protection of the GDPR and the e-Privacy Directive; questions the legality of such a move; urges all online platforms to apply the GDPR (and e-Privacy) standards to all of their services, regardless of where they are offered, as a high standard of protection of personal data is increasingly seen as a major competitive advantage'.

The different understanding and approach of the protection of personal data in the EU and the US and in addition the recent scandals had some impacts on the trust of the EU and its citizens concerning an adequate protection of their personal data in the US.

1. Safe Harbour Agreement

Prior to the aforementioned EU-US Privacy Shield Framework the EU and US had agreed on the International Safe Harbour Privacy Principles ('Safe Harbour Agreement')[20] back in 2000. The Safe Harbour Agreement guaranteed the possibility for US companies storing customer data to self-certify that they comply with the principles of the EU Data Protection Directive ('Directive').[21]

18 Jim Isaak and Mina J Hanna, 'User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection' IEEE Computer 51(2018), 56-59.

19 EU Parliament, Procedure 2018/2855(RSP), of 16 October 2018 <http://www.europarl.europa.eu/doceo/document/B-8-2018-0480_EN.html?redirect>

20 See the Commission communication to the European Parliament and the Council entitled 'Rebuilding Trust in EU-US Data Flows' (COM(2013) 846 final) ('Communication COM(2013) 846 final') of 27 November 2013.

21 The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281, 355 ('EU Data Protection Directive'). The GDPR has superseded the EU Data Protection Directive and became enforceable on 25 May 2018. The Directive provided that the transfer of personal data to a third country may take place only if that third country ensures an adequate level of protection of the data. Furthermore, it made clear that the EU Commission had the power to assess whether a third country ensures an adequate level of protection according to its domestic law or its international commitments and that each EU Member State should designate public authorities that are responsible for monitoring the application of the national provisions which have been adopted according the Directive. Based on this Agreement the EC adopted the Safe Harbour Decision (Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 /EC of the European Parliament and of the Council on the adequacy of the protection provided by the ´safe harbour` privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000 L 215, 7.). According to which the EC confirmed that the US data protection principles did comply with the Directive.

In its first landmark judgment, the CJEU clarified general principles of EU data protection and their application towards third countries. The CJEU declared in his judgment *Maximillian Schrems v Data Protection Commissioner* of 6 October 2015 ('*Schrems I*')[22] the Safe Harbour Agreement to be invalid. In summary, the judgment of the CJEU confirmed the EC's approach since November 2013 to review the Safe Harbour Agreement, to ensure a sufficient level of data protection as required by EU data protection law.

The judgment was preceded by a legal dispute on the adequacy of the US data protection regarding personal data transferred to the US. *Maximillian Schrems*, an Austrian citizen and a former Facebook user, lodged a complaint with the Irish Data Protection Commissioner (DPC) and argued that the law and practice of the US do not guarantee sufficient protection against surveillance by the public authorities of the data transferred to the US.[23] The DPC, however, rejected this complaint and took the view that the EC had already considered in the Safe Harbour Decision that under the Safe Harbour Agreement the US ensures an adequate level of protection of the personal data transferred.[24] The CJEU held that the existence of a Commission decision finding that a third country ensures an adequate level of protection of the personal data transferred cannot eliminate or reduce the powers available of the national supervisory authorities under the CFR and the Directive.[25] In addition, the CJEU pointed out that even if the EC has adopted a decision, the national supervisory authorities must be able to examine, with complete independence, whether the transfer of a person's data to a third country complies with the requirements laid down by the Directive.[26]

In the context of the validity of the Safe Harbour Decision, the CJEU held that the EC was required to find that the US in fact ensures in their domestic law and in accordance with international commitments a level of protection of fundamental rights essentially equivalent to the guaranteed rights within the EU under the Directive.[27] However, the CJEU pointed out, that the obligations were solely applicable to US undertakings and not to US public authorities and that the national security, public interest and law enforcement requirements in the US prevailed over the safe harbour scheme under the Safe Harbour Agreement, so that the US undertakings were bound to disregard, without limitations, the protection rules laid down by that scheme where they conflict with such requirements.[28] As a consequence, the US safe harbour scheme enabled interference by US public authorities with the fundamental rights of persons as guaranteed in the EU.[29]

The CJEU held in regard of the level of protection that legislation which permits public authorities to have access on a general basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life.[30] In addition, legislation which does not provide any possibility for an individual to pursue legal remedies to have access to personal data or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection inherent in the existence of the rule of law.[31] Finally, the CJEU found that the EC did not have competence to restrict the national supervisory authorities' powers to deny them their powers where a person calls into question whether the decision is compatible with the protection of the privacy and the fundamental rights and freedoms of individuals.[32]

---

22 CJEU, C-362/14 of 6 October 2015, ECLI:EU:C:2015:650 – Maximillian Schrems vs Data Protection Commissioner. The Schrems I judgment has been widely discussed, eg see Federico Fabbrini, 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the US' (2015) 28 Harvard Human Rights Journal, 65; Orla Linskey, The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: digital rights Ireland. Joined Cases C-293 & 594/12, Digital Rights Ireland Ltd and Seitlinger and others, Judgment of the Court of Justice (Grand Chamber) of 8 April 2014, CMLR 2014, 51; Yann Padova, 'La Cour de justice de l´Union européenne va-t-elle invalider les accords Safe Harbour?, Droit de l´immateriel – informatique, medias, communiation' 2014, n° 110, 14; Tuomas Ojanen, *Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter*, Cambridge University Press, July 28, 2016; Xavier Tracol, 'Legislative genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it' (2014) 30 Computer Law & Security Review 6, 736.

23 CJEU, C-362/14, (n 4) para 27, 28.

24 CJEU, C-362/14, (n 4) para 29.

25 CJEU, C-362/14, (n 4) para 53.

26 CJEU, C-362/14, (n 4) para 57.

27 CJEU, C-362/14, (n 4) para 69.

28 CJEU, C-362/14, (n 4) para 84.

29 CJEU, C-362/14, (n 4) para 87.

30 CJEU, C-362/14, (n 4) para 94.

31 CJEU, C-362/14, (n 4) para 95.

32 CJEU, C-362/14, (n 4) para 103.

With this judgment the CJEU has tried to strengthen the data protection law in the EU. Whereas Article 7 CFR contains the right to respect for private life Article 8(1) CFR guarantees that everyone has the right to the protection of personal data concerning him or her, whereas Article 8(2) CFR provides that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some legitimate basis laid down by law. In addition, Article 8(2) CFR guarantees that everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.[33] All these fundamental rights would have been compromised if the CJEU had decided otherwise.

2. EU-US Privacy Shield Agreement

In the wake of the CJEU judgment the EU Commission and the US agreed on 2 February 2016 the EU-US Privacy Shield with the objective to ensure data protection rights of EU citizens where their data is transferred to the US by including data protection obligations on companies receiving personal data from the EU as well as protection and redress measures for individuals and regulations for safeguards on US government access to data.[34] The objective of this framework was to ensure legal certainty for companies. The new EU-US Privacy Shield aims to reflect the requirements set out by the CJEU ruling in *Schrems* I by providing stronger obligations of US companies to protect personal data of EU citizens.

3. EU-US Privacy Shield & EU Model Clauses (*Schrems* II)

Six years later after privacy activist *Max Schrems* filed a legal suit (Schrems I) and asked the regulator whether *Facebook's* data transfer was in breach of the EU data protection law and EU citizens' fundamental rights, the case was taken before the CJEU again on 9 July 2019.[35] This case could potentially strike down two of the most important mechanisms to transfer data to third countries: i) the EU Model Standard Contractual Clauses (SCCs); and, ii) the EU-US Privacy Shield Framework. Thus, this could significantly disrupt the current legal framework and rewrite data protection law regarding trans-Atlantic data transfers outside of the EU/EEA Member States.[36]

The main parties involved in the *Schrems* II case[37] were: the Irish DPC (applicant), *Facebook Ireland Ltd.*, and *Maximilian Schrems* (defendants). Moreover, several other stakeholders participated in the hearing, including representatives from the European Parliament, the European Commission, the European Data Protection Board (EDPB), various EU Member States (Austria, Germany, Ireland, France, the Netherlands and the UK), the US Government and several other industry representative groups.[38]

a. EU Model Standard Contracting Clauses (SCCs) in Schrems II

Following the CJEU decision in *Schrems I*, several organisations (including Facebook) claimed that they were using the SCCs as an alternative mechanism to transfer data to third countries. The SCCs or 'model clauses' are valuable legal mechanisms for transferring data outside of the EU/EEA. Using these templates provide further evidence of sufficient safeguards on data protection within the scope of the GDPR.[39] The SCCs are by far the most ubiquitous and widely adopted data transfer systems currently used by hundreds of organisations in many countries

33 See also Claudia Seitz, 'Big Data in the pharmaceutical sector – Current developments and legal challenges' in Gert Vermeulen and Eva Lievens (eds.), *Data Protection and Privacy under Pressure – Transatlantic tensions, EU surveillance, and big data* (Maklu, 2017) 293 (306/307).

34 See EU Commission, EU-US data transfers – How personal data transferred between the EU and US is protected, <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en>.

35 John Oates, 'Facebook and Max Schrems Back in Court Again, Both Pissed Off at Ireland's Data Regulator' (10 July 2019) <https://www.theregister.co.uk/2019/07/10/irish_regulator_feels_heat_over_facebook_schrems_case/> accessed 10 November 2019.

36 DLA PIPER, 'Schrems 2.0 – The Demise of Standard Contractual Clauses and Privacy Shield?' (1 July 2019) <https://blogs.dlapiper.com/privacymatters/schrems-2-0-the-demise-of-standard-contractual-clauses-and-privacy-shield> accessed 10 November 2019.

37 Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 *Data Protection Commissioner v Facebook Ireland Limited , Maximillian Schrems* Case C-311/18.

38 Hunton Kurth, 'The Schrems Saga Continues: Schrems II Case Heard Before the CJEU' (10 July 2019), available at: https://www.huntonprivacyblog.com/2019/07/10/the-schrems-saga-continues-schrems-ii-case-heard-before-the-cjeu/ (accessed 10 November 2019).

39 Marcelo Corrales, Paulius Jurčys and George Kousiouris, 'Smart Contracts and Smart Disclosure: Coding a GDPR Compliance Framework' in Marcelo Corrales, Mark Fenwick and Helena Haapio (eds), *Legal Tech, Smart Contracts and Blockchain* (Springer, 2019) 212.

around the world.[40] SCCs allow EU Member States to transfer data safely to third countries using a set of unmodified standard clauses provided by the EU Commission. There are currently two sets of SCCs for data controllers established in the EU who want to transfer data to data *controllers* outside of the EU/EAA countries.[41] In addition, the EU Commission has also issued one set of SCCs for controllers established in the EU who want to transfer data to data *processors* outside the EU/EEA countries.[42]

The repercussions of *Schrems*, I lead the Irish DPC to request *Maximilian Schrems* to reformulate and amend his complaint since the EU-US Safe Harbour Framework has been ruled invalid. *Maximilian Schrems* contested the fact that personal data is now being transferred from *Facebook Ireland Ltd.* to *Facebook Inc.*, in the US by using the SCCs. The arguments were similar to those raised in the *Schrems* I case.[43] The Irish DPC brought the legal proceedings before the Irish Hight Court, which sought the CJEU advice and referred a series of questions for a preliminary ruling.[44]

During the hearing, the validity of the SCCs was critically and extensively discussed. There were many supporters of maintaining the SCCs Framework. The main partisans included the EU Commission, industry associations, and the governments of Ireland, France, Germany, etc. They argued that using the 'model clauses' provide sufficient safeguards to transfer data safely outside the EU/EEA countries and should not be invalidated. Even *Maximilian Schrems's* was in favor of keeping this mechanism. According to *Maximilian Schrems's* lawyer, 'the solution is not for the court to invalidate standard contractual clauses but for the DPC to enforce them.'[45] This means that for *Maximilian Schrems's* the mechanism is not the problem. He questioned *Facebook's* appropriate use of the SCCs and urged the Irish DPC to suspend it.[46]

The arguments in favor pointed to the fact that even if the laws of third countries do not provide an adequate level of data protection, the SCC's safeguards should. Such safeguards include the existence of data subject rights, strict obligations on the controllers and processors to ensure compliance with EU law and the crucial role of DPCs in enforcing the SCCs, including the discretional power to suspend data transfers. The rationale behind the SCCs framework is that the data exporter and data importer take on full responsibility and are therefore under a contractual obligation to provide the appropriate safeguards.[47] The supporting group also requested the CJEU to make separate judgments on the SCCs and its analysis of third country laws (in particular US law), which they claimed is independent and irrelevant in this case.[48]

It was clear from the discussion that rendering the SCCs void would totally disrupt data transfers from the EU with very serious collateral damages which would affect competitiveness and the normal func-

40 DLA PIPER, 'Schrems 2.0 – The Demise of Standard Contractual Clauses and Privacy Shield?' (1 July 2019) <https://blogs.dlapiper.com/privacymatters/schrems-2-0-the-demise-of-standard-contractual-clauses-and-privacy-shield/> accessed 10 November 2019.

41 Standard Contractual Clauses for Data Transfers Between EU and non-EU Member States <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en>; Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (notified under document number C(2001) 1539) (Text with EEA relevance) (2001/497/EC); Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271).

42 Commission Decision 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).

43 Noyb, 'CJEU Hears Case on EU-US Data Transfers (Standard Contractual Clauses and Privacy Shield)' Noyb (8 July 2019) <https://noyb.eu/en/cjeu-hears-case-eu-us-data-transfers-standard-contractual-clauses-and-privacy-shield> accessed 10 November 2019.

44 Reference for a preliminary ruling from the High Court (Ireland) made on 9 May 2018 – *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (Case C-311/18), <http://curia.europa.eu/juris/document/document.jsf?text=&docid=204046&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6462885> accessed 10 November 2019.

45 Simon Mortier and Benoit Van Asbroeck, 'Notes from the CJEU hearing on SCCs: Schrems C-311/18 CJEU Hearing of 9 July 2019' (July 2019) <https://www.twobirds.com/en/news/articles/2019/global/notes-from-the-cjeu-hearing-on-sccs> accessed 10 November 2019.

46 Noyb, 'CJEU hears case on EU-US data transfers (Standard Contractual Clauses and Privacy Shield)' (8 July 2019) <https://noyb.eu/en/cjeu-hears-case-eu-us-data-transfers-standard-contractual-clauses-and-privacy-shield> accessed 10 November 2019.

47 Simon Mortier and Benoit Van Asbroeck, 'Notes from the CJEU hearing on SCCs: Schrems C-311/18 CJEU Hearing of 9 July 2019' (July 2019) <https://www.twobirds.com/en/news/articles/2019/global/notes-from-the-cjeu-hearing-on-sccs> accessed 10 November 2019.

48 Davina Garrod et al, 'The Case of Schrems 2.0 – The Challenge of Standard Contractual Clauses Allowing Personal Data Transfer Outside the European Union' (10 July 2019) <https://www.akingump.com/en/experience/practices/cybersecurity-privacy-and-data-protection/ag-data-dive/the-case-of-schrems-2-0-the-challenge-to-standard-contractual.html> accessed 10 November 2019.

tioning of EU organizations. Some parties, including *Maximilian Schrems's*, plead that it was for the DPC to use its power and suspend or prohibit data flows which could have resolved this case.[49]

b. EU-US Privacy Shield in Schrems II

The CJEU also inquired about the legality of the EU Commission Implementing Decision (EU 2016/1250) on the adequacy of the protection provided by the EU-US Privacy Shield Framework. This action was brought on 25 October 2016 by *La Quadrature du Net*), French Data Network and *Fédération des Fournisseurs d'Accès à Internet Associatifs* (*Fédération FDN*) against the EU Commission in the case *La Quadrature du Net and Others v. Commission*.[50] The applicants in this case requested to annul the decision for infringing Articles 7, 8 and 47 of the CFR. They claimed inter alia that the decision wrongly found that the EU-US Privacy Shield Framework assures an adequate level of protection of fundamental rights that is tantamount to that guaranteed within the EU.[51]

During the *Schrems* II hearing, the CJEU insisted that this case is related and a separate hearing in this case has been deferred. A judgment is still pending.[52]

Some of the arguments against the EU-US Privacy Shield Framework during the hearing were that the current system is allegedly violating European citizen's privacy rights due to mass surveillance programs, which allows the US National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) to get extensive and unfettered access to EU citizens' data. According to *Maximilian Schrems*, there is a clear tension between surveillance laws in the US and privacy laws. This means that social media platforms such as Facebook do not adequately protect the data of EU citizens when data is transferred across the Atlantic. *Maximilian Schrems* argued that the EU-US Privacy Shield Framework should be invalidated as it is based on wrong interpretation of US law.[53] Finally, the EDPB also raised concerns regarding the effective remedies and concrete protection for EU citizens in the US.[54]

4. The AG's Opinion in Schrems II

In light of the significance of the issues at stake in *Schrems* II, it does not surprise that the recent opinion of the Advocate General (AG) Henrik Saugmandsgaard Øe's in this case had been eagerly awaited. While the AG's Opinion is completely independent and not binding on the CJEU, it is authoritative and judges might consider some of the legal solutions provided therein. In his opinion, which was delivered on 19 December 2019, the AG concluded that the SCCs mechanism for the transfer of personal data to processors established in third countries affords an adequate level of protection.[55] Therefore, transfers of data by such means are valid. However, the AG considers that if the transfers are in breach of the SCCs and appropriate protection mechanisms cannot be ensured by other means, the supervisory authority should examine with all due diligence any complaint filed by organisations 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 the transfer.[56]

As for the EU-US Privacy Shield Framework, the AG upheld that the CJEU does not need to render judgment on the validity of the EU-US Privacy Shield

---

49 Simon Mortier and Benoit Van Asbroeck, 'Notes from the CJEU hearing on SCCs: Schrems C-311/18 CJEU Hearing of 9 July 2019' (July 2019) <https://www.twobirds.com/en/news/articles/2019/global/notes-from-the-cjeu-hearing-on-sccs> accessed 10 November 2019.

50 Action brought on 25 October 2016 — *La Quadrature du Net and Others v Commission* (Case T-738/16) (2017/C 006/49 <https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2017.006.01.0039.01.ENG> accessed 10 November 2019.

51 Action brought on 25 October 2016 — *La Quadrature du Net and Others v Commission* (Case T-738/16) (2017/C 006/49 <https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2017.006.01.0039.01.ENG> accessed 10 November 2019.

52 Simon Mortier and Benoit Van Asbroeck, 'Notes from the CJEU hearing on SCCs: Schrems C-311/18 CJEU Hearing of 9 July 2019' (July 2019) <https://www.twobirds.com/en/news/articles/2019/global/notes-from-the-cjeu-hearing-on-sccs> accessed 10 November 2019.

53 Noyb, 'CJEU Hears Case on EU-US Data Transfers (Standard Contractual Clauses and Privacy Shield)' (8 July 2019) <https://noyb.eu/en/cjeu-hears-case-eu-us-data-transfers-standard-contractual-clauses-and-privacy-shield> accessed 10 November 2019.

54 Simon Mortier and Benoit Van Asbroeck, 'Notes from the CJEU hearing on SCCs: Schrems C-311/18 CJEU Hearing of 9 July 2019' (July 2019) <https://www.twobirds.com/en/news/articles/2019/global/notes-from-the-cjeu-hearing-on-sccs> accessed 10 November 2019; EU-US Privacy Shield – Second Annual Joint Review, adopted on 22 January 2019 <https://edpb.europa.eu/sites/edpb/files/files/file1/20190122edpb_2ndprivacyshieldreviewreport_final_en.pdf> accessed 10 November 2019.

55 Opinion of the Advocate General in the case C-311/18 Facebook Ireland and Schrems, No 165/2019 (19 December 2019) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-12/cp190165en.pdf> accessed 29 December 2019.

56 ibid.

Framework since that dispute lays only on the validity of Decision 2010/87 (SCCs).[57] Nevertheless, the AG raised some concerns whether this Framework met the adequacy threshold, in particular where data transferred to the US could be accessed by US intelligence agencies and judicial authorities. Based on the previous jurisprudence, the AG considered that such surveillance by US authorities was generally justified on the grounds of public interest. However, he also noted that the necessity and proportionality principles as well as the respect to private life should be considered on a case-by-case basis.[58]

The AG's Opinion may be influential, however, it is not legally binding. Therefore, the CJEU could still potentially invalidate the EU-US Privacy Shield Framework, resulting in transfers of personal data between the EU and US no longer lawful. This poses substantial legal risk to companies currently relying on the adequacy of this cross-border mechanism and may affect, in particular, the deployment of cloud-based medical AI technologies.

The decision is expected in the upcoming months where the CJEU will adjudge whether the SCCs and EU-US Privacy Shield Frameworks adhere to the GDPR requirements or not. In the *Schrems* I case, when the CJEU struck down the Safe Harbour Framework, there was an alternative scheme for international data transfers (such as the SCCs). Yet, the situation is less clear now in the pending *Schrems* II case since there is no quick and easy alternative solution to be implemented. Should both mechanisms be declared invalid, data could no longer lawfully be transferred to overseas countries.[59] This creates uncertainty and great challenges for AI-based companies, in particular, in the healthcare sector where personal data is regarded as highly sensitive. Recent cases and scandals exacerbated these concerns as explained in the section below.

IV. Recent US litigation involving Privacy Concerns in the Health Sector

Following the European *Cambridge Analytica* and *Facebook* scandal, the *Schrems* II challenge comes at a time of an additional recent US scandal that showcases the implications of privacy and data protection in the health and life sciences. In *Dinerstein v. Google*[60] the complaint accuses the *University of Chicago* (UC) and *Google* to have violated the Health Insurance Portability and Accountability Act (HIPAA)[61] by sharing and receiving hundreds of thousands of patients' records that contained sufficient information for the tech giant to re-identify patients. *Google* and UC claim that all shared data were 'de-identified' and in compliance with HIPAA. However, the complaint contests this and highlights that 'in reality, these records were not sufficiently anonymized and put the patients' privacy at grave risk.'[62] Specifically, the complaint highlights that *Google* has access (eg, through Android phones and mobile apps such as Waze and Maps) to a vast amount of information that empowers the tech company via data triangulation[63] to potentially re-identify medical records. The complaint also alleges that UC did not obtain patients' express consent before sharing their medical records with *Google* that pursues commercial purposes.[64] Ultimately, however, this case boils down to the question of what health information should be considered individually identifiable in the 21st century with increasing data sources and greater computational power allowing for re-identification. It is also a signifier that the HIPAA is showing its age and might be outdated.

It remains to be seen in how far this case will influence the ongoing US debate over a modernised

57 ibid 3; Martin Sloan, 'Schrems 2 – What can we take from the AG's Opinion on Standard Contractual Clauses' (20 December 2019) <https://brodies.com/blog/ip-technology/schrems-2-what-can-we-take-from-the-ags-opinion-on-standard-contractual-clauses/> accessed 29 December 2019.

58 Martin Sloan, 'Schrems 2 – What can we take from the AG's Opinion on Standard Contractual Clauses' (20 December 2019) <https://brodies.com/blog/ip-technology/schrems-2-what-can-we-take-from-the-ags-opinion-on-standard-contractual-clauses/> accessed 29 December 2019.

59 Stephanie Bodoni, 'EU Judges Face Another Major Facebook Privacy Case From Activist Schrems' (9 July 2019) <https://www.insurancejournal.com/news/international/2019/07/09/531544.htm> accessed 10 November 2019.

60 *Dinerstein v. Google,* LLC et al, Case Number 1:2019cv04311 <https://dockets.justia.com/docket/illinois/ilndce/1:2019cv04311/366172> accessed 10 November 2019).

61 'It is worth noting that *Google* is not a HIPAA-covered entity, and thus health data collected by the tech giant usually does not fall under HIPAA. In contrast, the California Consumer Privacy Act of 2018 (CCPA) and the European General Data Protection Regulation (GDPR) are broader in their scope' - See T Minssen, S Gerke and C Shachar, 'Is Data Sharing Caring Enough About Patient Privacy? Part I & II: Potential Impact on US Data Sharing Regulations' <https://blog.petrieflom.law.harvard.edu/2019/07/26/is-data-sharing-caring-enough-about-patient-privacy-part-i-the-background/> accessed 14 November 2019.

62 Dinerstein v. Google, LLC et al, Case Number 1:2019cv04311 <https://dockets.justia.com/docket/illinois/ilndce/1:2019cv04311/366172> accessed 10 November 2019.

63 ibid.

64 ibid.

Federal Data Protection Law, and in how far such a potential law would resemble the EU GDPR and the CCPA. Depending where these political processes lead, a new Federal US law might very well provide an adequate level of protection. Meanwhile, however, *Dinerstein v. Google* has the potential to evolve into a landmark case with regard to questions of when and under what circumstances patient data may be shared, whether patient data can be truly de-identified, and what could be potential safeguards.[65] By signifying the age and weaknesses of the current Federal Law on data protection, the case also casts doubts on the robustness of the US-EU Privacy Shield Framework. It can therefore be assumed that this case will be referred to in the *Schrems* II proceedings. But, what can be done to improve compliance with the current EU-US Privacy Shield Agreement? Some indications can be found in a series of three EU Commission reports.

V. Recent EU Commission Evaluation of the EU-US Privacy Shield

Since the EU-US Privacy Shield Framework entered into force the EU Commission monitors and evaluates its adequacy findings on an annual basis and, in addition, conducts an annual review of the functioning of the Privacy Shield. The EU Commission published its *first* annual report of the functioning of the EU-US Privacy Shield on 18 October 2017.[66] In this report the EU Commission noted that the first annual review had demonstrated that the US authorities have put in place the necessary structures and procedures to ensure the correct functioning of the Privacy Shield. The EU Commission concluded in this report that 'the United States continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the Union to organisations in the United States.'

In its *second* Report to the European P and the Council on the second annual review of the functioning of the EU-US Privacy Shield of 19 December 2018[67] the EU Commission noted in particular that the FTC had stepped up in its efforts to proactively monitor compliance with the Privacy Shield Principles, including issuing administrative subpoenas to request information from a number of Privacy Shield participants, as well as the FTC investigation into the *Facebook / Cambridge Analytica* case. The EU Commission pointed out in this report that this case and other revelations have shown, that it would be important that the EU and the US further converge in their responses.

The *third* annual review of the EU-US Privacy Shield Framework from the EU Commission was published on 23 October 2019. It confirms the EU Commission's findings in the adequacy decision, both concerning the commercial aspects of the framework and concerning the aspects relating to access to personal data transferred under the Privacy Shield by public authorities. In this respect, the EU Commission noted a number of improvements in the functioning of the framework as well as appointments to key oversight bodies. However, the EU Commission also concluded that a number of concrete steps need to be taken to better ensure the effective functioning of the Privacy Shield in practice.[68]

VI. Discussion

Irrespective of the precise position taken by the CJEU, it can be assumed that the CJEU's pending decision on the legitimacy of these adequacy and safeguard mechanisms will have a considerable impact on the

65 ibid.

66 1st Report to the European Parliament and the Council on the second annual review of the functioning of the EU-US Privacy Shield of 19 December 2018 <https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619> accessed 10 November 2019.

67 2nd Report to the European Parliament and the Council on the second annual review of the functioning of the EU-US Privacy Shield of 19 December 2018, <https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf> accessed 10 November 2019.

68 These include, (1) shorter time periods granted to companies for completing the re-certification process, (2) improved spot-check procedures for onward-transfers, (3) the development and more consistent use of better tools for detecting false claims of participation in the Privacy Shield from companies that have never applied for certification, (4) finding better ways to share meaningful information on ongoing investigations between the FTC and the EC, as well as with EU Data Protection Authorities that also have enforcement responsibilities under the Privacy Shield, and (5) development of common guidance on the definition and treatment of human resources data in the coming months. See the Report from the EU Commission to the EU Parliament and the Council on the third annual review of the functioning of the EU-US Privacy Shield, SWD(2019) 390 final <https://ec.europa.eu/info/sites/info/files/report_on_the_third_annual_review_of_the_eu_us_privacy_shield_2019.pdf> 7, 9. Note, however, that the 3rd report has also received considerable stakeholder criticism, see eg the Access Now letter from Estelle Massé and Jennifer Brody, <https://www.accessnow.org/cms/assets/uploads/2019/09/Access-Now-Submission-Privacy-Shield-Review-Questionnaire-Third-review-Final.pdf> accessed 10 November 2019.

future of transfers of personal data of EU citizens to the US. The outcome and the potential legal implications of this case might not only have a significant impact on the transfer of patient data from the EU to the US but could also affect cloud-based medical AI/ML companies that rely on cross-border dataflows, as well as the organisations implementing these solutions. Although the AG's Opinion in *Schrems* II delivered on 19 December 2019 indicates the possibility that radical changes to the current system might be avoided,[69] recent data breach scandals in the US and Europe, as well as national security rules obliging US companies to disclose data to US authorities have resulted in a complex situation. Moreover, and as pointed out before, the CJEU judges decide independently and does not have to directly follow the AG's opinion with regard to the SCCs and other aspects. Even if the CJEU decides not to rule on the Privacy Shield Framework as such, new cases that directly concern Privacy Shield Framework are on the horizon, such as *La Quadrature du Net and Others v. Commission*. All stakeholders should therefore be aware of the potential risk, remain vigilant and monitor the developments very carefully. It is therefore also advisable to consider various scenarios.

In the event that the CJEU finds the the EU-US Privacy Shield Framework or the current SCC system to be inadequate (ie, either in *Schrems* II or in a subsequent decision), this could have an immediate or even retroactive effect. Such a decision could knock down the foundations for many business- and research-essential data transfers between the EU and the US. This would have serious legal and economic consequences for a wide range of entities that rely on effective data transfers between the EU and the US, including companies engaging in cloud-based medical AI technologies in pharmaceutical R&D, clinical trials, and medical devices. In that case, companies depending on these transfer mechanisms will have to consider feasible alternative solutions and practical options to lawfully conduct data transfers.[70]

Binding Corporate Rules (BCRs)[71] could be considered a viable option in some cases[72] but their use is of limited applicability. BCRs are internal binding rules adopted by multinational companies.[73] Yet, the approval process by the Supervisory Authorities can be lengthy, and companies will probably need to have interim solutions in place before approval is granted.[74] Moreover, different solutions are most likely needed for transfers outside the group, although groups that act as processors for their clients can rely on their BCRs to receive personal data outside the EU from those clients.[75] Whether such an alternative is viable, practicable or indeed possible would therefore have to be assessed on a case-by-case basis by each individual entity that needs to comply with the EU data privacy rules.

Other alternatives include the derogations under Article 49 GDPR, such as explicit consent, contractual necessity, and public interest. Yet, these derogations are only applicable for specific situations, which often do not apply for repeated and large-scale data transfers. Although in line with the EDPB guidelines[76] they are restrictively interpreted, and it would be extremely difficult to obtain valid consent to transfers from affected individuals or to achieve approval from a competent supervisory authority for specific transfers, which has historically not been something they have done.[77] Although certainly an option that must be carefully considered in light of the discussed litigation, the EDPB guidelines consider these to be a last resort for use only where no other mechanism is available.[78]

With regard to the SCC option, it is worth noticing that the EU Commission is currently 'working on

69 See Section III.4.

70 Cf Davina Garrod, Jenny Arlington, Rachel Claire Kurzweil, Sahar Abas, 'The case of Schrems 2.0 – the challenge to Standard Contractual Clauses allowing personal data transfer outside the European Union' <https://www.akingump.com/en/experience/practices/cybersecurity-privacy-and-data-protection/ag-data-dive/the-case-of-schrems-2-0-the-challenge-to-standard-contractual.html> accessed 10 November 2019.

71 Art 47 of the GDPR.

72 Art 49 of the GDPR.

73 Marcelo Corrales, Paulius Jurčys and George Kousiouris, 'Smart Contracts and Smart Disclosure: Coding a GDPR Compliance Framework' in Marcelo Corrales, Mark Fenwick and Helena Haapio (eds), *Legal Tech, Smart Contracts and Blockchain* (Springer, 2019) 212.

74 Paul Maynard, 'Transfers on Trial: Privacy Shield and Standard Contractual Clauses go before the European Courts' <https://www.lexology.com/library/detail.aspx?g=4b9a70f6-9f3c-4297-8d87-020783fb3aa2> accessed 12 November 2019; See also DLA Piper, 'Schrems 2.0 – The Demise of Standard Contractual Clauses and Privacy Shield? <https://blogs.dlapiper.com/privacymatters/schrems-2-0-the-demise-of-standard-contractual-clauses-and-privacy-shield/> accessed 12 November 2019.

75 ibid.

76 Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 Adopted on 25 May 2018, available <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf> accessed 12 November 2019.

77 Mayard, (n 65).

78 ibid.

an update of the currently available SCCs, which will provide a ready-made contractual mechanism for international transfers.'[79] Many stakeholders would welcome such updates, since it could increase clarity about the use of the SCCs. The EU Commission's current SCC framework has resulted in some confusion since it does not contain all the elements required by Article 28(3) GDPR with regard controller-processor SCCs and the current versions still refer to the Data Protection Directive.[80] Yet, as pointed out by some commentators, 'it is not clear whether this work will be completed prior to the CJEU´s judgment, and future clauses may be subject to a challenge similar to that in *Schrems* II, on the basis that updated SCCs will not affect the underlying legal order of a non-EU jurisdiction'.[81] That said, SCCs require the data importer to implement appropriate technical and organisational measures to ensure secure processing. This often includes implementing pseudoanonymization, robust encryption, as well as the establishment of an Information Security Management System (ISMS) appropriate to the risks. In the medical and pharmaceutical context this often includes implementing an ISMS conforming to ISO 27001.

An important aspect of the GDPR is the concept of Privacy by Design and by Default.[82] This means that data controllers and processors must embed privacy and data protection requirements directly at the design stage the AI/ML cloud-based applications. This is often challenging in the context of medical AI/ML because it goes contrary to underlying 'big data' design philosophy for AI systems (ie, collect as much data as possible without necessarily knowing its purpose because it may improve the performance of the AI/ML system after training by uncovering previously unknown correlations). Additionally, medical AI/ML processors should aim to implement advanced 'pseudonymization' techniques to ensure secure processing (Art. 32 GDPR). The GDPR recognizes the privacy-enhancing effects of anonymisation and pseudonymisation. The main difference between anonymisation and pseudonymisation relies on whether the data subject can ever be re-identified or not.[83] Anonymisation is done by stripping away from any identifiers that can link to the data subject by all parties. Recital 26 of the GDPR stipulates that the principles of data protection do not apply to anonymous data since it prevents any future re-identification of the data subject. For this reason, anonymisation is considered to be the most desirable approach whenever possible.[84] In fact, if the data is completely anonymized (a very high standard under GDPR), it can be freely transferred across jurisdictions without the need of adequacy or appropriate safeguards.

When anonymisation is not possible, pseudonymisation techniques should be implemented by replacing personal data by one or more artificial identifiers or pseudonyms in such a way that data subjects cannot be linked directly to their corresponding nominative identities.[85] Therefore, pseudonymisation is also considered to be a security method to make health data less explicit and easy to manage.[86] In the context of GDPR, pseudonymisation 'means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject *without the use of additional information*, provided that such *additional information is kept separately* and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person' (Art. 4(5) GDPR). For example, the data controller (eg, the Clinical Trial Sponsor) may keep the subject IDs, while the processor (eg, medical device company processing the data) may receive the raw physiologic data without subject IDs.

79 ibid; See also Commissioner Jourová's intervention at the event 'The General Data Protection Regulation one year on: Taking stock in the EU and beyond' <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_19_2999> accessed 9 November 2019.

80 Mayard (n 65).

81 ibid, noting that: 'If the CJEU invalidates SCCs or Privacy Shield, the impact on businesses is likely to be so material that the EDPB will be under intense pressure to declare a 'grace period' where no enforcement action is taken by EU Member State data protection supervisory authorities. This would allow exporters time to assess the situation and put in place alternative solutions. [….]. A grace period is not, however, guaranteed. Nor would it prevent individuals from bringing private claims for compensation or group litigation claims and as noted above there are no obvious alternative mechanisms for a business to take to 'fix' the position in such a period.').

82 See Art 25 of the GDPR.

83 Robert Walters, Leon Trakman and Bruno Zeller, *Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches* (Springer 2019) 90.

84 Balaji Raghunathan, *The Complete Book of Data Anonymisation: From Planning to Implementation* (CRC Press 2013).

85 Sanjay Sharma, *Data Privacy and GDPR Handbook* (Wiley & Sons 2019) 88.

86 Heidelinde Hobel et al, 'Anonymity and Pseudonymity in Data-Driven Science' in John Wang (ed) *Encyclopedia of Business Analytics and Optimization* (IGI Global 2014) 128.

The Article 29 Working Party in its Opinion 05/2014 on Anonymisation Techniques[87] recommended that in order to meet the current anonymisation standards, data must be processed in such a way that the individual cannot be identified anymore by using 'all means likely reasonably to be used' either by the controller or a third party. This means that the requirements and the objectives of the anonymisation process must be clearly defined from the beginning in order to achieve the threshold.[88]According to the Working Party, however, there is no one-size-fits-all solution. Anonymisation should be considered on a case-by-case basis, using various classical methods and models such as: data randomisation and generalization (including, eg, noise addition, permutation, differential privacy, aggregation, k-anonymity, I-diversity and t-closeness). Therefore, data controllers are advised to tailor-make the anonymisation technique to the specific circumstances.[89] However, the problem with any of these techniques is that they are often hard to achieve as previously discussed above in the *Dinerstein v. Google* case (section 4). Big Tech companies can get access to vast amount of information that allows them to potentially re-identify medical record through data fusion. Data can be so distinct that it can be easily identified even if the identifying features are scrubbed away from the data subject.[90] This refers to the data triangulation problem as explained before.

Furthermore, various data leak scandals exacerbated public concerns. The *Google* DeepMind deal with the UK's National Health Service (NHS)[91] is a good example. *Google's* artificial intelligence firm was authorised to access health data from over 1.6 million patients to develop app monitoring kidney disease called 'Streams.' However, corroborative research studies indicated that the *Google* DeepMind deal had access to other kinds of sensitive data and failed to comply with data protection law.[92]

Recently, the *Google's* 'Nightingale Project' was also accused of allegedly secretly gathering personal health records across 21 states in the US on behalf of *Ascension* (a Catholic chain of 2,600 hospitals, doctors' offices and other facilities). The data collected without patients and even doctors' awareness included inter alia lab results, doctor diagnoses and hospitalisation records. *Google* and *Ascension* claimed that the Project Nightingale upholds security and privacy of patients, however due to the vast amount of information that the Big Tech company has, it can easily link up to other kinds of personal and sensitive data.[93] In addition, the project has been criticised since it is feared that *Google* takes away patient´s control over their own data and that the data has been transferred under private contracts within public-private partnerships which makes it difficult to get transparency.[94] Finally, it has been noted that health organisations are under increasing pressure to improve efficiency and quality of care and many are turning to AI in an effort to sharpen their services, even if sensitive patient data is handled.[95]

In sum, when it comes to cross-border data transfers between the EU and the US, the 'bone of contention' is two-fold. One the one hand, there is a conceptual legal problem regarding the definition and understanding of what constitutes 'anonymization' and 'pseudonymization', which is not fully harmonized and varies greatly between the EU and the US. The failure to come to grip with these concepts creates misunderstandings and legal issues. According to the GDPR and the Working Party, pseudonymized data is still regarded as personal data. Therefore, the requirements fall under the scope of the GDPR and must also be protected accordingly in the US. On the other hand, there is a technical and pragmatic problem. While anonymisation might be the most desirable approach, the threshold to achieve it in the EU is too high.[96] This creates challenges at the moment

87 See, Opinion 05/2014 on Anonymisation Techniques adopted on 10 April 2014.

88 M Corrales Compagnucci, J Meszaros, T Minssen, A Arasilango, T Ous and M Rajarajan, 'Homomorphic Encryption: The 'Holy Grail' for Big Data Analytics & Legal Compliance in the Pharmaceutical and Healthcare Sector?' (2019) 3 European Pharmaceutical Law Review 4, 144-155.

89 ibid.

90 Kelsey Campbell-Dollaghan, 'Sorry Your Data Can Still Be Identified Even If It's Anonymized' (12 October 2018), <https://www.fastcompany.com/90278465/sorry-your-data-can-still-be-identified-even-its-anonymized>

91 See National Health Service (NHS) <https://www.nhs.uk>

92 Janos Meszaros, Chih-hsing Ho and Marcelo Corrales, 'Nudging Consent & the New Opt-out System to the Processing of Health Data in England' in Marcelo Corrales et al, (eds) *Legal Tech & the New Sharing Economy*, (Springer 2020).

93 Mary Griggs, 'Google Reveals Project Nightingale After Being Acussed of Secretly Gathering Personal Health Records' (11 November 2019) <https://www.theverge.com/2019/11/11/20959771/google-health-records-project-nightingale-privacy-ascension>

94 BSCC, 'Project Nightingale: Google accesses trove of US patient data' <https://www.bbc.com/news/technology-50388464> accessed 10 November 2019.

95 ibid

96 (n 91).

of implementing overseas projects between the EU and the US, most notably in the context of cloud-based technologies, big data, and AI in the medical sector.

It is clear that these technical and legal issues must be addressed to reconcile the needs of technological possibilities and R&D with the GDPR compliance in the forthcoming *Schrems* II decision and in potential future litigation. The same holds true with regard to the implementation of the EU initiatives published in the Ethics Guidelines for AI (2019)[97] and the most recent Commission White Paper on Artificial Intelligence[98], which was published on 19 February 2020 together with a companion Communication on EU data strategy[99], and a report on the safety of AI systems.[100] These initiatives outline the wide-ranging plan to develop artificial intelligence (AI) in the EU based on common values, but also aim at making more data sets available for business and government to promote AI development. The health and life sciences are mentioned as one of the most significant application areas. The Communication on the European Data strategy, in particular, mentions the creation of European Data Spaces that should be operated and governed in accordance with European values.[101] In line with this principle, a first priority for operationalising the vision is to put in place an enabling legislative framework for the governance of such common European data spaces.[102] According to the EU Commission:

> '[...] such governance structures should support decisions on what data can be used in which situations, facilitate cross-border data use, and prioritise interoperability requirements and standards within and across sectors, while taking into account the need for sectoral authorities to specify sectoral requirements. The framework will reinforce the necessary structures in the Member States and at EU level to facilitate the use of data for innovative business ideas, both at sector- or domain-specific level and from a cross-sector perspective.'[103]

One day, such EU data spaces might reduce the need for cross-border data transfers, but as the European Data Space takes shape and the EU values that are at the core of these spaces become more homogeneous, this could also lead to further frictions with foreign data spaces, such as in the US. It can therefore be assumed that legal battles over the EU-US Privacy Shield Framework or other data transfer agreement will most likely continue, and that preparations will have to be made to enable cross-border data transfers in an environment of legal uncertainty.

VII. Conclusions

Recent litigation, developments, and technical challenges have resulted in a high degree of legal uncertainty with regard to the robustness and validity of the international legal frameworks for US/EU data transfers. This is generally troubling news for innovative companies on both sides of the 'pond,' and particularly for private and public stakeholders in drug development and healthcare, which depend on effective international transfer and cloud computing.

Both from the innovation and legal perspectives it is vital to improve and stabilize the regulatory and technical set-ups for international data transfer to allow for an optimal use and sharing of health-related data. Since the future improvement of research, drug development and treatment of patients, especially in the context of personalised medicine, needs safe data highways that allow for cross-border transfers and access to high value data, the effective development of innovative tools to protect patients and to defend diseases should not be unduly hampered. At the same time, it is important to acknowledge public concerns and fears of intransparent and abusive use of health data and the need for a special protection of health related data compared to other personal data because

97 European Commission, 'Ethics Guidelines for Trustworthy AI' <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai> accessed 2 February 2020.

98 European Commission, 'White Paper On Artificial Intelligence - A European approach to excellence and trust' (19 February 2020) COM(2020) 65 final <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> accessed 10 March 2020.

99 European Commission, 'Communication: A European strategy for data, (19 February 2020) COM(2020) 66 final, <https://ec.europa.eu/info/files/communication-european-strategy-data_en> accessed 11 March 2020.

100 European Commission, 'Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics (19 February 2020) COM(2020) 64 final <https://ec.europa.eu/info/publications/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics_en> accessed 9 Mach 2020.

101 (n 25) 13.

102 ibid.

103 ibid.

of their sensitivity and their special protection under the GDPR and evolving US data protection laws.[104] A wide implementation and adoption of the technical possibilities requires a certain degree of public trust which might result from transparency and legal certainty and which might result in a willingness to share valuable health data. It is therefore imperative to have sufficiently effective and transparent legal frameworks for the protection of such data. This requires a complex balancing act since it is possible for that overly strict data protection rules might undermine the usefulness and therewith the very goals of recent data transparency legislation,[105] as well as data sharing and transfer initiatives.[106] In that regard, it is important to recognise new challenges, including the further development of technologies that allow for decryption and data re-identification, such as data fusion and triangulation, as well as the enormous potential of quantum computing technology.[107] It is therefore imperative to provide for appropriate data protection safeguards and supplementing new technologies,[108] while improving transparency, remedies and compensations that should be available if breaches occur. Hence, there is a strong need for adequate, enforceable and legally sound mechanisms that a) provide the certainty for stakeholders to operate within data applications, and b) provide sufficient remedies for concerned parties to protect their rights.

Finally, to address some of the current challenges and to alleviate the effects of a potential failure of the EU-US Privacy shield agreement, it is important to also consider a variety of possibilities provided by technical solutions, as well as the development of 'codes of conduct', and 'certification mechanisms' contemplated by GDPR. It is evident that further legal, technical, and socio-economic research is necessary to improve reasonably safe data transfer systems to enable the next generation of biomedical research and development, especially in data intensive applications such as cloud-based medical AI/ML.

Post scriptum: This paper could consider developments until 14 March 2020. Since the CJEU decision in "Schrems II" is expected in the coming weeks, we will follow up on any developments in a future issue of EPLR.

---

104 WN Price II, K Spector-Bagdady, T Minssen and M Kaminski, 'Shadow health records meet new data privacy laws' (2019) 363 Science 6426, 448.

105 See also eg Regulation (EU) 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 (referred hereafter as 'Regulation (EU) 536/2014'). For a more detailed analysis cf.

106 As for the clinical trials sector, see eg T Minssen, N Rajam and M Bogers, 'Clinical Trial Data Transparency and GDPR Compliance: Implications for Data Sharing and Open Innovation' in Katerina Sideri and Graham Dutfield (eds), *Openness, Intellectual Property and Science Policy in the Age of Data Driven Medicine* <https://ssrn.com/abstract=3413035> accessed 10 November 2019.

107 A Dubovitskaya et al, 'Intelligent Health Care Data Management Using Blockchain: Current Limitation and Future Research Agenda' in Gadepally V et al (eds.) 'Heterogeneous Data Management, Polystores, and Analytics for Healthcare' Lecture Notes in Computer Science, vol 11721 (Springer, 2019).

108 (n 91).