Next

Stella Galehr

Generation

Transatlantic Data Transfers under the GDPR: Developments and Outlook

Nr. 1

EIZ Publishing

Publisher: EIZ Publishing (https://eizpublishing.ch)
Layout & Production: buch & netz (https://buchundnetz.com)
DOI: https://doi.org/10.36862/eiz-ng001
Version: 1.00-20231013

This work is available in print and various digital formats in **OpenAccess**. Additional information is available at: https://eizpublishing.ch/publikationen/next-generation/.

Next Generation

The “Next Generation” series offers a platform for young academics in all areas of law. The aim is to promote the visibility of special talents at an early stage. The volumes in this series are published in Open Access and can therefore be shared and distributed via social media and other channels. Each contribution undergoes a peer review process before it is published.

Transatlantic Data Transfers under the GDPR*

Developments and Outlook

Stella Galehr**

Table of Content

* The author thanks Prof. Dr. Heinemann for his input and support in publishing on this topic. The author also appreciates EIZ Publishing for offering young scholars a platform, and the UZH Open Access Publication Fund for providing financial support.

** Stella Galehr is a PhD candidate and university assistant at the chair of Prof. Dr. A. Heinemann for European Economic Law at University of Zurich. Her research focuses on digital and competition law. Galehr holds an MLaw Degree of the University of Zurich as well as an LL.M. Degree of UC Berkeley.

I. Introduction

> *"The case raises issues of very major, indeed fundamental, concern to millions of people within the European Union and beyond. First, it is relevant to the data protection rights of millions of residents of the European Union. Secondly, it has implications for billions of euros worth of trade between the EU and the US and, potentially, the EU and other non-EU countries (...) There is considerable interest in the out-come of these proceedings by many parties having a very real interest in the issues at stake."*[1]

This statement originates from the Irish national court's judgement, that referred the Schrems II case[2] to the Court of Justice of the European Union (CJEU) and emphasizes the overall importance of regulating international data transfers. Data exchange is inherent to the developments of globalization. Access to information – independent of time and space – comes with advances: The analysis of big data is crucial to public policy, business operations and academia, the sharing of information enables e-commerce, advanced marketing strategies, smooth business operations and staying connected with friends and family kilometers away.

The topic of international data transfer is fascinating in this context because many of its conflicts occur at the intersection of real border politics and seemingly borderless data space. As borders blur due to increasing interconnectedness, nation states become alarmed by the risks of data misuse. They, *in casu* the European Union (EU), then may seek to regulate data flows, leading to debates about where data should be stored, accessed and transmitted. Some accuse nation states of 'data protectionism', i.e. under the pretext of data protection concerns, domestic economic interests are being protected as regulations impose trade barriers, impeding the free flow of data across borders.[3]

---

1 Irish High Court, 3 October 2017, *The Data Protection Commissioner v Facebook Ireland and Maximilian Schrems*, 3.

2 CJEU, 16 July 2020, C-311/18 – *Schrems II*, ECLI:EU:C:2020:559.

3 For a deep-dive on the topic see Naef, Data Protection without Data Protectionism, EYIEL, Vol. 28, available: <https://link.springer.com/content/pdf/10.1007/978-3-031-19893-9.pdf?pdf=button> (last accessed: 13 July 2023).

The value of data highly depends on the (technical but also) legal ability to extract information from it. However, such information can be personal, and the question arises what role the individual's privacy is attributed. There is no globally unified approach to privacy or data protection. Cultural and political differences in the understanding of the handling of data between the EU and United States (US) have led to disputes over the last decades.

The discussion often centers around data protection concerns. But there are several regulatory dimensions to data processing and data transfers: data protection and privacy as a human right, national security concerns, constitutional principles, and, as indicated, serious implications on trade.[4]

This paper analyzes the transfer regime under the General Data Protection Regulation (GDPR) (Chapter II). It then focuses on transatlantic relations between the EU and the US (Chapter III) and highlights developments in the recent decade. The author strives to balance the theoretical and textual backgrounds with the court cases and political elements. The complaint filed by Maximilian Schrems against Meta (formerly: Facebook) back in 2014, decisively shaped the discussion and serves as a starting point for the analysis. The complaint led to an astounding ping pong game between the data protection authorities, NGOs, national and European courts, legislative initiatives as well as intervening governments, and finally parliamentarians, will be mapped out and scrutinized in the following text.

On 10 July 2023 a renewed adequacy decision for the US, 'EU-U.S. Data Privacy Framework' was put into place by the European Commission. Chapter IV dives into the process leading up to the framework, lays out the key elements and provides a first assessment. The outlook (Chapter V) lays down what indicates a Schrems III scenario in front of the European Courts.

II. International Data Transfer Regime under the GDPR

1. The GDPR: Principles and Definitions

The GDPR must be applied since 25 May 2018 and supersedes the Data Protection Directive, which already had a transfer regime in place.[5] The GDPR aims to protect individuals with regard to the processing of their personal data as well

---

4 Further reading: Chander/Schwartz, Privacy and/or Trade, Chander, University Chicago Law Review, 49 (2023), <https://ssrn.com/abstract=4038531 or http://dx.doi.org/10.2139/ssrn.4038531>.

5 Art. 25 et seq. Directive 95/46/EC (Data Protection Directive).

as it deals with the free movement of such data. Personal data in the meaning of the GDPR includes "any information relating to an identified or identifiable natural person ('data subject')", e.g., name, location data, or any other information that, standing alone or evaluated cumulatively can identify the data subject.[6]

In 1980 the first international instrument on data protection was introduced: the Guidelines by the Organization for Economic Cooperation and Development (OECD) governing the Protection of Privacy and Transborder Flows of Personal Data.[7] To avoid a disruption in transborder flows of personal data the OECD recommended its member countries to take into account certain guiding principles with regard to data protection legislation, in order to enable a sustainable economic and social development.

The GDPR itself builds upon seven principles, which are strongly inspired by the aforesaid OECD guidelines from 1980.[8] The core issues in this paper must be considered in the light of these central principles:

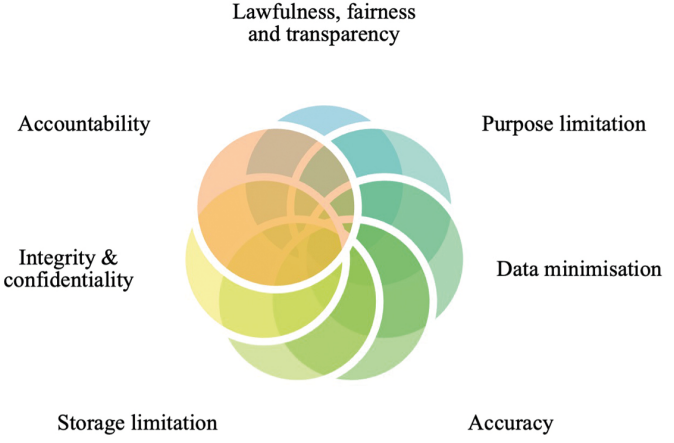

Figure A: The seven principles underpinning the GDPR.

6 Art. 4 GDPR.

7 OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980.

8 Principles are laid down in Art. 5 GDPR.

The GDPR holds several provisions for data transfers to third countries and aims to facilitate data transfers to third countries while guaranteeing a high level of protection.[9]

This confirms the applicability of the GDPR to international transfers. The GDPR's applicability is based on Art. 2, 3 GDPR. Art. 2 GDPR encompasses the material scope, that is, the wholly or partly automated processing of personal data as well as the non-automated processing of personal data stored or to be stored in a file system. Art. 3 GDPR refers to the territorial scope: in principle, the GDPR applies to any establishment of a controller or processor within the EU, wherever the processing takes place. Further, according to sec. 2, it applies, when personal data of a data subject located in the EU is processed in the course of offering goods or services or the monitoring of the behaviours of the data subject.[10]

Since the level of data protection is largely harmonized through the GDPR, data transfers within the EU are not subject to any form of restriction. Naturally however, third countries often strongly differ in terms of their privacy culture and legislation. The European legislator as well as the European courts in their case law, make it clear, that their data protection efforts do not stop at the European borders, but aim at global reach.[11]

2. Toolkit for Transfers

a. Overview

Art. 44 GDPR restricts all transfers of personal data to third countries, by subjecting them to certain conditions. Chapter V of the GDPR provides guidance, under which circumstances processors and controllers can transfer personal data to third countries. The chapter is to be applied in a way, that the mechanisms in place ensure "that the level of protection of natural persons" guar-

---

9 See Recital 6 GDPR.

10 Art. 3 GDPR; on the interplay between Art. 3 and Chapter V GDPR see: EDPB, Guidelines 05/2021, available at <https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf>.

11 In 2014 the CJEU ordered Google to delete information, that was deemed unlawful, not only within EU member states, but worldwide; see CJEU, 13 May 2014, C-131/12 - *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos* (AEPD) *and Mario Costeja González*, ECLI:EU:C:2014:317.

anteed by the GDPR "is not undermined".[12] At the same time, by elevating international transfers to an adequately protected level, the legislator intends to promote the free flow of data.[13]

Chapter V of the GDPR allows to account for different risks and take a transfer specific approach, thus allowing to protect the various dimensions of the privacy of the data subject.

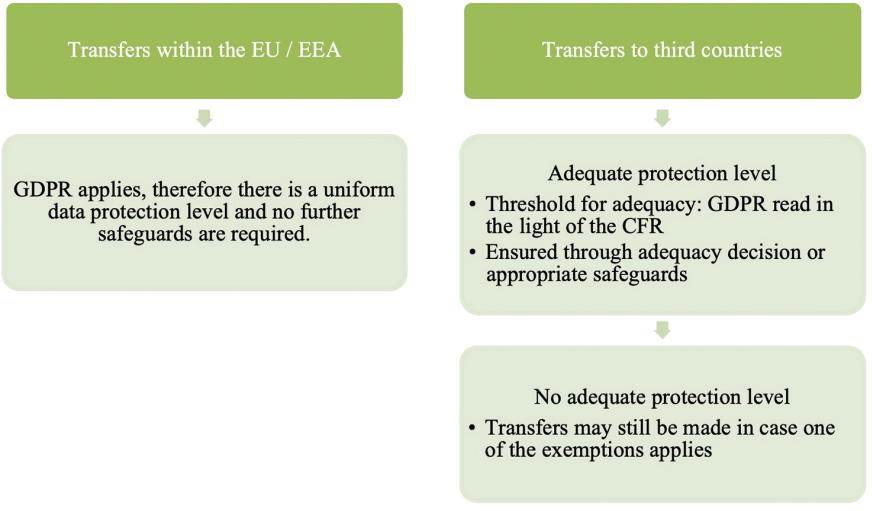

Figure B: The GDPR: Transfers of personal data inside/outside the EU and EEA

b. Adequacy Decisions

The first transfer mechanism is a so-called "adequacy decision": the European Commission (Commission) is competent to determine the adequacy of the level of data protection in the third country pursuant to Art. 45 GDPR. The Commission considers the rule of law, the respect for human rights and fundamental freedoms, relevant legislation and its application in the third country and the availability of judicial remedies. If the Commission finds adequacy and

12 Art. 44 GDPR.

13 See Kuner, Art. 44, 757 in: Kuner/Bygrave/Docksey (eds), GDPR Commentary, 1st edition, 2020.

issues a decision,[14] no further measures need to be taken for data transfers that are covered.[15] The Commission must reassess its decision at least every four years.[16]

Currently there are fifteen valid adequacy decisions,[17] focus of Chapter IV of this paper is the adequacy decision of 10 July 2023 granted to the US.

The reason for choosing the US as the focus country is twofold: Firstly, its relevance draws from the sheer size: Data transfers between the EU and the US form the basis for cross-border trade worth approximately CHF 860 billion (EUR 900 billion), with the US being the EU's most weighty trading partner.[18]

Second, there have been two decisions in the last decade in which the CJEU invalidated the adequacy of US transfers and the recent adoption of a new adequacy decision by the Commission. So, there are some crucial developments and a lot of discussion.

c. Appropriate Safeguards

If no adequacy decision is taken or if a decision is withdrawn, Art. 46 GDPR stipulates that a controller or processor can legally transfer data, if they can provide for appropriate safeguards and, in addition to that, individuals are guaranteed enforceable rights and effective remedies.[19] Such safeguards can be either of legal (such as Binding Corporate Rules, Standard Contractual Clauses (SCCs)) or technical nature, usually it is a combined application of both.

---

14 On this process see Chapter IV.1. Approval Procedure in this paper.

15 See Recital 103 GDPR: "The Commission may decide . . . that a third country . . . offers an adequate level of data protection, thus *providing legal certainty and uniformity* throughout the Union as regards the third country . . . In such cases, transfers of personal data to that third country . . . *may take place without the need to obtain any further authorisation* . . ." (emphasis added).

16 Art. 45 para. 3 GDPR.

17 The Commission has recognized an adequate data protection level in Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, United Kingdom and Uruguay. More information available at <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>.

18 See *European Commission*, Factsheet, EU-US Data Privacy Framework, <https://ec.europa.eu/commission/presscorner/detail/en/fs_23_3754>.

19 Art. 46 GDPR.

When using SCCs, the parties involved contractually agree to provide for appropriate safeguards to ensure an adequate level of data protection. The instrument was not introduced by the GDPR but was taken over from the Data Protection Directive.[20] Model clauses facilitate the process of providing legal appropriate safeguards pursuant to Art. 46 GDPR by providing a predefined set of rules that contractually establishes adequate protection.[21] The Commission has issued four Directives regarding SCCs, the most recent one in 2021, following the Schrems II decision.[22] While it can be valuable for companies to use a predetermined set of clauses, it is not enough to download and sign such a framework, a meaningful implementation and effective control mechanisms are crucial.

Art. 46 sec. 2 GDPR provides a non-exhaustive list of remedies that need no further approval by a supervisory authority, such as Binding Corporate Rules or SCCs. sec. 3 gives the opportunity to rely on case-specific agreements, that need to be approved by the supervisory authority after successfully running a consistency mechanism referred to in Art. 63 GDPR.[23] Binding Corporate Rules can solely be used for data transfers within one company or a group of affiliated companies and are separately regulated in Art. 47 GDPR.

This means that a company needs to know its own data protection policies and procedures and how they comply with EU law. That is the starting point. Further, a company must be knowledgeable regarding its partners' procedures, the laws of the countries in which the partner operates and determine whether they provide adequate protection under EU law. Once the risks are identified, they need to find ways to mitigate them contractually and/or through technical means. The practical burden this puts on entities, must be justified by the risks for the individuals involved.[24] The risk, and thus the extent of risk reduction, depends entirely on the type of transmission. In practice, a combination of technical and legal safeguards are key.

The complexity of determining an adequate protection level based on a contractual level, points to the importance of having adequacy decisions in place, especially with major economic partners.

---

20 Art. 26 sec. 4 Data Protection Directive.

21 Schwartz, The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures, Harvard Law Review 2013, 1966 (1982).

22 Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("SCC Decision 2021").

23 Art. 46 GDPR.

24 Recitals 71, 74, 76, 77, 81 GDPR.

d. Derogations

Art. 49 GDPR exhaustively lists seven cases, where data transfers are exempted from the conditions laid down in Art. 45, 46 GDPR. These are explicit consent, necessity for contract conclusion or performance, necessity for public interest, necessity for legal claims, necessity for vital interests of the data subject. Where none of the derogations apply, personal data can still be transferred, if the transfer is not repetitive and only concerns a limited number of data subjects, whose interests are protected. The controller further provides information on the transfer to the supervisory authority as well as to the concerned data subject.[25] There is an ongoing discussion under which conditions the exemptions can be relied upon. A majority takes the view that as exemptions they therefore require strict interpretation.[26]

III. Case History: From Schrems I to the DPC's May 2023 Decision

1. Timeline and Overview

As indicated in the introduction, the focus points of this paper shall be the personal data transfers within the transatlantic relation between the EU and the US. Based on the Data Protection Directive from 1995, in 2000 the first adequacy decision between the EU and US, the "Safe Harbor Decision" was adopted. Both parties agreed that the far advanced and irreversible international intertwinement, specifically in e-commerce, needed regulation. But because of the vast differences in the approach to privacy of the two countries, sensitivity was required.

The idea was to create a new type of governance, where general rules are established by states, based on which private actors can realize a policy of their own. The result was a self-certification mechanism in form of the Safe Harbor Decision, where US companies could sign up.[27]

---

25 Art. 49 GDPR.

26 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, 4; Günther, Ein Abgesang auf den internationalen Datenverkehr? Privacy in Germany 2020, 192 (197); Loof, Datenschutz in Matrixstrukturen nach Schrems II, Corporate Compliance Zeitschrift 2021, 42 (45).

27 Farrell, Constructing the International Foundations of E-Commerce – the EU-U.S. Safe Harbor Agreement, International Organization 2003, 277 (280 et seq).

The Safe Harbor Agreement contained the following seven principles:

1. obligation to notify about data processing,
2. opt-out choices for data subjects,
3. protection of onward transfers,
4. security of data transfers,
5. provisions protecting data integrity,
6. reasonable access to personal data as well as
7. an enforcement mechanism for the rights guaranteed.[28]

While sounding promising, the Agreement itself was fundamentally toothless, which is why it had only a "chilly reception" in the European Parliament, who rejected the principles as "too weak". Nonetheless the Commission approved Safe Harbor in 2000 and was signed by nearly 5 000 US companies, among them Microsoft, Facebook, and Google.[29]

In 2008, a report was published that revealed major compliance issues with the Safe Harbor regime. However, unlike anticipated, in beginnings of the Safe Harbor regime, no Data Protection Authority has filed a complaint to the competent US authority, the Federal Trade Commission (FTC). The FTC handled a few compliance cases itself – e.g., against Google, Facebook and MySpace, respectively alleging a breach of the Safe Harbor Agreement.[30] Despite efforts, the system was effectively impractical and could not suffice to protect a level of data protection, essentially equivalent to what was guaranteed under EU law. The Safe Harbor regime was a first pragmatic solution for a clash concerning the approach to privacy in the two jurisdictions, but unsatisfactory in result due to a lack of enforcement.

In June 2013 revelations by Edward Snowden regarding the massive scope of power and scale of surveillance through US intelligence services, brought a new momentum to the privacy movement in Europe. The US countered and alleged, European surveillance works essentially the same way, and that Europeans played the privacy card as a form of economic protectionism.[31] While the dispute on an inter-state level was ongoing, concerns arose also among European individuals; one of them was Maximilian Schrems.

---

28 Ibid., 286.

29 Padova, The Safe Harbour is invalid: what tools remain for data transfers and what comes next? International Data Privacy Law 2016, 139 (140).

30 Hoofnagle, Federal Trade Commission Privacy Law and Policy, 320 et seq.

31 Ibid., 323.

2. Leading up to Schrems I & Key Elements of CJEU decision

Maximilian Schrems, back then still an Austrian law student and today a well-known privacy activist, doubted the presumption of adequacy given by the Commission. As a European Facebook user, he had – upon registration – entered into a contract with Facebook Ireland. Some or all personal data gathered by Facebook Ireland is transferred to and processed by Facebook Inc., the US establishment.[32] In 2013 he brought a complaint against the Irish Data Protection Commissioner (DPC), requesting them to prohibit transfers to the US, arguing that under these circumstances adequate protection was not provided. The Irish DPC disregarded his complaint on the basis of finding it "unfounded", pointing to the Commission's Safe Harbor decision as a legal basis for the transfers. Schrems challenged the DPC's decision in front of the Irish High Court, which stated that transfers would be deemed unconstitutional when it comes to Irish law and that, the true question raised was whether the Safe Harbor decision was still valid and further, whether the DPC was bound by an adequacy finding by the Commission or could re-evaluate data transfers in the light of Art. 7, 8 and 47 Charter of Fundamental Right (CFR) and, in any case, prohibit them.[33] The Irish High Court, in the framework of a preliminary procedure, posed these questions to the CJEU.

Concerning the DPC's powers, the CJEU ruled that although a decision by the Commission has a binding effect and is "in principle presumed to be lawful", this does not preclude the DPC from its competence of reviewing data transfer.[34] If a DPC finds, that the arguments for questioning the validity of an adequacy decision brought forward are well-founded, it must enable legal proceedings in national courts, with the possibility of forwarding the case to the CJEU.[35] Invalidating an adequacy decision is exclusively possible within the scope of the CJEU's monopoly on jurisdiction.[36]

As is known today, the CJEU has declared the Safe Harbor decision invalid. The court did so mainly for two reasons: firstly, because the decision enabled interference with European fundamental rights through US authorities, disregarding the kind of data being processed, and not providing limits to any interference. According to standing CJEU case law, such interference could only reach to the extent of what is strictly necessary.[37] Secondly, because the de-

---

32 CJEU, 6 October 2015, C-362/14 – *Schrems I*, ECLI:EU:C:2015:650. para. 27.

33 CJEU, 6 October 2015, *Schrems I*, paras. 29 to 35.

34 Ibid., paras. 52, 55.

35 Ibid., para. 65.

36 Ibid., para. 61.

37 Ibid., paras. 86 to 88, 92.

cision did not refer to any existing effective legal protection for individuals. The court referred to *Digital Rights Ireland and Others*[38] stating that an infringement of fundamental rights must be based on "clear and precise rules governing the scope and application of a measure and imposing safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data."[39]

Because the Commission did not satisfactory lay down in its decision, how the US adhere to these criteria, the CJEU declared the Safe Harbor decision invalid on 6 October 2015. Because of the Schrems I judgement by the CJEU, the Irish High Court invalidated the DPC's decision.

3. Implementing Privacy Shield

In an attempt to close the bridge left by the invalidation of the Safe Harbor regime and to create a new legal basis for data transfers between the EU and the US, the Commission issued a new adequacy decision, which entered into force on 12 July 2016. The Privacy Shield, again, was a *limited* adequacy decision,[40] allowing transfers without any additional safeguards between companies, that were certified in the US under the Privacy Shield, and European actors. It was a system based on self-certification, viz US companies could self-constrain their data processing by following a certain set of principles set out in the EU-US Privacy Shield. The processors contractually agreed to act on instruction of the EU controller and committed to help the controller to handle requests of data subjects to exercise their privacy rights.[41]

In comparison to the former Safe Harbor decision, the Privacy Shield did provide for a stricter regime.[42] For example, the right of data subjects to access data, acknowledgement of jurisdiction of a US enforcement agency, and liability for onward transfers were added to the requirements for the privacy policy.

---

38 CJEU, 8 April 2014, C-293/12/C-594/12 – *Digital Rights Ireland and Seitlinger and Others*, ECLI:EU:C:2014:238, paras. 54, 55.

39 CJEU, 6 October 2015, *Schrems I*, para. 91.

40 See Minssen/Seitz et al, The EU-US Privacy Shield Regime for Cross-Border Transfers of Personal Data under the GDPR, European Pharmaceutical Law Review 2020, 34 (36).

41 See recital 14 of the Privacy Shield Decision (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-U.S. Privacy Shield).

42 As recognized by Tzanou, European Union Regulation of Transatlantic Data Transfers and Online Surveillance, Human Rights Law Review 2017, 545 (563); Hatzopoulos/Roma, Caring For Sharing? The Collaborative Economy under EU Law, Common Market Law Review 2017, 81 (109); and others.

Onward transfers broadly were further specified in detail. Data subject's enforcement was strengthened by introducing a binding arbitration mechanism and accepting liability in case of a violation.

However, jurisdiction of the courts, where the data exporter is located, as well as any permission for the DPA in the country of the exporter to undertake an audit were still missing. The only sanction provided for was injunction; but no fines could be implemented under Safe Harbor or the Privacy Shield.[43]

As a result of a series of assurances made by US authorities, such as the Office of the Director of National Surveillance, the US department of Justice and the US Secretary of State, the Commission concluded that data processing for the purpose of national security was restricted to "what is strictly necessary to achieve the legitimate objective in question".

Further, the Commission was convinced, that a number of US law revisions and changes, such as the PPD-28 or the US Judicial Redress Act, could suffice, for US law to be essentially equivalent to EU law. Ultimately an Ombudsperson was introduced: as part of the State Department, (s)he was to guarantee that "individual complaints are properly investigated and addressed".[44]

Among others, the EDPS raised major concerns when the draft of the Privacy Shield Decision was first reviewed.[45] Many observers and privacy activists were critical too, whether real substantive improvements were made. Specifically, that the US had mainly pointed towards existing legal framework when arguing a sufficient level of protection, as well as the rather weak position of the European data subject in front of the Ombudsperson left observers wondering whether there was real progress. Many therefore accused the Commission of basing the Privacy Shield on toothless assurances, with no further effective commitments on side of the US.[46]

---

43 For a comparison of the Safe Harbor and Privacy Shield Decisions, see Zetoony, A Side-by-Side-Comparison of "Privacy Shield" and the "Safe Harbor", Bryan Cave LLP 2019.

44 See Art. 1, paras. 117 Privacy Shield Decision (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-U.S. Privacy Shield).

45 EDPS, Opinion 4/2016 on the EU–US Privacy Shield draft adequacy decision, 30 May 2016; Article 29 WP, Opinion 01/2016 on the EU–U.S. Privacy Shield draft adequacy decision, 13 April 2016, WP 238.

46 Tzanou, European Union Regulation of Transatlantic Data Transfers and Online Surveillance, Human Rights Law Review 2017, 545 (562 et seq).

4. Schrems II: Main elements, invalidating Privacy Shield

As a consequence of the Schrems I case, the DPC had to reopen the causa on international data transfers between Facebook Ireland and Facebook Inc. The invalidation of the Safe Harbor decision prompted the DPC to call on Maximilian Schrems to reformulate his complaint. Within the framework of an investigation on the part of the DPC, Facebook Ireland claimed to transfer data to Facebook Inc. pursuant to SCCs. Schrems claimed, the lack of sufficient protection of data in the US cannot be sufficiently counteracted through SCCs. Particularly, he pointed to US state authorities, such as the National Security Agency and the Federal Bureau of Investigation, to which transferred data is being made available to. He argued that such extensive monitoring is incompatible with fundamental European rights, as guaranteed in Art. 7, 8 and 47 FRC. He therefore asked the DPC to suspend or prohibit future transfers to the US conducted pursuant to SCCs.[47]

The DPC, on 24 May 2016, issued a "draft decision" on the matter. The DPC elaborated that its investigation relied on two strands: the first one related to in how far and on what legal basis Facebook Ireland has continued to transfer data to the US after the Schrems I judgement and the second one on whether the US can ensure an adequate protection as prescribed by the adequacy criteria in Art. 25 sec. 2 Data Protection Directive (compare Art. 45, 46 GDPR).[48] Facebook Ireland stated that they continuously have transferred data, relying on SCCs as the legal basis.[49] Further, the DPC analyzed a range of US laws relating to data privacy as well as the availability of effective remedies and concluded, that there are open questions concerning redress and particularly SCCs. Therefore, the DPC considered Schrems' reformulated complaint regarding the questionable protection provided through SCCs well founded. The validity of the SCC Decisions by the Commission could not be decided by the national Data Protection authority or a national court, but only by the CJEU. The DPC therefore decided to approach the Irish High Court as the competent national court with the matter, noting that in the event the concerns are being upheld, the Irish High Court may refer the case to the CJEU for a preliminary ruling.[50]

---

47 CJEU, 16 July 2020, *Schrems II*, paras. 54, 55.

48 Draft Decision of the Data Protection Commissioner under sec. 10(1)(b)(ii) of the Data ProtectionActs, 1988 & 2003, Ref: 3/15/766, 24 May 2016, para. 34.

49 Ibid., para. 37.

50 Ibid., paras. 62, 63.

The decision was issued as a draft, in order to give Facebook Ireland and Maximilian Schrems further opportunity for submissions.[51] On 31 May 2016, the DPC brought the case before the Irish High Court.

On 3 October 2017 the Irish High Court proposed to refer the questions to the CJEU. The Court not only limited its assessment to what was brought forward in the DPC's decision, but argued that "all of the evidence, all of the law and all of the arguments advanced by any of the parties" must be considered, particularly insinuating to also consider the meanwhile issued Privacy Shield Decision.[52] Hence, the Irish High Court referred eleven questions with a request for a preliminary ruling to the CJEU in accordance with Art. 267 TFEU.[53]

There were eleven questions referred to the CJEU; that can be summed up in five main points:[54]

a. Does EU law apply on matters regarding data processing for purposes of foreign law enforcement and conduct of foreign affairs?
b. How is the level of protection that needs to be assured in a third country to be assessed? Does it constitute a violation of European fundamental rights if data is being transferred from the EU to the US?
c. How far does the competence of the DPA, here the DPC, reach if there is a breach of European data protection in the view of the respective DPA?
d. Are the SCC Decisions still a valid instrument? Specifically, do they suffice to guarantee an adequate level of protection?
e. Is the Privacy Shield Decision binding on the DPAs as well as the member states' courts?

The following sub-chapter provides a more detailed insight to the key subjects of international data transfers as well as an analysis of the CJEU's response to these five questions.

---

51 Ibid., Preliminary Points I (b).

52 Irish High Court, 3 October 2017, *The Data Protection Commissioner v Facebook Ireland and Maximilian Schrems*, No 2016/4809 P, para. 90.

53 Irish High Court, 4 May 2018, *The Data Protection Commissioner v Facebook Ireland and Maximilian Schrems*. No 2016/4809 P.

54 Irish High Court, 12 April 2018, *The Data Protection Commissioner v Facebook Ireland and Maximilian Schrems* (Preliminary Reference to CJEU), No 2017/4809 P.

a. Applicable Laws

The first question deals with Facebook Ireland's objection, EU data protection law would not be applicable due to the limited material scope of the GDPR set out in Art. 2 sec. 1, 2 lit. a, b, d GDPR, specifically if read together with Art. 4 sec. 2 TEU. Art. 4 TEU governs the distribution of competences between the EU and its member states, and stipulates that national security remains competence of the member states. The CJEU found that this provision concerns the EU member states only, therefore is "irrelevant" for the interpretation of Art. 2 GDPR in the constellation in question.[55]

What is remarkable is that this argument was not brought forward in the context of the Data Protection Directive in Schrems I.[56] However, the line of case law remains valid under the GDPR, and also a black letter interpretation provides clear results: Transfers of personal data from an EU branch to a third country also underlie the scope of the GDPR, in the sense of Art. 2 sec. 1 GDPR.[57] Exemptions to the application exist but are to be interpreted strictly.[58]

An exemption does not apply in this case. Neither does the transfer take place in the context of a private or household activity, nor is Facebook's activity outside of EU law or falling within Title V Chapter 2 of the Treaty of the EU (TEU).[59] Rather are the transfers in question between two legal persons, namely Facebook Ireland and Facebook Inc.[60] Art. 2 sec. 2 lit. d GDPR exempts data processing by competent authorities for the "purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".[61] Data processing by authorities in a third country after a transfer from an EU member state can never cause the inapplicability of the GDPR. The very aim of the GDPR is to protect EU data subjects from unproportionate data access. This is also implied by Art. 45 GDPR, whereby the Commission must also examine in the course of the adequacy procedure whether access for purposes of public security, or similar, by foreign authorities happen only to the extent necessary.[62]

---

55 CJEU, 16 July 2020, CJEU, 16 July 2020, *Schrems II*, para. 81.

56 CJEU, 6 October 2015, *Schrems I*.

57 Art. 2 sec. 1 GDPR.

58 CJEU, 10 July 2018, C-25/17 – *Jehovan todistajat*, para. 37.

59 Chapter 2 of the refers to the Common Foreign and Security Policy.

60 CJEU, 16 July 2020, *Schrems II*, paras. 83 to 85.

61 Art. 2 sec. 2 lit. d GDPR.

62 Art. 45 GDPR; CJEU, 16 July 2020, *Schrems II*, para. 87.

Whether Maximilian Schrems actually suffered such an unproportionate data access was not relevant. The CJEU's approach to data privacy is broader than the requirement of *victim status* as used by the European Court of Human Rights (ECtHR), as stated already in Schrems I and is now a long-standing court tradition.[63] This is coherent with the aims of data protection, since already a well-founded suspicion of a lack of privacy can have consequences: the mere possibility of surveillance can have a chilling effect on the exercise of fundamental rights.

The GDPR explicitly targets third country transfers and seeks to protect EU data subjects' rights, not to have their data being accessed by foreign authorities by an extent neither necessary nor proportional. The judgement, in this respect, underlines the position of the CJEU not to limit data protection to EU territory only, but to achieve a global level of protection for EU data subjects.[64]

While some argue the EU's position in that regard is chauvinistic and "disconnected" from the US perspective,[65] it seems reasonable that as long as there is no sufficient protection level on a global level that respects fundamental and human rights, there is no alternative but to adopt this European view and to apply EU law to any third country transfers. The EU has this regulatory effect in various areas; scholars also aptly speak of the "Brussels effect".[66]

However, such a serious protection gap in the law of a third country must first be identified, which is why a non-exhaustive overview of relevant US legislation will be given in a next step in this paper and problems with compatibility with EU law will be addressed.

US laws, as the CJEU found, have several shortcomings that impede the protection of personal data and violate the GDPR.[67] In essence, the court pointed to the far-reaching possibilities of surveillance that exist under the US national security laws (inter alia US Foreign Intelligence Surveillance Act (FISA) Sec-

---

63 See CJEU, 6 October 2015, *Schrems I*, para. 87; CJEU, 8 April 2014, *Digital Rights Ireland and Seitlinger and Others*..

64 See CJEU, 16 July 2020, *Schrems II*,; CJEU, 3 October 2019, *Glawischnig-Piesczek*; CJEU, 6 October 2015, *Schrems I*; CJEU, 13 May 20214, *Google Spain and Google*; CJEU, 8 April 2014, *Digital Rights Ireland and Seitlinger and Others*.

65 See e.g. Bender, Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective, International Data Privacy Law 2016, 117 (128).

66 Hadjiyianni, The European Union as a Global Regulatory Power, Oxford Journal of Legal Studies 2020, 1 (3).

67 This overview of US law is limited on the relevant statutes in the Schrems II case. More detail on the newer EO 14086 follows in Chapter IV.2.b) Executive Order 14086 in this paper.

tion 702[68], Executive Order (EO) 12333[69] and Presidential Policy Directive 28 (PPD-28)[70]).[71] EO 12333, a presidential instrument issued in 1981 by President Ronald Reagan, legitimizes extended surveillance powers through US authorities.[72] Two programs that were examined more closely by the court are PRISM and UPSTREAM, both operate under the umbrella of FISA 702 that authorizes warrantless surveillance. But one has to consider that these are known forms of surveillance, to what extent US authorities intercept data subjects is uncertain. Both are US surveillance programs and collect data either directly from undersea cables or through providers, i.e. private entities.[73] Found problematic was specifically that there is no limitation as to the scope of application of the program or any minimum safeguards.[74]

What was not considered by the CJEU but is certainly noteworthy: PRISM operates – as a secret program – in complete opacity, and discriminates according to nationality, with an over 50% probability of a foreign target.[75] Even more biting is, that the US Supreme Court has held[76] that individuals may not bring a claim under FISA 702, since they cannot know whether they have been surveilled or not.[77] The Foreign Intelligence Surveillance Court (FISC) does not accept complaints brought by foreigners, as its jurisdiction is limited to US residents only. US law is discriminatory of nationality also in the regard that it offers constitutional protection, under the First and Fourth Amendments,

---

68 Foreign Intelligence Surveillance Act of 1978, 95th Congress of the United States, Pub.L. 95-511, 92 Stat. 1783, S. 1566, 25 October 1978 (FISA).

69 Executive Order 12333 of 1981, signed by President Ronald Reagan, 4 December 1981 (EO 12333).

70 Presidential Policy Directive 28: Signals Intelligence Activities, signed by President Barack Obama, 17 January 2014 (PPD-28).

71 CJEU, 16 July 2020, *Schrems II*, paras. 60 to 65.

72 Bender, Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective, International Data Privacy Law 2016, 117 (120); Cappello, Big Iron and the Small Government: On the History of Data Collection and Privacy in the United States, Journal of Policy History 2017, 177 (179).

73 Churchess/Zalnieriute, "Contracting Out" Human Rights in Inter-national Law: Schrems II and the Fundamental Flaws of U.S. Surveillance Law, Harvard International Law Journal Online 2020, <https://harvardilj.org/2020/08/contracting-out-human-rights-in-international-law-schrems-ii-and-the-fundamental-flaws-of-u-s-surveillance-law/>, 4.

74 See Ibid., 6.

75 See Tzanou, European Union Regulation of Transatlantic Data Transfers and Online Surveillance, Human Rights Law Review 2017, 545 (555 et seq).

76 See judgement by U.S. Supreme U.S. Supreme Court, 26 February 2013, *Clapper v Amnesty International*, 5668 U.S. 398.

77 See Tzanou, European Union Regulation of Transatlantic Data Transfers and Online Surveillance, Human Rights Law Review 2017, 545 (551).

solely to US residents.[78] These issues are not solved by the Judicial Redress Act either, as national security is excluded from its scope.[79] An attempt to counteract the revelations and restrict these extensive powers, was PPD-28. It provides for certain principles and limits for data processing, e.g. in order to identify "new or emerging threats and other vital national security information".[80] Critics, including the CJEU in Schrems II, found that the definitions are too broad and the aims too wide to be considered "targeted".[81]

The CJEU concluded, that US legislation, as a combination of extensive data access by authorities with a lack of effective remedy for Europeans, infringes fundamental rights, also stressing the lack of independency of the appointed Ombudsperson.[82]

b. Legal Test: What constitutes an adequate level of protection?

In a next step, the CJEU elaborated how the level of protection needs to be assessed in order to be considered 'adequate'. The judgement states that the "term 'adequate level of protection' must, (...) be understood as requiring the third country in fact to ensure, (...), a level of protection of fundamental rights and freedoms that is *essentially equivalent* to that guaranteed within the European Union" (emphasis added).[83] Again, it is made clear that the standards, to which further data processing is subject, must not undermine European law. Clarifying the scope of European law guaranteeing fundamental rights, the CJEU specified that the CFR is authoritative, and the European Convention of Human Rights (ECHR) provides mere guidance, since the EU itself has not yet joined it.[84]

According to Art. 46 sec. 1 GDPR data transfers "must be afforded appropriate safeguards, enforceable rights and effective legal remedies".[85] Appropriateness, enforceability and effectiveness are to be interpreted in the light of the CFR. And data transfers are deemed appropriate under the GDPR if they can

78 Ibid., 545 (555).

79 Judicial Redress Act of 2015, 114th Congress of the United States, Pub.L. 114-126, 130 Stat. 282, S. 125, 24 February 2016 (Judicial Redress Act).

80 Sec. 2 PPD-28.

81 CJEU, 16 July 2020, *Schrems II*, paras. 181, 183; previously already noted in EDPS opinion, 30 May 2016, 8.

82 See CJEU, 16 July 2020, *Schrems II*, paras. 168, 190.

83 See CJEU, 16 July 2020, *Schrems II*, para. 94.

84 See CJEU, 16 July 2020, *Schrems II*, para. 98.

85 See CJEU, 16 July 2020, *Schrems II*, para. 103.

hold up to that high threshold, by living up to the requirements under the GDPR read in combination with fundamental rights in the CFR. The phrases "read in the light", "interpreted in a compatible manner", "interference with fundamental rights enshrined" are used repeatedly in the judgement.[86] However, the CJEU, in Schrems II, leaves open what exactly such an understanding means. Significantly, the court did not find, that the digital economy or any other protected interest could provide for justification to legitimize of a violation of fundamental rights.[87] The role of the CJEU in protecting fundamental rights in this respect and the possibility for individuals to successfully bring an action also shows that the court stands for an EU that is a union of shared values and that it also takes into account Art. 2 TEU; and not only for the protection of a mere economic alliance.

In order to understand the criteria laid down in Schrems II, not only a detailed understanding of the GDPR, but also profound insights into applicable fundamental rights and their interpretative value are crucial. Therefore, a brief overview of the relevant provisions Art. 7, 8 and 47 CFR follows.

Art. 7 CFR contains the more general right of respect for private and family life, while Art. 8 CFR specifically protects personal data, and guarantees fair processing on a legitimate basis only, as well as a right to access and rectification. Further, an independent authority has to oversee compliance with these rights.[88] The fair trial provision, Art. 47 CFR, enshrines the fundamental right to an effective remedy in the event of a violation of one's rights, which apply under EU law.[89] Schrems I as well as Digital Rights Ireland were the first two cases, where the CJEU developed a framework and boundaries around fundamental rights to privacy, and Schrems II fits right in.[90] The court followed the concept of "impairment of essence" whereby a complete lack of remedy, available to EU data subjects in the US, in the meaning of Art. 47 CFR constitutes a violation;[91] peculiarly the court did not indicate any "overriding reasons" that

---

86 Can be found in CJEU, 16 July 2020, *Schrems II*, paras. 64, 94, 97, 101, 132.

87 Seubert/Becker, The Democratic Impact of Strengthening European Fundamental Rights in the Digital Age: The Example of Privacy Protection, German Law Journal 2021, 31 (36).

88 Art. 7, 8 CFR.

89 Art. 47 CFR.

90 See CJEU, 6 October 2015, *Schrems I*; CJEU, 8 April 2014, *Digital Rights Ireland and Seitlinger and Others*.

91 Brkan, The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning, German Law Journal 2019, 864 (868).

could potentially justify a violation.[92] Remarkably, the CJEU held that a possibility access personal data, without further differentiation, directly violated the essence of Art. 8 CFR.[93]

That being said, it is unfortunate that, once again,[94] the CJEU did not provide an in-depth analysis on fundamental rights and EU privacy laws.

The CJEU left it open, how exactly an "adequate protection" looks like. In order to be compatible with European fundamental rights, two pillars stand out: firstly, there must be an effective remedy made available to Europeans. In this regard, e.g., an independent Ombudsperson as a truly quasi-judicial mechanism could do the trick. Secondly, the complete lack of transparency of the scope of the surveillance is extremely problematic. This issue might be more difficult to resolve, since then again, secret operations are inherent to the functioning of the programs. But the fact that there are no limits to data processing, such as effective necessity and proportionality tests, is untenable, and are deemed to be incompatible with European fundamental rights.

c. Competences and Obligations of Supervisory Authorities

What exactly is the role of the DPC, or any Supervisory Authority? Must, and if so, when must the Supervisory Authority pull the emergency brake on transfers? Chapter VI of the GDPR sets up the framework for European Supervisory Authorities, which are the competent authorities to execute the GDPR and, respectively, data privacy in Europe. In their role the Supervisory Authorities are obliged to handle complaints brought by EU data subjects and forward them to the national courts if necessary.[95]

Art. 58 GDPR sec. 2 lit. f and j GDPR make it clear, that the corrective powers include to impose a ban to process data as well as an order to suspend international transfers. The question imposed on the CJEU was: Does the Supervisory Authority have to use this power, if it concludes that a transfer is in violation

---

92 Some believe the court did not want to balance a non-EU public interest at stake: US national security against an EU fundamental right; Azoulai/van der Sluis, Institutionalizing personal data protection in times of global institutional distrust: Schrems, Common Market Law Review 2016, 1343 (1365).

93 Critized inter alia by Bender, Having mishandled Safe Harbor, will the CJEU do better with Privacy Shield? A US perspective, International Data Privacy Law 2016, 117 (128); Brkan, The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning, German Law Journal 2019, 864 (875).

94 As in CJEU, 6 October 2015, *Schrems I*.

95 See CJEU, 16 July 2020, *Schrems II*, para. 157.

of the GDPR? While it is up to the Supervisory Authority to determine when it deems it necessary and appropriate to take action, and the GDPR leaves some room for maneuver, it is the Supervisory Authority's primary task to monitor GDPR implementation and it is "required to exercise its responsibility for ensuring that the GDPR is fully enforced with all due diligence".[96] It is to be differentiated whether a transfer relies on an adequacy decision, or appropriate safeguards. Only the CJEU can render an adequacy decision by the Commission invalid, which means, that acting according to EU law, the Supervisory Authority cannot challenge such a decision. If the Supervisory Authority finds – on its own initiative or through investigation of a well-founded complaint – that a transfer pursuant to an adequacy decision is in violation of the GDPR, it must forward the case to the CJEU, as the competent court.[97] The court hereby consolidated its monopoly on interpretation and its role as shaper of European data protection.[98]

If a data transfer is based on SCCs, the Supervisory Authority, if it finds a breach, can not only suspend or prohibit the transfer, but is obliged to do so, as this competence is directly conferred on the Supervisory Authority in the SCC Decisions, but also by the GDPR.[99]

As the duties are thus quite clearly set out, the question arises as to what the consequences of the Supervisory Authority's failure to act in such a case might be?

d. Validity of Standard Contractual Clauses

The CJEU gauged on the validity of the SCC Decisions in terms of their ability to ensure appropriate protection, as SCCs bind the controller established in the EU as well as the recipient of the data in the third country, but as a general rule they do not bind authorities of a third country; nor can they bind them, as only signatory parties are bound by the agreement due to its contractual nature. The SCC Decisions by the Commission do not guarantee protection against access by authorities in the third country.[100]

---

96 See CJEU, 16 July 2020, *Schrems II*, paras. 107 to 112.

97 See CJEU, 16 July 2020, *Schrems II*, paras. 120 and 156; already held in CJEU, 6 October 2015, *Schrems I*, para. 61.

98 See Tzanou, European Union Regulation of Transatlantic Data Transfers and Online Surveillance, Human Rights Law Review 2017, 545 (554).

99 See recital 5 SCC Decision 2016; CJEU, 16 July 2020, *Schrems II*, para. 157.

100 See CJEU, 16 July 2020, *Schrems II*, para. 123.

There is 'no one size fits all' solution for data transfers, foremost because the type and amount of data, the purpose of the transfer, the legislation in the third country, and parties involved differ significantly, therefore the infringement of rights and the threshold varies greatly too. Thence, the court found while for some transfers the SCCs can provide for sufficient protection, for others they cannot.

As a general rule, when using SCCs, there is no restriction to using the clauses in a SCC Decision by the Commission, in fact the GDPR encourages the data exporter to ensure an adequate level of protection, by appropriate safeguards; viz *any* appropriate measure.[101] While an adequacy decision by the Commission needs to assess the protection level in a specific country, the SCC Decision provides mere guidance for contractual safeguards to transfer data to any third country under Art. 46 GDPR. Therefore, the transfer will always require a tailored approach and further assessment, with the responsibilities for evaluation resting with the parties involved in the specific transfer, i.e. the data processor or the controller.[102] The CJEU has therefore concluded that the SCC Decisions are still a valid instrument in general and an examination in the light of the CFR, or the competence of the SA could not contradict this assumption of validity.[103]

e. Validity of the Privacy Shield Decision

The last item on the court's agenda was to rule on the validity of the Privacy Shield Decision. The issue was raised neither by the Irish DPC nor by Maximilian Schrems directly, naturally also because he filed his reformulated complaint before Privacy Shield was even issued. However, the question was brought up in the preliminary proceedings by the referring court, as it specifically wondered whether the introduction of the Ombudsperson mechanism could live up to the requirements of Art. 47 CFR.[104]

---

101 See Art. 46 GDPR; this view is also stressed again in COMMISSION IMPLEMENTING DECISION (EU) .../... of XXX on standard contractu-al clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Proposal SCC Decision 2020), recital 3.

102 See CJEU, 16 July 2020, *Schrems II*, para. 134.

103 See CJEU, 16 July 2020, *Schrems II*, para. 149.

104 See CJEU, 16 July 2020, *Schrems II*, para. 150.

The question of validity was not directly raised, and the Advocate General decided not to deal with the matter in these proceedings, but the CJEU did so anyways.[105] The court may have done so in the name of procedural economy, as the issue was raised in another proceeding. A French NGO fighting for privacy and digital rights brought an action against the Commission with the allegation of having taken a manifestly unlawful adequacy decision and requesting to declare Privacy Shield void. The case was closed with order in December 2020, since the matter has been settled with Schrems II.[106]

As in Schrems I, Schrems II tore down the adequacy decision over a provision that limits the applicability of the principles in the Privacy Shield to the "extent necessary to meet national security, public interest …" and other exemptions.[107] Perceived as problematic in this matter was that this access, enabled by US law through FISA 702 and EO 12333 surveillance programs like PRISM or UPSTREAM, by public authorities was not subject to any further limitation, such as necessity or proportionality. In addition, neither PDP 28 nor EO 12333 provide for a judicial remedy for EU data subjects in US courts, reprieving them of their fundamental right to an effective remedy.[108]

The introduction of the Ombudsperson mechanism with the Privacy Shield decision could not counteract this criticism. This is firstly, because of the lack of independency from the Secretary of State and secondly, because there is no indication that a decision by the Ombudsperson is even remotely quasi-judicial, e.g. there are no special safeguards to protect the person from being removed from office, but also there is no assurance that a decision by the Ombudsperson is binding for US authorities either.[109] The mechanism for judicial remedy in the Privacy Shield thus fell far short of the requirements of Art. 47 CFR. The Privacy Shield did not meet the criteria of Art. 45 GDPR and was therefore declared invalid as of the date of the judgement.[110]

---

105 Compare Opinion of Advocate General Saugmandsgaard Øe delivered, 19 December 2019, C-311/18, *Schrems II*, ECLI:EU:C:2019:1145

106 See CJEU, 14 December 2020, T-738/16, *La Quadrature du Net and Others v Commission*, ECLI:EU:T:2020:638.

107 See para. I. 5 Annex II Privacy Shield Decision.

108 See CJEU, 16 July 2020, C-311/18 – *Schrems II*, para. 192.

109 See CJEU, 16 July 2020, *Schrems II*, paras. 195, 196.

110 See CJEU, 16 July 2020, *Schrems II*, paras. 201, 202.

5. Post-Schrems II era

a. Reactions and business practices

When the DPC Ireland brought the case to the CJEU, it set things all over Europe as well as cross-Atlantic in motion. The judgement was long awaited in the data protection arena; and came as a surprise to few. Privacy shield was heavily criticized by many, even before introduction.[111] The CJEU has already made it clear in its case law that it will act against ongoing data breaches and that it prioritizes data protection globally in general.[112]

After Schrems II there was a big outcry. Many journals and authors produced vivid titles: 'Schrems II hits business hard' or 'A farewell to international data traffic?'.[113] Unquestionably Schrems II is landmark judgement and lives up to the importance conjured up by the Irish High Court.[114]

Two remarks: Data is collected and transferred everywhere. It is a reality in our modern economy. Nonetheless, transfers are often made in a wildly careless, i.e., illegal manner. If something is to change about that, this must also be allowed to manifest. Despite the changes in the legal landscape, in practice such a shock could not be observed yet. Secondly, even in the absence of a valid adequacy decision *and* if there are no appropriate safeguards available, transfers according to Art. 49 GDPR, namely pursuant to a contract or based on explicit consensus by the data subjects or transfers necessary for "important reasons of public interest", remain always possible.[115]

It is useful to keep in mind that the data transfers concerned are not personal data where a transfer may be obvious to the data subject, e.g. hotel bookings or texting a friend in the US via Facebook messenger, but immense data streams that go far beyond such purposes, that neither the data subjects, nor, as often the case, has the processor mapped out data transfers comprehensively. As the volume of personal data involved is simply enormous, it is hard to assess

---

111 EP Resolution, 5 July 2018; Baker, Ars Technica, 2 February 2016; Tzanou, European Union Regulation of Transatlantic Data Transfers and Online Surveillance, Human Rights Law Review 2017, 545 (561).

112 For case law compare: CJEU, 6 October 2015, *Schrems I*; CJEU, 13 May 20214, *Google Spain and Google*; CJEU, 8 April 2014, *Digital Rights Ireland and Seitlinger and Others*.

113 See Günther, Ein Abgesang auf den internationalen Datenverkehr? Privacy in Germany 2020, 192 (192); Knyrim, EuGH Schrems II trifft Unternehmen hart, Datenschutz Konkret 2020, 73 (73).

114 Irish High Court, 3 October 2017, *The Data Protection Commissioner v Facebook Ireland and Maximilian Schrems*, 3.

115 Art. 49 GDPR.

risks or impact on fundamental rights of the data subjects on the basis of an individual transfer. But eventually, that is exactly what companies that are processing personal data on a large scale, however innocuous it may seem, must thoroughly examine.

In November 2020, the European Data Protection Board (EDPB)[116] published its guidelines for companies.[117] To bridge the time between the invalidation of the Privacy Shield and a new framework, the EDPB lays out a six-step plan, that essentially reads as follows:

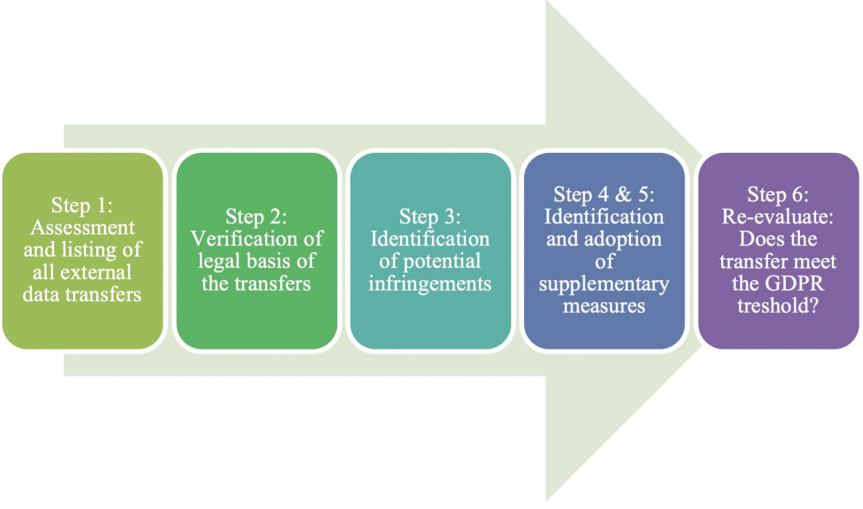

Figure C: Assessment of data transfers by controllers after Schrems II.

From a practical point of view, this guidance posed a variety of problems. The regulations for data transfer have changed constantly, were and some still are in a state of flux, i.e., there was a lot of general uncertainty. Most companies were not sure as to how to react to Schrems II and were mostly waiting for further regulatory guidance.[118]

---

116 The EDPB is an independent European body that unites the national authorities in the EU and aims to ensure consistent enforcement of the GDPR.

117 EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 10 November 2020.

118 Fieldfisher, Schrems II Impacts Report, 9 September 2020, <https://res.cloudinary.com/fieldfisher/image/upload/v1599655199/PDFs/Fieldfisher_-_Schrems_II_Impacts_-_Report_r8eow5.pdf>.

Further, particularly small and medium sized companies (SMEs) in Europe did and do not have the necessary resources to conduct a data assessment in an exhaustive manner. It poses even more difficult, when a European SME that is transferring data, is a controller, and the processor is a huge US corporation. The GDPR provides for the controller to consult the processor to clarify legal issues in the third country. In the rarest of cases, cooperation as envisaged in the GDPR will work.

The most problematic, although economically understandable, development is that companies gauge data protection as a risk, rather than a core element in their business development. The lack of practical implementation of the enormously high penalties tempts companies to make calculations: Yes, the penalty is high, but the probability of prosecution is low.[119]

It follows: Long-term one cannot rely on companies being able or willing to assign the fitting importance to data protection. I.e., to provide financial and human resources, to regularly update legal conditions, to consider and implement technical advances, and what is more: to comply and keep up with the regulations in the country of destination of the data exports. If there is no gross pressure from the data subjects affected, data exporters also have effectively no reason to take and advertise sufficient data protection measures on such a large scale.

The Schrems II case – first and foremost – produced moderate or high costs with regards to time and money spent in legal and compliance.[120] From a data protection standpoint, the consequence may have been the printing and signing standardized clauses at best, and no change at all, at worst, as industries remained in shock while waiting for a *deus ex machina* to produce a solution.

---

119 See CPDP Conference, International Data Transfers: What shall we do to avoid a Schrems III? <https://www.youtube.com/watch?v=gj3wDP_Uhck>.

120 Compare an early (November 2020) survey conducted by Digital Europe: *Digital Europe*, Schrems II. Impact Survey Report, available at <https://cdn.digitaleurope.org/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf>.

b. Finale of the Schrems saga: Largest GDPR fine & transfer suspension

Ultimately, the case was again split into two matters: in addition to the Schrems complaint, the Irish DPC continued its own volition investigation into the transfers.[121]

This paper follows up on the own-volition investigation.[122] After several more submission rounds, judicial review, legal challenges, dismissed applications, renewed invitations to make submissions, and a US government intervention, the Irish DPC issued a revised preliminary draft decision in February 2022.

In its Draft Decision, the Irish DPC found the following:

1. "US law does not provide a level of protection that is essentially equivalent to that provided by EU law".
2. "SCCs cannot compensate for the inadequate protection provided by US law",
3. "Meta does not have in place any supplemental measures which would compensate for the inadequate protection provided by US law".
4. Derogations as set out in Art. 49 GDPR do not justify "systematic, bulk, repetitive and ongoing transfer of users".[123]

Accordingly, the Irish DPC found that Meta violated Art. 46 GDPR. Consequently, the Irish DPC deemed it "appropriate, necessary and proportionate" to order Meta to suspend the data transfers in question.[124]

In accordance with Art. 60 sec. 3 GDPR the Irish DPC shared the Draft Decision with other Supervisory Authorities.[125] Pursuant to Art. 60 sec. 4 any other European DPC may veto the decision within four week: The Austrian, German,

---

121 In May 2021 the Irish High Court published its judgement on the proceedings brought by Facebook Ireland and dismissed all claims and reliefs brought and sought by Facebook Ireland; ultimately approving the DPC's approach to, in addition to the Schrems complaint, start its own volition investigation: Irish High Court, 14 May 2021, *Facebook Ireland v Data Protection Commission*.

122 The complaint-based inquiry (IN-6-3) is "separate and standalone" and to the author's knowledge still pending. See also EDPB, Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR), 5.

123 See EDPB, Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR), para. 23.

124 Ibid, para. 25.

125 See Timeline provided in *Ibid*, 6.

Spanish and French Supervisory Authorities made use of this right. While the supervisory authorities agreed with the findings on the GDPR infringement, the crux of the objections were the remedies. While the Irish DPC thought it sufficient to impose a suspension order, the vetoing authorities insisted on additional corrective measures. They effectively called for two things:

1. Imposing an administrative fine;[126]
2. Demanding the return or deletion of data that has been unlawfully transferred.[127]

As the dispute could not be settled, the matter was brought in front of the EDPB, initiating the dispute resolution procedure.[128] The mechanism aims to ensure a harmonized application of the GDPR in procedures affecting two or more member states.[129]

In April 2023 the EDPB issued a binding decision. The EDPB agreed with the vetoing authorities on both counts.

Firstly, the Irish DPC was instructed to issue a fine considering the factors laid down in Art. 83 sec. 2 GDPR, including e.g.,

- the gravity of the infringement in view of the large scope of processing and amount of data subjects affected,
- that Meta "committed the infringement . . . with at least the highest degree of negligence",
- Meta's high degree of responsibility.[130]

The EDPB concluded with a clear positioning: "in accordance with the EDPB Guidelines on calculation of fines [this] should lead to determining the starting amount for further calculation of the fine at a point between 20 and 100% of the applicable legal maximum."[131]

---

126 See Ibid, paras. 37 et. seq.

127 See Ibid, paras. 192 et seq.

128 See Ibid, 7; also Art. 65 GDPR.

129 More on the Dispute Resolution Procedure under GDPR, see here *EDPB*, Guidelines 03/2021 on the application of Article 65(1)(a) GDPR, adopted on 24 May 2023.

130 See *EDPB*, Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR), para. 272.

131 Ibid, para. 274.

One of the GDPR's characteristic features is that it provides for sanction payments of up to EUR 20 000 000 or 4% of a company's total worldwide annual turnover for certain behaviors, including infringements of the provisions in Chapter V or non-compliance with an order by the data protection authority.[132] The fines were the result of a strong democratic backing, the EU legislator wanted to legislate a culture of harsh sanctioning and enforcement against GDPR violations.[133] As of July 2023, a cumulative amount of EUR 4 billion has been fined.[134]

Secondly, the EDPB requested the Irish DPC to "include in its final decision an order for Meta [...] to bring processing operations into compliance with Chapter V GDPR, by ceasing the unlawful processing, including storage, in the US of personal data of EEA users transferred in violation of the GDPR, within 6 months"[135]

On 22 May 2023 the Irish DPC published its final decision on the matter. Meta was fined EUR 1.2 billion, and was required to suspend future transfers of personal data to the US within the following five months and required to bring its processing into compliance with the provisions regarding international transfers in the GDPR, among other things, by ceasing the processing of illegally transferred data within six months.[136] The Irish DPC therefore executed the EDPB Binding Decision. After over a decade in court, Meta now had to return relevant data to the EU and pay the heftiest fine under the GDPR yet. Considering the reported revenue amounts to roughly EUR 108 billion (USD 116.61 billion), the Irish DPC's fine amounts to roughly 25% of the legal maximum, thus ranking at the lower level of the EDPB imposed benchmark.[137]

---

132 Art. 83 GDPR.

133 Recital 148 GDPR.

134 See GDPR Enforcement Tracker, <https://www.enforcementtracker.com/?insights>

135 See EDPB, Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for ist Facebook service (Art. 65 GDPR), para. 279.

136 Full decision: DPC, 12 May 2023, Inquiry Reference IN-20-8-1, published on the EDPB website: <https://edpb.europa.eu/system/files/2023-05/final_for_issue_ov_transfers_decision_12-05-23.pdf>

137 See Ibid, para. 9.124 for the reported revenue. Calculations are the author's.

IV. The EU-US Data Protection Framework

1. Approval Procedure of the new Framework

The time of uncertainty after Schrems II came to an (preliminary) end in July 2023. For the third time the European Commission renegotiated the third adequacy decision, the EU-US Data Privacy Framework. In March 2022, EU and US leaders reached what was called an "agreement in principle" to address the CJEU's concerns regarding transatlantic data transfers. In October 2022 the International Association for Privacy Professionals (IAPP) titled: "The EU-US Data Privacy Framework: A new era for data transfers?". This question mark remains, even after the new framework entering into force on 10 July 2023. This chapter provides a short overview over procedure and negotiations surrounding the Data Protection Framework.

After the issues brought up in Schrems II mainly pointed protection gaps under US law, many in the EU looked to the US to act. In October 2022 the US white house released an executive order (EO 14086), which served as a basis for a new framework addressing (some of) the concerns brought up by the CJEU in Schrems II.[138] 2.5 years after Privacy Shield got invalidated, in December 2022 the European Commission published a draft for a new adequacy decision.[139] The EDPB issued a nonbinding opinion on 28 February 2023, generally welcoming the improvements made but requires the Commission to clarify certain points as well as ensure sufficient monitoring.[140]

Second to last step is approval of decision by member states. 24 EU member states representing a population of more than 424 million voted in favor of the new framework. 3 member states abstained from voting.[141] The formal adoption through the European Commission College of Commissioners closes the

---

138 See US Department of Justice, 7 October 2022, Executive Order 14086: Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities, <https://www.justice.gov/opcl/executive-order-14086>. Further reading on EO 14086 can be found in Chapter IV.2.b) Executive Order 14086.

139 Commission, Commission Implementing Decision Draft, <https://commission.europa.eu/system/files/2022-12/Draft adequacy decision on EU-US Data Privacy Framework_0.pdf>.

140 EDPB, 28 February 2023, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework. More on the matter in Chapter IV.2.

141 IAPP Dashboard News, 24 EU member states support EU-US Data Privacy Framework, <https://iapp.org/news/a/24-eu-member-states-support-eu-us-data-privacy-framework/#:~:text=Twenty-four EU member states,is more than 424 million>.

process: On 10 July 2023 the European Commission published its implementing decision finding the level of protection of personal data under the EU-US Data Privacy Framework adequate, thus completing the procedure.

See an overview of the approval procedure of an adequacy decision:

Figure D: Overview of Approval Procedure

2. The new Framework on the Merits

Article 1 of the decision reads:

> "*For the purpose of Article 45 of Regulation (EU) 2016/679, the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States that are included in the 'Data Privacy Framework List', maintained and made publicly available by the U.S. Department of Commerce. . .*"[142]

[142] Art. 1, Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework (Implementing Decision DPF).

Once again, a political agreement has been reached, whereby under certain circumstances, data transfers under GDPR are facilitated. What are such "certain circumstances"? Like its predecessors, the adequacy decision is based on a self-certification mechanism, the Data Privacy Framework. Where organizations are certified, data *can* be transferred to without the further need of safeguards under Chapter V. Needless to say that relying on additional safeguards continues to be an option. When organizations self-certify, they declare their commitment to follow the principles laid down in the framework. The US Department of Commerce maintains a public list of organizations that have certified.[143]

This process looks familiar to those who had been acquainted with the Privacy Shield system. What changes prompted the Commission to enter this partnership? Essentially there are two key elements:

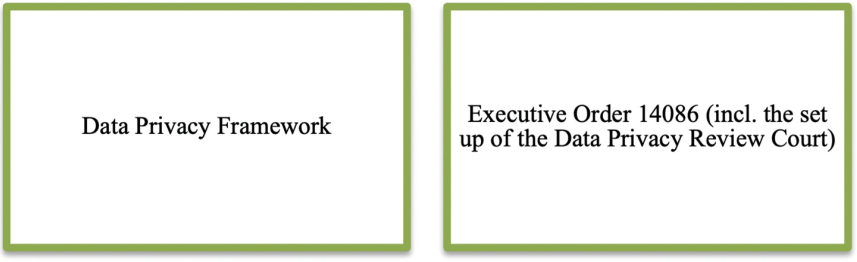

Figure E: Two components leading up to the new adequacy decision

Below the two elements will be critically analyzed.

a. Data Privacy Framework

The Data Privacy Framework is the predecessor of the Privacy Shield Framework, invalidated by Schrems II. When comparing the texts of Privacy Shield with the text of the Data Privacy Framework, little change is apparent. In fact, a rough estimate of about 90% remains the same.[144] Considering that the focus of the CJEU in Schrems II was on the national security aspects rather than the commercial part of the agreement, this comes as no surprise. Nonetheless, the author provides a quick overview of the structures and modifications.

---

143 See Department of Commerce, Data Privacy Framework List, <https://www.dataprivacyframework.gov/s/participant-search>; As of 11 August 2023 the list shows a total of 2486 active and 3748 inactive participants.

144 See Zweifel-Keegan, Unofficial redline (from PS to DPF Principles), available here <https://iapp.org/media/pdf/resource_center/from_privacy_shield_to_dpf_redline.pdf>

The Data Privacy Framework consists of principles (that remain exactly the same), supplemental principles (also barely altered, despite e.g. the amount of the annual fee for organizations is no longer capped at USD 500 and will be co-determined by the Commission and the Department of Commerce).[145] One update to the text of the framework is that it now makes direct references to the GDPR text. The Privacy Shield was negotiated when the GDPR was still in the works, and thus references were made to the Data Protection Directive.[146]

More relevant alterations concern the provisions laid down for participating or potentially participating organizations.[147] There are three scenarios:[148]

- Companies who continued to be certified under the framework, even when it was invalidated and want to keep up the certification: Companies may update their policies within the three months transitional period,[149] and will stay certified without the need to submit a certification request.
- Companies who continued to be certified under the framework, even when it was invalidated and want to withdraw must initiate a formal withdrawal process.
- Companies wanting to certify may sign up via the Data Privacy Framework Website: https://www.dataprivacyframework.gov/

Overall, the way the privacy framework is set up, it achieves continuity and operational simplicity.

Once organizations have signed up, they of course must adhere to the provisions laid down in the Data Privacy Framework. Violations of the Data Privacy Framework are enforceable by the US Federal Trade Commission. Sec. 5 of the Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or affecting commerce".[150]

While this provides for a rather broad authority, the Federal Trade Commission does not have jurisdiction over all companies. There are exempted institutions in various sectors: for example, financial institutions, air carriers, telecommunication companies, and other.[151]

---

145 See Ibid, III. Sec. 5 lit. e.

146 See Ibid, I, Sec. 1.

147 See Ibid, III. Sec. 6.

148 More on this can be found on the Data Privacy Framework Website: <https://www.dataprivacyframework.gov>.

149 That deadline translates to 17 October 2023.

150 Sec. 5 Federal Trade Commission Act (15 U.S. Code § 45).

151 15 U.S. Code § 45 (a) (2); Solove/Schwartz, Information Privacy Law, 7th edition (2021), 869.

The Federal Trade Commission already enforced previous frameworks: Safe Harbor and Privacy Shield.[152] What is more, the failure to deliver on privacy promises is one of the virulent triggers for Federal Trade Commission complaints in US case law.[153]

b. Executive Order 14086: Key elements

> *An attempt to counteract the revelations and restrict these extensive powers, was PPD-28. It provides for certain principles and limits for data processing, e.g. in order to identify "new or emerging threats and other vital national security information". Critics, including the CJEU in Schrems II, found that the definitions are too broad and the aims too wide to be considered "targeted".*[154]

In the Schrems II case, the ECJ focused on national security concerns. EO 14086 was adopted to address the CJEU's conclusion and lay the groundwork for new collaboration. Thus, EO 14086 mostly replaces the PPD-28 mentioned above.

What is EO 14086 all about? It provides for new rules to safeguard data with regards to the specific data collection regimes, such as Sec. 702 FISA and EO 12333.[155] Specifically, it provisions that data collection must only be conducted in pursuit of certain objectives, including protection against terrorism, espionage, or cybersecurity threats.[156] In the light of the objectives, EO 14086 introduces the principles of necessity and proportionality into the US legal framework.[157] This change is relevant as the CJEU in Schrems II required such an "objective criterion" and will require the US Intelligence Community to not only update their procedures and policies, but also implement meaningful changes. It is upon the Commission to monitor whether changes are im-

---

152 See e.g. Fair, FTC settlement focuses on those other Privacy Shield Framework requirements, <https://www.ftc.gov/business-guidance/blog/2020/06/ftc-settlement-focuses-those-other-privacy-shield-framework-requirements>

153 Find an overview of the FTC's Privacy and Security Enforcement here: <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement>

154 See Chapter III.4.a) Legal Applicability in this paper.

155 Compare discussion on these frameworks in Chapter III.4.a) Applicable Laws in this paper.

156 Sec. 2, lit. b (i) (A) EO 14086.

157 Sec. 2, lit. b (i) (B) EO 14086; Also recognized by the EDPB in its opinion: EDPB, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, 4.

plemented and operationalized sufficiently.[158] Critics, inter alia Maximilian Schrems' organization noyb, were quick to point out that while the EO 14086 declares that bulk collection must now be exercised in a way that is "proportionate", there is no agreement between the EU and US as to what that must mean in practice.[159] Notably also, the EO states, while signals intelligence collection must be "necessary", this does e.g. not mean "signals intelligence does [not] ha[s] to be the sole means available [...]".[160] This seems to be a deviation from the understanding of necessity under EU law, according to which the restriction of a person's fundamental rights must be strictly necessary, i.e. a less intrusive means must be used if feasible.[161]

EO 14086 further continues to allow bulk collection of data. While stipulates that "targeted collection shall be prioritized", where "determined to be necessary" bulk collection may be still executed. The limitation found in the EO 14086 states: "Intelligence Community [shall] apply reasonable methods and technical measures in order to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information."[162]

Another point of criticism by the EDPB as well as the European Parliament, was that the EO lacks concise data retention rules.[163]

In Schrems II, the CJEU recalled that a quasi-judicial authority is necessary to fulfill the redress mechanism requirement:

---

158 Also called for by EDPB, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, 31.

159 noyb, European Commission gives EU-US data transfers third round at CJEU, 10 July 2023, <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu>

160 Sec. 2 (a) (ii) (A) EO 14086.

161 On the EU concept of necessity, see e.g., EDPS, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 19 December 2019, <https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf>.

162 Sec. 2 (c) (ii) A EO 14086.

163 This point was brought up by the EDPB as well as the European Parliament; see EDPB, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, paras. 132 et seq; European Parliament, European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)), para. 4.

> *The introduction of the Ombudsperson mechanism with the Privacy Shield decision could not counteract this criticism. This is firstly, because of the lack of independency from the Secretary of State and secondly, because there is no indication that a decision by the Ombudsperson is even remotely quasi-judicial, e.g. there are no special safeguards to protect the person from being removed from office, but also there is no assurance that a decision by the Ombudsperson is binding for US authorities either.*[164]

Sec. 3 of the EO 18046 introduces a renewed redress mechanism to substitute the Ombudsperson and fill in the protection gap. A complaint procedure in front of the Civil Liberties and Privacy Officer (CLPO), an Officer of the Office of the Directive of National Intelligence, in combination with a newly established Data Protection Review Court provides for a two-tier review mechanism to handle complaints. In a first step, the CLPO may investigate qualifying complaints. After completion of its review, the CLPO may

> *"inform the complainant, through the appropriate public authority (...) and without confirming or denying that the complainant was subject to United States signals intelligence activities, that:*
>
> (1) *'the review either did not identify any covered violations or the Civil Liberties Protection Officer of the Office of the Director of National Intelligence issued a determination requiring appropriate remediation'";*[165]

Reading the EO, step 1 of the process appears to be fairly standardized, and it is hard to imagine quasi-judicial procedure and principles being applied.

If the complainant is not content with this outcome, in a second step, he or she may request a review by the Data Protection Review Court. In this case, the Data Protection Review Court appoints a special advocate to represent the complainant's interests during the process.[166] This special advocate is an improvement, as to the representation of the individual in these procedures. Notably, the individual will still not be directly involved in these procedures. This court consists of legal practitioners with relevant experience in the field of data privacy as well as national security law. The individuals may not be US government employees at the time of their appointment. When a complainant requests review, a three-judge panel will "impartially" review the CLPO's determinations, considering the complainant's submissions as well as contributions by the special advocate. The panel further will be guided and is bound by relevant case law by the US Supreme Court.[167]

---

164 See Chapter III.4.e) Validity of the Privacy Shield Decision in this paper.

165 EO 14086 sec. 3 (c) (E) (1)

166 EO 14086 sec. 3 (c) (E) (2), (3).

167 Ibid. sec. 3 (d).

Upon completion, the complainant, in any case, will receive a notice by the Data Protection Review Court that will neither confirm nor deny "that the complainant was subject to United States signals intelligence activities, [and] that '*the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation*'."[168] In essence, then, the complainant never learns whether or not his rights have been violated. Nor will he learn anything about the remedies or have any assurance that he will be protected in the future. What will happen is that the outcome of the procedure, in the form of a classified report, will be subject to oversight by the FISC. This is significant in the sense that it creates at least indirect access to the FISC for foreign individuals. As already discussed, foreigners were previously excluded from access to the FISC.[169]

Overall, the "court" consisting of independent individuals with a certain degree of experience in the relevant field, is a welcome advancement. However, with a pre-determined outcome, restrictions on the complainant's participation in the proceedings, and no further avenues of appeal (e.g., in US federal courts), it is difficult to trust that the new appeal mechanism will endure as a form of "judicial redress" within the meaning of Article 47 CFR in front of the CJEU.[170]

Even if the EO provided sufficient protection, critics argue that it is not enough because it does not come to the level of a law. The US president may by EO, e.g. expand collection by updating the list of objectives.[171] What is more, the EO may be revoked by a subsequent president or overturned by the US congress. However, the adequacy decision is reviewed annually by the Commission. It is to be expected that, in case the EO will be revoked, e.g., under a new presidency, the Commission may reciprocally withdraw the adequacy decision.

Particularly interesting for the international transfer regime (and many European Data Protection Officers): The EO 14086 and national security commitments apply to all transfers. This could allow companies to also use SCCs to

---

168 Ibid. sec. 3 (d) (i) (H).

169 Compare remarks on the FISC in Chapter III.4.a) Applicable Laws in this paper.

170 Also: the EDPB found the Data Protection Review Court "not per se insufficient" but yet shared concerns, see EDPB, Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, adopted on 28 February 2023, para. 220; European Parliament, European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)), para. 8; noyb, European Commission gives EU-US data transfers third round at CJEU, 10 July 2023, <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu>.

171 Sec. 2 (b) (i) B.

transfer personal data to the US. As long as the national security commitments are eligible to uphold adequate protection under the umbrella of the adequacy decision, they are also able to address national security related concerns in the SCC context.

Finally, the major shortcoming of the new agreement is that there is no reform of FISA 702, the main obstacle to transatlantic cooperation. The sunset clause of FISA 702 causes the law to expire by end of 2023, so the timing for reforming the law would have been ideal. As pressure from the EU has now waned, there is little incentive left to significantly reform FISA 702, although some US organizations are urging Congress to do so.[172]

In conclusion: The EO 18046 contains certain textual improvements. Whether they are operationalized must be determined. The Commission issued the adequacy decision within days of the US announcing that the commitments under the EO 18046 have been completed.[173] As pointed out earlier, Art. 45 GDPR requires the Commission to not only consider the "law in the books" but go further and consider implementation too. In the present constellation, such an assessment was not possible[174] and only after the adoption of the decision is the Commission in a position to monitor the level of protection provided by the framework.

V. Outlook: Schrems III on the horizon?

The European Parliament, in its May 2023 resolution, found that the "Framework fails to create essential equivalence in the level of protection".[175] On 10 July 2023 (the date of the noyb titled on its website: "European Commission

---

172 See e.g. American Civil Liberties Union (ACLU), Warrantless surveillance under sec. 702 of FISA, <https://www.aclu.org/issues/national-security/warrantless-surveillance-under-section-702-fisa#:~:text=Under Section 702 of the,emails, and other electronic communications>.

173 IAPP, The latest on the EU-US Data Privacy Framework, <https://iapp.org/news/a/the-latest-on-the-eu-us-data-privacy-framework/>.

174 As highlighted also by the European Parliament, European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)), para. 16; also Recital 104 GDPR.

175 European Parliament, European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)).

gives EU-US data transfers third round at CJEU" indicating the organization still sees fundamental issues with the new framework and is ready to challenge it by bringing another claim.[176]

Before Maximilian Schrems could reach into his drawer to pull out the ready lawsuit,[177] a new name was added to the list of Who's Who in the international data transfer sphere: Philippe Latombe. Philippe Latombe is a French Parliamentarian and member of the French DPA, who has been politically active in topics around surveillance law.[178] On 7 September 2023 he announced, that he would challenge the new framework before the CJEU, in his capacity as an EU individual.[179] He reportedly filed two complaints: one requesting the immediate suspension of the framework, another calling for a review of the text. His claim is pursuant to Art. 263 sec. 4 TFEU, which allows any natural or legal person to request a legality review under certain conditions.

A claim under Art. 263 TFEU has already once been brought with regards to the Privacy Shield, where a French NGO started an annulment procedure pursuant to Art. 263 TFEU against the Commission, for issuing an unlawful adequacy decision which allegedly infringed European fundamental rights as well as the GDPR. In the light of Schrems II, the procedure was set aside and then settled reasoning that there is no longer a need to adjudicate because the Privacy Shield Decision was invalidated with Schrems II.[180]

Besides being concerned about the fundamental rights of Europeans, Latombe also shares concerns about compliance with procedural rules, such as the fact that the text had been published only in English and not in the Official Journal of the EU.

---

176 noyb, European Commission gives EU-US data transfers third round at CJEU, 10 July 2023 <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu>.

177 In a talk on 20 July 2023, Maximilian Schrems indicated in a conversation with Luiza Jarovsky that noyb had a "lawsuit in the drawer" and they were waiting for companies to sign the new framework as well as for a "person whose data has been transferred under the framework". Talk was published on YouTube and is available here: <https://www.youtube.com/watch?v=p1_F9Sorgjg>.

178 His Wikipedia page reads: "Since 2022, he has also co-chaired a fact-finding mission on video surveillance in public spaces." (see <https://en.wikipedia.org/wiki/Philippe_Latombe>).

179 See Latombe, Communiqué de presse, available here <https://www.politico.eu/wp-content/uploads/2023/09/07/4_6039685923346583457.pdf> (French only).

180 CJEU, 25 October 2016, *La Quadrature du Net and Others v Commission*.

This procedure has the advantage that, unlike the procedure Maximilian Schrems followed, there is no need to wait for the companies to sign and for an individual's data to be transferred (i.e., to wait for the damage to be done). Under Art. 263 TFEU, a legality review can directly be requested. One hurdle to admissibility is that it must be shown that the legal act represents a direct and individual concern. It is therefore not certain that such a request would be admissible. Latombe acted quickly; whether he will succeed remains to be seen.

The story of transatlantic data transfers is therefore far from closed. And the battle in court continues with the new framework. The issue remains economically and politically relevant and affects every citizen in the EU, and probably almost every business.

The GDPR focuses on personal data but beware that the instruments of the new EU Digital Strategy also include provisions on the subject of international data transfers.

The Data Act for example, demands safeguards for non-personal data in the context of international access and transfer.[181] According to the proposal, the stakeholder consultation showed that "76% of respondents perceive potential access to data by foreign authorities on the basis of foreign legislation as a risk to their organisation, with 19% indicating that it is a major risk."[182] There is no doubt that the issues arising from non-personal data are of a different nature than those covered by the GDPR, where the focus is on the underlying fundamental rights of the individual. Nevertheless, a trend can be seen that the EU legislator wants to gradually extend the protection in different areas in the digital economy.

It would therefore be all the more desirable to finally look for long-term solutions. Legislators continue to envision strong data protection in Europe through such "data borders," but implementation continues to fail. 5 years after the entry into force of the GDPR and almost 30 years after the entry into force of the general provisions of the Data Protection Directive. As the technological potential for business grows exponentially and impacts every life, the conversation is just beginning.

181 Chapter VII Data Act Proposal (COM/2022/68 final).

182 Ibid., Explanatory Memorandum, 3. Stakeholder Consultations.