Koç University

Graduate School of Social Sciences and Humanities
LL.M. Private Law

Master Thesis

"Transfers of personal data from the EU to the US: A legal assessment of the current and future framework"

Name: Cihan K. Parlar

Supervisor: Asst. Prof. Dr. Zeynep Ayata

Table of Contents

Introduction

Data is regarded as "the new oil of the digital economy"[1]. Not surprisingly, the European Union understood early that for the proper functioning of the internal market, it needed to apply the free movement of goods principles to the transfer of data across borders. This became especially necessary with regard to personal data, the use of which is restricted at a fundamental rights level by Art. 8 of the Charter of Fundamental Rights of the European Union (Charter) as well as Art. 8 of the European Convention on Human Rights (ECHR).

Personal data is defined as any information relating to an identified or identifiable natural person (so called data subject)[2], and thus comprises a large variety of information such as names, birthdates, ethical background, origin or a simple address. Any use of personal data (referred to as processing)[3], such as collection, storage, alteration, erasure, destruction and equally transfer of data, is prohibited until explicitly permitted by law.[4]

Today the free flow of data between EU member States (intra-EU) is regulated in Art. 1 (3) og the General Data Protection Regulation (GDPR) and has previously been regulated by the GDPR predecessor Directive 95/46/EC (so called Data Protection Directive) under Art. 1 (2).[5] The free movement of data finds its end, when personal data is transferred to so called third countries such as the US or China which are neither a member of the EU nor the European Economic Area (EEA).[6]

Data transfers to third countries are subject to a complex regulation by the GDPR and until May 2018 the Data Protection Directive based on three legal bases, namely *adequacy decisions* by the European Commission (Article 45 GDPR and Article 25 Data Protection Directive), *adequate safeguards* (Article 46 f. GDPR and Article 26 (2) Data Protection Directive), and *derogations* (Article 49 GDPR and Article 26 (1) Data Protection Directive). In its essence, these provisions aim to guarantee a level of protection for personal data transferred outside the EU that is at least similar to the level of protection such data would be provided with within the EU.

Only recently the regulation of third country transfers has been subject to high-stake litigation before the European Court of Justice (ECJ).[7] The European Court of Justice on 6 October 2015, handed down the case *Maximillian Schrems v Data Protection Commissioner* (hereinafter

[1] Joris Toonders, Data Is the New Oil of the Digital Economy, Wired (July 2017), https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (last accessed: 07.03.2018).
[2] See Article 2 (a) Directive 95/46/EC; Article 4 (1) GDPR.
[3] See Article 2 (b) Directive 95/46/EC: "[…] shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction[…]".
[4] See Article 7 Directive 95/46/EC.
[5] Provided a valid legal basis for the processing of data is given.
[6] See Article 44 ff. GDPR and 25 f. Data Protection Directive.
[7] C-362/14 Schrems v. Data Protection Commissioner [2015] (hereinafter Schrems Case).

Schrems Case), regarded as one of the most influential rulings on cross-border data flow[8]. The Schrems Case annulled Safe Harbour[9], an adequacy decision by the European Commission based on Article 25 Data Protection Directive (hereinafter also referred to as DPD) and the primary legal basis for data transfers between the EU and US.

Although the European Commission by now has replaced Safe Harbour by its successor Privacy Shield[10] and Article 29 Working Party[11] issued a Statement declaring "Standard Contractual Clauses and Binding Corporate Rules [both back then still based on the second main legal basis in Article 26 (2) DPD] can still be used"[12], an inconvenient uncertainty persists among data transferring companies from the US such as Facebook, Amazon or Google.

This Master Thesis will hook into the aforementioned uncertainty caused by the Schrems Case by assessing to what extend stakeholders involved in EU-US transfers can rely on the European Data Protection framework for third country transfers of personal data after the Schrems Case. Due to its similarities and only recent adoption (May 2018), this Master Thesis will extent the assessment In light of the adoption of the General Data Protection Regulation (GDPR)[13], which replaced the Data Protection Directive in May 2018, this Master Thesis will expand the assessment not only to the GDPR but also to its predecessor the DPD.

The proposed research works from the hypothesis that the Schrems Case has repercussions -beyond Safe Harbour- for all of the aforementioned three legal bases, *adequacy decisions*, *adequate safeguards*, and *derogations*. The key research question which this Master Thesis aims to answer is thus: *From a pure legal perspective, should companies continue to transfer personal data from the EU to the US after the ECJ Schrems Case?* The research question is of fundamental importance, in that it essentially challenges the regulatory tools and possibilities under the EU data protection framework for third country transfers.[14] It furthermore is also of high economic relevance because a company that transfers data to the US without a valid legal ground can be subjected to administrative fines up to 20 000 000 Euro or up to 4% of the total worldwide annual

[8] Fanny Coudert, Schrems vs. Data Protection Commissioner: A Slap on the Wrist for the Commission and New Powers for Data Protection Authorities, Europen Law Blog (October 2015), accessible under http://europeanlawblog.eu/2015/10/15/schrems-vs-data-protection-commissioner-a-slap-on-the-wrist-for-the-commission-and-new-powers-for-data-protection-authorities/ (last accessed: 07.03.2018).
[9] European Commission Decision 2000/520/EC, 26 July 2000 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.
[10] European Commission Decision 2016/1250/EC, 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.
[11] Article 29 Working Party (hereinafter WP29) is an expert body on EU level, consisting of representatives from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission, advising on data protection related issues.
[12] Article 29 Working Party, Statement of the Article 29 Working Party, 16 October 2015.
[13] Regulation (EU) 2016/679, accessible under http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679 (last checked: 07.03.2018).
[14] "Much more than just derailing the EU-US Safe Harbor arrangement, this could spell the demise for every legal mechanism used to transfer data out of Europe, with significant implications on global trade" (Gabe Maldoff and Omer Tene, 'Essential Equivalence' and European Adequacy after Schrems: The Canadian Example, Wisconsin International Law Journal, 2017, Vol. 32 Issue 2, page 1).

turnover.[15] Finally the research questions also carries high social relevance considering that potentially affected companies such as Facebook, Amazon, Yahoo or Google are providing services we use on a daily basis.

This research question will be investigated via five sub-research questions:

1) To what extent can personal data be transferred between the EU and the US under the former European Data Protection framework?
2) How is the Schrems Case relevant for the Data Protection framework in regards to third country transfers in itself?
3) To what extent does the Schrems Case affect the reliability of the framework for third country transfers under the Data Protection Directive?
4) To what extent does the Schrems Case affect the reliability of the framework for third country transfers under the GDPR?
5) Do valuable alternative solutions exist to the GDPR framework for third country transfers?

This thesis will be divided into five different chapters corresponding to the sub-research questions presented above. Chapter 1 will analyse and define what actually accounts for a data transfer to a third country, followed by a general portrayal of the three legal bases for third country transfers, *adequacy decisions* (Article 25 DPD), *adequate safeguards* (Article 26 (2) DPD), and *derogations* (Article 26 (1) DPD). The Chapter will focus on the DPD, since the GDPR was not in force when the ECJ decided the Schrems Case and therefore presents a building block for the subsequent Chapters. Chapter 2 will first, in order to provide for a better understanding, briefly discuss Safe Harbour, before analyzing the Schrems Case which annulled it. The goal of this Chapter is to filter out potential requirements by the ECJ that need to be considered when transferring data to a third country. Chapter 3 and 4 than apply the findings of Chapter 2 to the framework for third country transfers under the Data Protection Directive and the new GDPR. The outcome of these assessments in Chapter 3 and 4 will already substantially provide an answer to the key research question. To provide for a bigger picture, Chapter 5 will analyze potential alternative solutions to the new GDPR framework for third country transfers. Finally, this Master Thesis will be completed by a conclusion which will answer the key research question.

[15] See Article 83 (5) (c) GDPR.

Chapter 1: The former EU legal framework for third-country data transfers

Introduction

Studies concerning the regulation of transborder data flows, especially focusing on the varying levels of data protection provided within each EU member State, date back to 1973.[16] More than 20 years later, the European Union adopted Directive 95/46/EC (hereinafter Data Protection Directive), which exclusively lays down the grounds upon which personal data can be transferred from an EU country to countries outside the EU, referred to as third countries. Although the DPD in May 2018 was replaced by the GDPR, this Chapter will present the framework based on the DPD to provide not only for a better historical understanding but also in order to provide for a building block in light of the Schrems Case, which will be discussed in Chapter 2. The

The Data Protection Directive provided for three legal grounds for such a data transfer, namely *adequacy decisions* by the European Commission (Article 25), *adequate safeguards* (Article 26 (2), and *derogations* (Article 26 (1)). This chapter will in a first step define and analyze what actually accounts for a data transfer to a third country, before portraying the aforementioned legal grounds in more detail, and thereby establish to what extent personal data could be transferred to third countries under the former applicable European Data Protection framework.

1. Defining: "Data transfer to a third country"

The key element of this Master Thesis is data transfer to a third country, in particular to the US. Unfortunately, as the European Court of Justice (hereinafter ECJ) in its *Bodil Lindqvist*[17] ruling explicitly pointed out, the Data Protection Directive does not provide a definition for the term "transfer to a third country" as used in Art. 25.[18]

Bodil Lindqvist marks a cornerstone decision in international data transfers and concerns the Swedish resident Mrs. Linquist, who created and hosted a homepage on her PC, on which she uploaded personal information about co-workers without obtaining prior consent.[19] The ECJ used *Bodil Lindqvist* as an opportunity to elaborate upon data transfers. The Court determined that merely making personal data accessible on a webpage, does not qualify as a data transfer and stressed that a direct sending of data between the sender and the recipient would be required.[20]

[16] Christop Kuner, Transborder Data Flows and Data Privacy Law (2013), page 38.
[17] Case C-101/01 *Bodil Lindqvist* [2003].
[18] Ibid., at 56.
[19] Ibid., at 12.
[20] Ibid., at 68 f.

The ECJ states that Article 25 f. DPD "sets up a special regime, with specific rules" which constitute "a complementary regime to the general regime […] concerning the lawfulness of processing of personal data".[21] It is important to distinguish between data transfers and mere data transits. A mere data transit is at hand, when for instance a German Google user (or generally data subject), logs into the Google Server in the US to write an email. It is clear that data is transferred from the German user's computing device to the service provider (or generally data controller[22]), but that did not require the special regime of Art. 25 Data Protection Directive to be applied. The Directive already provided protection for data subjects against the processing of data by a data controller, even when the controller was not established within the European Union.[23] The special regime of Article 25 Directive was only required and thus applicable when data was not only sent from a data subject to a controller but sent between controllers (or processors[24]).

Finally, the data had and has to be transferred from inside the EU to a recipient outside the EU or EEA.[25] Article 25 f. Data Protection Directive did not explicitly address the problem of onward transfers, meaning the further transferring of data from the country of import to another third country or to another recipient in the same third country. Article 29 Working Party (WP29)[26] stated that "further transfers of the personal data from the destination third country to another third country should be permitted only where the second recipient country also affords an adequate level of protection."[27] It can therefore be determined that onward transfers under the described circumstances constituted themselves a transfer of personal data to a third country and had to therefore be in compliance with the regime of Article 25 Data Protection Directive.

According to the aforementioned, a data transfer to a third country in the sense of Article 25 f. Data Protection Directive was therefore the sending of personal data by a controller/processor from within the EU directly to a recipient (controller/processor) outside the EU, including onward transfers to a recipient within the same third country or to another third country.

---

[21] Ibid., at 61 ff.

[22] See definition in Article 2 (d) DPD: "'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law".

[23] Article 4 (1) (c) Data Protection Directive.

[24] See definition in Article 2 (e) DPD: "shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".

[25] See also Paal/Pauly, DS-GVO BDSG, 2nd edition 2018, Article 44 at 6.

[26] Article 29 Working Party was an expert body on EU level, consisting of representatives from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission, advising on data protection related issues. Under the GDPR the body was renamed European Data Protection Board (EDPB); see also See also Paal/Pauly, DS-GVO BDSG, 2nd edition 2018, Article 44 at 4.

[27] Article 29 Working Party, First orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy, 26 June 1997, at 6.

Although discussed in more detail in Chapter 4, it is here also important to point out that the aforementioned but also the following (to a large extent) also applies to the current data protection framework under the GDPR. Article 44 GDPR determines that third country transfers shall only take place if the conditions laid out in Chapter 5 - "Transfers of personal data to third countries or international organizations"- are met. Furthermore, the provision also clarifies that onward transfers are deemed to be a third country transfer themselves.

Hence, for the purpose of this Master Thesis it can be determined that the US under the provided definition accounted and still accounts to a third country, whereby all transfers of personal data between the EU and the US fell or fall within the scope of Article 25 f. Data Protection Directive or Art. 44 ff. GDPR.

2. Transfer based on an adequacy decision

This section will analyze the first of the three aforementioned (former) legal bases for third country transfers, namely adequacy decisions. Article 25 DPD provided for a legal ground to transfer personal data to a third country, if the third country in question ensured an adequate level of data protection. Adequacy does not equal equivalence, which allowed for flexibility when assessing a third country's implementation of data protection rules.[28] Article 25 (2) DPD stated that the "adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations". The provision furthermore specified that particular consideration shall *inter alia* be given to "the nature of data, purpose and duration of the proposed processing operation" as well as "the rules of law, both general and sectoral, in force in the third country in question". Additionally, the Data Protection Directive steped away from a pure legal provisional assessment and allowed the consideration of "professional rules and security measures which are complied with in that country".

Although each EU member State could assess the adequacy level of a third country autonomously, the DPD in Art. 25 (3) to (6) provided for European harmonization. Article 25 (3) DPD ensured that EU member States, horizontally, with each other as well as vertically to the European Commission, communicated any *inadequacy* of a third country. The European Commission was afforded a predominant role in the adequacy evaluation process of a third country by Article 25 (6) and Article 25 (4) DPD. According to Article 25 (4) DPD the European Commission could assess and decide that a third country did not provide for adequate protection, which had binding virtue for all EU member States. Article 25 (6) DPD awarded the commission with the power to issue binding adequacy decisions, thereby determining that a third country possesses the required adequate level of protection.

Up until now, twelve adequacy decisions for Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, New Zealand, US and Eastern Republic of

[28] Handbook on European data protection law, 2014, page 133.

Uruguay have been issued and are active.[29] Talks are ongoing with South Korea and the adoption procedure of the adequacy decision concerning Japan was launched on 5 September 2018. From EU-US perspective most relevant was the controversial example of an adequacy decision by the European Union, *Safe Harbour*[30], which was annulled by the Schrems Case and was recently replaced by a succeeding framework referred to as *Privacy Shield*[31] (both discussed in more detail in Chapter 2 and 3 below). An adequacy decision was and still is published in the Official Journal of the European Union and is binding for all EU/EEA member States, including bodies of the EU. Based on such a decision, data transfers to the respective third country could and can be conducted without any explicit approval by the national Data Protection Authorities (DPAs).

In its adequacy evaluation, the European Commission, according to Article 25 (6) DPD, had to ensure an adequate level of protection by considering the respective third country's domestic law or international commitments the country had entered into. Such an evaluation process was and is usually conducted with consultation of the Article 29 Working Party, which has provided frequent feedback on the topic in recent years.[32] Besides assessing the third country's legal system as a whole, the European Commission could and can also restrict itself to certain aspects of the legal system and even single types of data transfers for a specific sector. For instance, in case of Canada the sector private commercial legislation was declared adequate.[33] Notably, such adequacy decisions do not have to be based on an assessment of legal provision, but as for instance in the case of *Safe Harbour*, they can relate to rules that can be described as a (self-regulatory) code of conduct.

The aforementioned laid out the first of the former three legal bases with which it was possible to transfer data to a third country. It is important to recall that any adequacy decision by the European Commission did and does not declare a third country to have an equal but an adequate level of data protection. Transfers to third countries based on such an adequacy decision could and can be conducted without prior authorization and other restrictions.

---

[29] Website of the European Commission, accessible under https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en (Last checked: 15.02.2018); see also Ariel Teshuva, Why Has the EU Made So Few Adequacy Determinations?, Law Blog (January 2017), accessible under https://www.lawfareblog.com/why-has-eu-made-so-few-adequacy-determinations (last checked: 07.03.2018).

[30] European Commission Decision 2000/520/EC, 26 July 2000 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

[31] European Commission Decision 2016/1250/EC, 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.

[32] Inter alia Article 29 Working Party Working document on transfers of personal data to third countries: applying Article 26 (2) of the EU Data Protection Directive to binding corporate rules for international data transfers, WP 74, 03 June 2003; and Ibid., Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995, WP 114, 25 November 2005.

[33] European Commission Decision 2002/2/EC, 20 December 2001, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act.

3. Transfer based on Adequate Safeguards: Contractual Clauses and BCRs

In absence of an adequacy decision, Article 26 (2) DPD provided for a second legal basis allowing EU member States to authorize particular data transfers to the US or any other third country provided *adequate safeguards* were put in place. Similar to Article 25 DPD (adequacy decisions), the provision at hand, in its paragraph (3), provided again horizontal and vertical harmonization measures. Accordingly, any authorization given by an EU member State for a transfer "vehicle" to establish *adequate safeguards* pursuant to paragraph (2) had to be reported to the European Commission as well as disagreement about such an authorization could be challenged by other EU member States as well as the European Commission itself.

3.1. Contractual Clauses

Article 26 (2) DPD explicitly mentioned "contractual clauses" as a vehicle to establish *adequate safeguards*. Contractual clauses were and still are concluded between the data exporter and the data recipient residing in a third country.

Similar to an adequacy decision (see above under 2), according to Article 26 (4) DPD, the European Commission could and can publish a decision determining "certain standard contractual clauses" offer sufficient safeguards. Such standard contractual clauses, if not modified, could and can be used by the data exporter and the recipient to transfer data to a third country, without additional approval by the Data Protection Authorities.

The most important content of standard contractual clauses still are 1) a third-party beneficiary clause, allowing data subjects to exercise rights although not party to the contract; and 2) the recipient agrees to be subjected to the jurisdiction of the exporter country's DPA and courts.[34] Up until now, there are still only three types of standard clauses available: two types of standard clauses for the transfer of an EU controller a third country controller (controller-to-controller)[35] as well as one type of clauses for a controller-to-processor[36] transfer. Additionally, WP29 released in 2014 a working document concerning the transfer of a EU processor to non-EU sub-processors, which was yet not adopted by the European Commission.[37]

Besides such standardized clauses, the so called *ad hoc* clauses could be drawn up between the data exporter and data recipient. Oppose to standard model clauses, ad hoc clauses required and

---

[34] Handbook on European data protection law, 2014, page 137.

[35] For the first type see Annex to European Commission Decision 2001/497/EC, 15 June 2001, on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC; for the second type the Annex to European Commission Decision 2004/915/EC, 27 December 2004, amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries.

[36] European Commission Decision 2010/87/EU, 5 February 2010, on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

[37] Article 29 Working Party, Working document 01/2014 on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor", WP 214, 21 March 2014.

explicit approval by the national DPAs before any transfer could be conducted. The Council of Europe's Consultative Committee on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, published a guide on the preparation of ad hoc contractual clauses.[38] The guide lists fourteen principles that all needed to be considered, *inter alia* information to be provided to the data subject (principle 2), the obligations of the data importer to respect the data protection principles (principle 4), rights of the data subject (principle 7), third party beneficiary clause (principle 8) and jurisdiction of the data exporters establishment (principle 11).[39]

3.2. Binding Corporate Rules

Another vehicle to establish *adequate safeguards* were and under the GDPR still are Binding Corporate Rules (BCRs). BCRs are usually used for transfers within multinational groups of companies, which are established in more than one country and thereby fall under the jurisdiction of more than one national DPA. BCRs can be best described as a legally binding internal code adopted by a corporate group, which provides a legal framework for data transfers within that group.[40]

Similar to *ad hoc* contractual clauses, BCRs require a prior approval by a national DPA. Since often more than one national DPA will be involved, the first approval has to be made to the lead DPA, which will inform all other DPAs about the evaluation carried out.[41] The lead authority shall be determined based on the location of the group's European headquarters. If the headquarter lies outside the EU or it is not clear which the headquarter is, the lead DPA will be determined based on an evaluation of the following points:
a) location of the company within the group with delegated data protection responsibilities;
b) location of the company which is best placed (in terms of management function, administrative burden etc.) to deal with the application and to enforce the binding corporate rules in the group;
c) the place where most decisions in terms of the purposes and the means of the processing are taken;
d) the member States within the EU from which most transfers outside the EEA will take place.[42]

[38] The Council of Europe's Consultative Committee on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data protection, 2002, page 10 ff.
[39] Ibid.
[40] Christopher Kuner, Reality and Illusion in EU Data Transfer Regulation Post Schrems, German Law Journal Vol. 18 No. 04, 2017, page 907.
[41] Handbook on European data protection law, 2014, page 138; see procedure under the GDPR according to Article 47 (1), 63, 60 ff. GDPR.
[42] Article 29 Working Party, Model Checklist: Application for approval of Binding Corporate Rules, WP 102, 25 November 2004.

WP29 has published several documents on BCRs which especially address their relevant content and approval process before the DPA.[43] Accordingly, BCRs should include the Privacy Principles (transparency, fairness, purpose limitation, data subject rights etc.), tools of effectiveness (audit, training, complaint handling system etc.) and an element providing that BCRs are binding (intra group agreement, liability commitment, third party beneficiary clauses).[44]

In conclusion, what can be pointed out for the (former) second legal basis for third country transfers presented thus far is that *adequate safeguards* in the form of contractual clauses or BCRs would and for the GDPR still only allow for data transfers in clearly determined and agreed upon cases. Except for standard contractual clauses, usability of *adequate safeguards* for third country transfers was and under the GDPR still is highly dependent on authorization by the national DPAs.

4. Transfer based on Derogations

The third legal bases for third country data transfers was (and the GDPR equivalent still is) only relevant in case neither an adequacy decision nor an appropriate safeguard is applicable. Article 26 (1) DPD listed a catalog of circumstances (a-f), in which the interest of the data subject may justify the transfer of data to a third country:

- (lit. a) unambiguous consent given by data subject;
- (lit. b) the transfer is necessary for the performance of a contract – or preparation to enter into a contract – which was initiated by the data subject;
- (lit. c) the transfer is necessary for the conclusion or performance of a contract conducted between a data controller and a third party in the interest of the data subject;
- (lit. d) the transfer is necessary or legally required on important public interest, e.g. for the establishment of legal claims (except for national or public security);
- (lit. e) the transfer is necessary to protect vital interests of the data subject;
- (lit. f) the transfer is made from a from public registers which according to laws or regulations is intended to provide information to the public.

By definition, the above had to be seen as derogations from an adequacy decision or appropriate safeguards, and as such interpreted restrictively.[45]

[43] See inter alia Article 29 Working Party: WP102; WP 153; WP 154; WP 155 accessible under http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm (checked: 29.08.2017).
[44] Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 153, 24 June 2008; Article 29 Working Party Working document on transfers of personal data to third countries: applying Article 26 (2) of the EU Data Protection Directive to binding corporate rules for international data transfers, WP 74, 03 June 2003.
[45] Article 29 Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, WP 114, 25 November 2005, page 7.

4.1. Consent (lit. a)

Consent had to be given freely[46], informed and specific as well as prior to the processing. To ensure that there has been no doubt by the data subject, a rather active way of consenting was required. Mere implied consent, for instance by not objecting to an announced data processing activity, would not qualify.[47] Especially in the employment context, it was (and is) questionable whether the data subject can feely consent, due to the power imbalance between employer and employee.[48] That is why additional safeguards must often be applied, such as consultation by a work council.[49]

4.2. Performance of a contract (lit. b) and (lit. c)

WP29 points out, that although the legal ground "performance of a contract" seems to be very broad, it was essentially limited by necessity.[50] Accordingly, the data transfer in question had to be necessary for the performance of the respective contract. Thus, a close link between the purpose of the data transfer and the performance of the contract in question had to be established.

4.3. Important public interest (lit. d)

Similar to the performance of a contract (lit. b) and (lit. c), the important public interest had to be closely linked to the data transfer, thus necessary. Furthermore, only an important public interest identified by "the national legislation applicable to data controllers established in the EU" and thus not the third country was valid. [51]

4.4. Vital interest of the data subject (lit. e)

WP29 refers to vital interest in the context of a medical emergency.[52] Furthermore, the transfer had to be relevant for the treatment at hand, and not be of general nature.[53]

---

[46] Consent is only given freely, "if the data subject is able to exercise a real choice and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent", see Article 29 Working Party, Opinion 15/2011 on the definition of consent, WP187, 13 July 2011, page 12.
[47] Article 29 Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, WP 114, 25 November 2005, page 12.
[48] Ibid.
[49] Ibid., page 11.
[50] Article 29 Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, WP 114, 25 November 2005, page 12 ff.
[51] Ibid., page 15.
[52] Ibid., page 15 f.
[53] Ibid.

4.5. Public register (lit. f)

Finally, data transfers from public registers were seen as a valid legal ground due to their "open nature" which supposed to also be consultable by individuals in third countries.[54] Recital 58 to the DPD restricted the amount of data that can be transferred to individual cases and data.

Conclusion

Chapter 1 set out to answer sub-research question 1, namely to what extent personal data could be transferred between the EU and the US under the former European Data Protection framework. To answer this question this Chapter first assessed and defined the term "Data transfer to a third country" as the sending of personal data by a controller/processor from within the EU directly to a recipient (controller/processor) outside the EU, including onward transfers to a recipient within the same third country or to another third country. Since the US is neither a member of the EU nor the EEA, it falls under the definition of a third country.

In a second step all (former) three legal grounds for such a data transfer, namely *adequacy decisions* by the European Commission (Article 25), *adequate safeguards* (Article 26 (2), and *derogations* (Article 26 (1)) have been analyzed and laid out.

This chapter concludes that although all three legal bases allowed for transfers of personal data between the EU and the US, only *adequacy decisions* by the European Commission (Article 25), such as the annulled Safe Harbour or the newly adopted Privacy Shield allowed for comprehensive and unrestricted processing activities. Standard contractual clauses based on the second legal ground *adequate safeguards* (Article 26 (2), also provided a low level of restriction, since no approval for the transfer by the Data Protection Authorities was required, nonetheless the scope of the data transfer was limited to the contractual agreement. Data transfers to a different US company or different purpose would require the data exporter and data recipient to conclude a new agreement.

On the other hand, BCRs as opposed to contractual clauses, both also based on the second legal ground *adequate safeguards* (Article 26 (2), required approval by the Data Protection Authorities, which made their actual use rather cumbersome. Finally, *derogations* based on Article 26 (1) were only really be useful on a case-by-case basis, and thereby very limited in scope and usability for companies that required a legal basis for permanent transfer of personal data to a third country, such as the US.

[54] Ibid., page 16.

Chapter 2: Safe Harbour, the Schrems Case and the ECJ's requirements for proper regulation of third-country transfers

Introduction

After Chapter 1 assessed the extent to which personal data could be transferred between the EU and the US under the Data Protection Directive, the Chapter at hand now shifts the focus to a Case decided by the European Court of Justice on 6 October 2015, namely *Maximillian Schrems v Data Protection Commissioner*[55] (Schrems Case). The Schrems case, as already mentioned in the introduction of this Master Thesis is regarded as one of the most influential rulings on cross-border data flow.[56] The last time the ECJ had addressed the data flow to a third country issue was its *Bodil Lindqvist*[57] ruling dating back to 2003. Considering that giants such as Google, Yahoo, Amazon and Facebook back then where still in their infant shoes and the global internet usage has almost tripled since 2003, the Schrems Case is a landmark ruling, one that may establish case law for the years to come.

The Schrems Case annulled Safe Harbour, which was the primary legal basis for data transfers between the EU and US. As laid out in Chapter 1, Safe Harbour constituted an adequacy decision by the European Commission according to Art. 25 (6) and was in July 2016 succeeded by *Privacy Shield*.

Chapter 2 aims at answering sub-research question 2, namely how the Schrems Case is relevant for the Data Protection framework in regards to third country transfers in itself. To answer this question, the Chapter will first have to briefly discuss Safe Harbour in order to provide for a better understanding of the subsequently analyzed Schrems Case. The goal of this Chapter is to filter out potential requirements by the ECJ that need to be considered when data is transferred to a third country such as the US. This will allow this Master Thesis to apply the outcome to the framework for third country transfers under the Data Protection Directive (Chapter 3) as well as the GDPR (Chapter 4) and thereby assess the impact the Schrems Case has on these frameworks.

[55] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015].
[56] Fanny Coudert, Schrems vs. Data Protection Commissioner: A Slap on the Wrist for the Commission and New Powers for Data Protection Authorities, Europen Law Blog (October 2015), accessible under http://europeanlawblog.eu/2015/10/15/schrems-vs-data-protection-commissioner-a-slap-on-the-wrist-for-the-commission-and-new-powers-for-data-protection-authorities/ (last checked: 07.03.2018).
[57] Case C-101/01 *Bodil Lindqvist* [2003].

1. Safe Harbour

Safe Harbour[58] was an adequacy decision by the European Commission based on Article 25 Data Protection Directive and the primary legal basis for data transfers between the EU and US. Under this legal basis, a "free" flow of data between the EU and US was possible. Most of our daily used service providers, such as Facebook, Amazon, Google, Yahoo, Twitter, Apple or Microsoft originate as well as headquarter in the US and more importantly process European citizens' data from the US or on US stored servers. Understandably, Safe Harbour is not only relevant from a data protection perspective but is predominantly a matter of commercial trade, which is an important element of the transatlantic relationship between the US and the EU.

Article 1 (1) of Safe Harbour (hereinafter Decision 2000/520), provides that the Safe Harbour Principles, which are annexed to Safe Harbour, ensure an adequate level of protection as required by Article 25 DPD. Annex I of Decision 2000/520 lays out these principles to which US companies can voluntarily subscribe. The principles are regarded as a type of code of conduct.[59] The principles consist *inter alia* of:

- an obligation to inform the respective data subject about all (planned) processing activities of its data and choice to opt-out (Notice and Choice)

- an obligation making any processing of the data subjects data beyond the initially declared purpose such as transferring the data to another third party depending on the data subject's consent or authorization (Onward Transfers)

- an obligation to secure any personal data in possession against unauthorized access or loss (Security)

- an obligation to allow the data subject to access its data and where inaccurate alter, delete or amend the data (Access and Integrity)

- an obligation to establish a recourse mechanism for the data subject in case of non-compliance with by the respective US controller/processor with the aforementioned principles (Enforcement).

Compliance with these principles by a US company is based on a self-regulatory mechanism, by which the company in question needs to issue an accordant privacy policy and declare to the United States Department of Commerce that it complies with the Safe Harbour principles.[60] Companies can demonstrate compliance by joining a self-regulatory privacy program, by

[58] European Commission Decision 2000/520/EC, 26 July 2000 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.
[59] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 13.
[60] Article 1 (3) Decision 2000/520/EC.

establishing their own program or by subjecting the company to an appropriate body of law.[61] Scrutiny and oversight is provided through private dispute resolution by an independent party.[62] Complaints can also be brought before the Federal Trade Commission (FTC).[63] Notably, exceptions to the Safe Harbour principles are justified to the extent necessary to meet national security, public interest or law enforcement requirements as well as in case compliance would be in conflict with US law.[64] Any exception from the principles must be limited to what is necessary to meet the prevailing legitimate interest.[65]

2. Maximillian Schrems v Data Protection Commissioner (*Schrems* Case)

After analyzing Safe Harbour and its fundamental principles, the second part of this Chapter is devoted to the *Schrems* Case. This section will firstly summarize the keypoints of the *Schrems* Case, before analyzing the reasoning of the ECJ as well as its requirements for a legitimate cross-border data flow to a third country in the aforementioned case.

2.1. The *Schrems* Case: A brief Summary

Maximilian Schrems, an Austrian Data Protection Researcher, challenged, on June 25th 2013, Facebook's EU-US transfer policy of personal data, including his own personal data, before the Irish Data Protection Commissioner (national DPA of Ireland).[66] Complaints against Facebook fall within the jurisdiction of the Irish DPA, since Facebook's international headquarter is based in Dublin.

Maximilian Schrems especially focused on Facebook's use of Safe Harbor (Article 25 DPD) to transfer data, and claimed that the US privacy laws, as the 2013 Snowden revelations proved[67], do not provide enough protection against access and use of personal data by intelligence surveillance.[68] The Irish DPA refused to investigate these claims, and pointed to the applicability of the still valid adequacy decision by the EU Commission based on Article 25 (6) DPD - Safe Harbour - as well as its binding effect for EU member States.

---

[61] Article 1 (2) (a) Decision 2000/520/EC; also Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 18.
[62] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 19.
[63] Article 1 (2) (b) Decision 2000/520/EC
[64] Kühling/Buchner, DS-GVO BDSG, second edition, 2018, Article 45 at 38; Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 20.
[65] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 20.
[66] Ibid., at 26 f.
[67] Elaborating upon the link between the Snowden revelations and the Schrems Case: Gabe Maldoff and Omer Tene, 'Essential Equivalence' and European Adequacy after Schrems: The Canadian Example, Wisconsin International Law Journal, 2017, Vol. 32 Issue 2, page 14 ff.
[68] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 28; for a brief description of the US system of law and surveillance see Peter Swire, US Surveillance Law, Safe Harbor, and Reforms Since 2013, Georgia Tech Scheller College of Business Research Paper No. #36 (December 2015), page 3 ff.

In seeking judicial review, Mr. Schrems brought a case against the DPA before the Irish High Court. The High Court asked the ECJ for preliminary ruling upon two questions: (1) whether national DPA's are bound by an adequacy decision by the European Commission; or (2) whether the national DPA needs to conduct its own evaluation when such a case is brought before them.

The ECJ issued its judgement on October 6th, 2015. Addressing the respective questions, the Court ruled that Article 25 (6) DPD does not prevent national DPAs from investigating challenges with regard to adequacy brought before them. The Court states that Article 25 (6) DPD needs to be evaluated in light of the European Charter for Fundamental Rights (hereinafter Charter), and the independence of the DPAs is of high value. If an adequacy decision based on Article 25 (6) DPD, such as Safe Harbour, would restrict national Data Protection Authorities to not challenge adequacy decisions, this would conflict with their mandate to act as an independent watchdog for data protection related matters. Although, the ECJ pointed out that national DPAs may investigate a claim challenging adequacy, only the Court has the power to rule upon an adequacy decision.

The ECJ then pointed out, that Maximilian Schrems in essence contested that US law does not ensure an "adequate level of protection" within the meaning of Article 25 DPD, and therefore to give the Irish High Court a "full answer", the ECJ decided to assess whether Safe Harbour in form of Decision 2000/520/EC actually complies with the DPD in light of the European Charter for Fundamental Rights.[69] Ultimately the Court found the assessment to weigh negatively for Safe Harbour, and went on to annul Safe Harbour.

2.2. The *Schrems* case: The ECJ's requirements for legitimate cross-border data flow to a third country

The ECJ started out its assessment addressing what an adequate level of protection according to Article 25 (2) DPD actually constitutes. The Court acknowledges that neither Article 25 nor any other provision in the Data Protection Directive contain a definition of the term "adequate".[70] As already pointed out in Chapter 1 above, Article 25 (2) DPD only states that the "adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operation"[71] including the consideration of "professional rules and security measures which are complied with in that country"[72].

However, the ECJ draws attention to Article 25 (6) DPD and determines two crucial points. Firstly, the provision requires that "a third country 'ensures' an adequate level of protection by reason

[69] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 67.
[70] Ibid., at 70.
[71] Article 25 (2) DPD.
[72] Ibid.

of its domestic law or its international commitments".[73] Secondly, any assessment that is carried out must consider "the protection of the private lives and basic freedoms and rights of individuals".[74] Although adequate cannot mean identical, according to the ECJ, "the term 'adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter."[75]

Notably, the Court in defining *adequate level of protectio*n as protection that is of *essential equivalence with EU law*, sets a high level of data protection standard for transfers to a third country. This reasoning changes the past understanding that adequacy does not equal equivalence, as pointed out in Chapter 1.[76] The ECJ furthermore specifies its concept of *essential equivalence*, in carving out some (to some extent overlapping) key points[77]:

- Any assessment must take into account the third country's domestic law and international commitments[78];
- The respective country must possess a high level of fundamental rights protection[79]; and
- The respective country must have means for ensuring that a high level of protection can also be achieved in practice[80];
- The system in place must be based on effective detection and supervisory mechanisms; especially allowing for a penalization in case of non-compliance by the controlling/processing company in the third country[81];
- Limitations of such a protection system based on national security, public interest, or law enforcement cannot result in the third country's law primacy over EU law[82];
- Any interference with personal data by public authorities in the third country must be limited and respect fundamental rights[83].

Two focal points can be identified. The first one is the supervision mechanism with regard to private companies and the second one is the protection of transferred personal data against interference by public authorities in the third country. I will now elaborate further on these two points.

---

[73] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 71.
[74] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 71.
[75] Ibid., at 73.
[76] Handbook on European data protection law, 2014, page 133; see also Kühling/Buchner, DS-GVO BDSG, second edition, 2018, Article 45 at 11.
[77] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 73 ff.
[78] Ibid., at 73.
[79] Ibid., at 74.
[80] Ibid.
[81] Ibid., at 81.
[82] Ibid., at 85-87.
[83] Ibid., at 88.

2.2.1. Supervision Mechanism in regards to private companies

The Court acknowledges that Safe Harbour is based on a self-certifying mechanism (see above under point 1) and as such not per se contrary to the requirements of adequate protection.[84] Nonetheless, the Court states that the reliability of such a supervision mechanism "is founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights […] to be identified and punished in practice."[85]

With regard to Safe Harbour (see also above under point 1), the Court points out that a supervision mechanism for detecting non-compliance by US companies is in place. Scrutiny and oversight are provided through private dispute resolution by an independent party[86] as well as the Federal Trade Commission (FTC) (see also above under point 1).[87]

2.2.2. Protection against interference by public authorities in the third country

The ECJ assessed in depth the protection of transferred personal data against any interference by US authorities.[88] The Court stressed that although companies are to some extent sufficiently bound by the Safe Harbour principles, US public authorities are not required to comply with them.[89] A procedure before the Federal Trade Commission (FTC) is only available in case of a commercial dispute.[90]

Consequently, the data subject in question will not have the possibility to access, alternate or erase data relating to him/her. As a result, Decision 2000/520/EC (Safe Harbour) does not provide sufficient legal remedies for the data subject against interference by US authorities[91] and thereby infringes upon the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter[92].

As already pointed out, the Safe Harbour principles may be limited "to the extent necessary to meet national security, public interest, or law enforcement requirements" as well as in case compliance with the principles would be in conflict with US law.[93] The Court stresses that EU legislation involving interference with the fundamental rights enshrined in Article 7 (Respect for private and family life) and 8 (Protection of personal data) Charter, such as Decision 2000/520 (Safe Harbour), must "lay down clear and precise rules governing the scope and application of a

---

[84] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 80 f.
[85] Ibid., at 81.
[86] Ibid., at 19.
[87] Article 1 (2) (b) Decision 2000/520/EC
[88] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 83 ff.
[89] Ibid., at 83.
[90] Ibid., at 89.
[91] Ibid.
[92] Ibid., at 95.
[93] Paragraph four of Annex I (Decision 2000/520); see Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 20.

measure and imposing minimum 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", and that Safe Harbour fails to do so. [94]

However, the Court does not stop here. Under the pretext of assessing Decision 2000/520 (Safe Harbour), the ECJ goes on to essentially assess the level of protection for private life in the US. The ECJ states that legislation in the US is not limited to what is strictly necessary, since it authorizes the storage of personal data that has been transferred from the EU to the US, as well as allows public authorities to access such stored data, and all on a generalized basis.[95] The Court ultimately declares such legislation as "compromising the essence of the fundamental right to respect for private life" under Article 7 Charter.[96] Since Safe Harbour does not establish safeguards that mediate the threat such legislation poses for private life, the ECJ declares the level of protection for privacy and data protection in the US of being essentially <u>not</u> equivalent to the protection level in the EU.[97]

Conclusion

In order to answer sub-research question 2, namely how the *Schrems* case is relevant for the Data Protection framework with regard to third country transfers in itself, Chapter 2 analyzed the *Schrems* case and especially filtered out the ECJ's requirements that need to be considered when data is transferred to a third country. The *Schrems* case focused on Safe Harbour, which represented an adequacy decision by the European Commission based on Article 25 Data Protection Directive and was the primary legal basis for data transfers between the EU and US.

After acknowledging that neither Article 25 nor any other provision in the Data Protection Directive contain a definition of the term "adequate", the ECJ went on to define an *adequate level of protectio*n as protection that is of *essential equivalence with EU law*. This is notable since such a reasoning changes the past understanding of adequacy as not being equal to equivalence.[98] The Court thereby increased the level of data protection standard a third country needs to meet.

The analysis of the *Schrems* case identified two focal points the ECJ put explicit emphasis on when assessing *essential equivalence*. First, that adequacy requires the existence of supervision

---

[94] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 91 ff.
[95] Also acknowledged by the European Commission, see Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 90 and 93.
[96] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 94.
[97] Ibid., at 93; see also Sergio Carrera & Elspeth Guild, Safe Harbour or into the storm? EU-US data transfers after the Schrems judgment, No. 85 CEPS Paper in Liberty and Security, 2015, page 1 ff; see also Kühling/Buchner, DS-GVO BDSG, second edition, 2018, Article 45 at 13; similar Ehmann/Selmayr, Datenschutz-Grundverordnung, second edition 2018, Art. 45 at 6.
[98] Handbook on European data protection law, 2014, page 133.

mechanisms with regard to private companies. Second, the ECJ stressed that an adequate level of data protection requires sufficient protection against interference by public authorities in the respective third country.

To the aforementioned extent, the *Schrems* case might only carry relevance for existing and future adequacy decisions by the European Commission. However, the analysis of the *Schrems* case identified that the ECJ in its judgement went beyond an assessment of Safe Harbour and actually declared that the level of protection for personal data in the US is *essentially* not *equivalent* to the protection level in the EU.[99] Thereby the Court acknowledged that besides the actual legal basis permitting the third country transfer, the level of protection for the transferred personal data in the respective country, based on its legal system and practices, must also be taken into consideration when assessing a transfer of personal data to a third country. The ECJ thereby implicitly declared that none of the existing legal basis for third country transfers, whether based on *adequacy decisions* by the European Commission, *adequate safeguards* or *derogations*, can itself guarantee the legitimacy of such transfers.

The aforementioned therefore clearly shows, that the *Schrems* case possesses fundamental relevance for all legal bases that permit third country transfers, and therefore the framework of such transfers itself. It is therefore necessary to assess to what extent each legal basis in light of the aforementioned can guarantee a level of protection that is *essentially equivalent* to the level of protection in the EU.

[99] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 93; see also Sergio Carrera & Elspeth Guild, Safe Harbour or into the storm? EU-US data transfers after the Schrems judgment, No. 85 CEPS Paper in Liberty and Security, 2015, page 1 ff.

Chapter 3: The former legal framework for third country transfers (DPD) in light of the *Schrems Case*

Introduction

After having carved out in Chapter 2 the relevance of the *Schrems* case for the framework of third country transfers as a whole, Chapter 3 will know investigate the extent to which the *Schrems* case affected the former data protection framework for third country transfers under the Data Protection Directive. Companies such as Google, Amazon or Facebook that have built their business model on such data transfers fundamentally depend on a reliable legal framework that provides legal certainty.

The Court in the *Schrems* case acknowledged that besides the actual legal basis for third country transfer, the level of protection for the transferred personal data in the respective country, based on its legal system and practices must also be taken into consideration when assessing a transfer of personal data to a third country. In order for companies to estimate the legitimacy of any third country transfer that accrued between the Schrems case and the replacement of the DPD in May 2018, it is essential to assess whether the respective legal bases, namely *adequacy decisions* by the European Commission (Article 25 DPD), *adequate safeguards* (Article 26 (2) DPD), and *derogations* (Article 26 (1) DPD), could themselves establish a level of protection that is *essentially equivalent* to the protection of personal data guaranteed within the European Union.[100]

While determining the required level of protection, the ECJ especially criticized the fact that legislation in the US authorizes a generalized storage of personal data that has been transferred from the EU to the US, as well as access to such stored data by the public authorities.[101] In order for the aforementioned legal basis to provide enough reliability for data transferring companies, it is therefore essential, that these legal bases can mitigate or provide sufficient legal remedies for the data subject against interference by foreign authorities to personal data originating from the EU.[102]

This Chapter aims to examine the potential impact of the *Schrems* case upon the former legal framework under the DPD, by firstly taking a look at the newly adopted Privacy Shield[103] as a representative for *adequacy decisions* by the European Commission (Article 25 DPD), followed

[100] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 73.
[101] Also acknowledged by the European Commission, see Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 90 and 93.
[102] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 89.
[103] The European Commission introduced Privacy Shield as a successor to the annuled Safe Harbour; European Commission Decision 2016/1250/EC, 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.

by an examination of *adequate safeguards* (Article 26 (2) DPD), and *derogations* (Article 26 (1) DPD). At the end of the chapter a conclusion regarding the former legal framework for third country transfers in light of reliability for companies will be drawn.

1. Privacy Shield

Privacy Shield constitutes an adequacy decision by the European Commission based on Article 25 DPD. It is the result of intense diplomatic discussions between the EU and US.[104] Similar to Safe Harbour, Privacy Shield is based on a system of self-certification by US companies[105] and commits to same principles of notice, choice, onward transfer, access, security, data integrity and enforcement.

As opposed to Safe Harbour, Privacy Shields focuses more on the individual rights of data subjects, especially with regard to monitoring and scrutiny of US companies, redress possibilities, as well as limitation of interference with personal data by US public authorities.[106] This does not come as a surprise, since both the supervision mechanism with regard to US companies as well as protection against generalized interference by US authorities were the two major points of criticism by the ECJ in the *Schrems* case.[107] What is surprising is the quality of solutions and safeguards with which the EU Commission addresses these two points. To recall, the ECJ did especially point out that the respective country must possess a high level of fundamental rights protection and that the respective country must have means for ensuring that a high level of protection can also be achieved in practice.[108]

Privacy Shield lays out in detail the different paths a data subject can take to file a complaint as well as which organizations will provide adequate monitoring. The Department of Commerce, the Department of Transportation and Federal Trade Commission together will oversee compliance and provide periodic reviews as well as work closely together with domestic DPAs in the EU member States.[109] The European Commission especially provides for enhancements with regard to redress and enforcement mechanisms. Besides direct complaints to the US company, which are similar to Safe Harbour, US companies can now on a voluntary basis subject itself to national DPAs, come up with its own internal compliance mechanism or contract with an independent party. Data subjects can also seek a binding decision by an independent Dispute

---

[104] Kühling/Buchner, DS-GVO BDSG, second edition, 2018, Article 45 at 42 ff.

[105] 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, at 14.

[106] For a more detailed overview Tobias Bräutigam and Samuli Miettinen, ‘Data Protection, Privacy and European Regulation in the Digital Age’, Helsinki Legal Studies Research Paper 46 (December 2016), page 157 ff.

[107] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 81 ff.

[108] Ibid., at 74.

[109] 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, at 34 ff.

Resolution Body (DRB)[110]. In case of non-compliance with a DRB's decision, the data subject can refer its complaint to the Department of Commerce[111]. Notably, US companies now have to subject themselves to the jurisdiction of domestic DPAs in the EU when processing employment data.[112] And finally as a novelty, Privacy Shield establishes the "Privacy Shield Panel", a "last resort" arbitration instance issuing binding decision, which can be used in US courts.[113]

The aforementioned level of protection against US companies clearly presents an upgrade compared to Safe Harbor, which cannot be said for the protection against interference by US authorities, which appears to have increased on paper but essentially still lacks in quality and practice. The EU Commission provides in length the legal framework in the US but never really addresses the concerns raised by the ECJ in the *Schrems* case. Instead, with Privacy Shield the EU Commission establishes a new monitoring mechanism in the so-called Ombudsman, to whom EU citizens can file a complaint when data is somehow processed by US intelligence agencies. Whether and how such a complaint will then be dealt with is not addressed. The European Commission elegantly overlooks access rights by the data subject as well as the possibility to seek a judicial decision in such cases, except for the possibility to sue for damages.[114] What must be seen as an attempt to whitewash the non-existing applicability of the US Constitutions Fourth Amendment to non-US residents, the European Commission points out that the constitutional guarantees are also incorporated in US statutory law and thereby capture the required level of fundamental right protection applicable in the EU.

The ECJ made massive and indiscriminate surveillance by US authorities the key element of its Safe Harbour analysis and decision in the *Schrems* case. Unfortunately, Privacy Shield still fails to provide judicial remedies against interferences by intelligence agencies and more so no constitutional guarantees for EU data subjects and their data.[115] Statutory provisions reflecting Constitutional guarantees falls short in practice, as the Snowden Revelations in 2013 so vividly demonstrated[116]. One cannot help but wonder, how the ECJ's will rule on Privacy Shield, taking into account that cases are currently pending.[117] Judging by its reasoning in the *Schrems* case,

---

[110] 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, at 45.
[111] Ibid., at 47.
[112] Ibid., at 48.
[113] Ibid., at 52 ff.
[114] Similar Neil M Richards, Report of Professor Neil Richards in Data Protection Commissioner v. Facebook ('Schrems 2'), Irish High Court 2017., Washington University in St. Louis Legal Studies Research Paper (February 2018), page 2.
[115] See also Irena Nesterova, Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards, European Society of International Law (ESIL) 2016 Annual Conference (Riga) (January 2017), page 14.
[116] Owen Bowcott, Mass surveillance exposed by Snowden 'not justified by fight against terrorism', The Guardian (December 2014), accessible under https://www.theguardian.com/world/2014/dec/08/mass-surveillance-exposed-edward-snowden-not-justified-by-fight-against-terrorism (last checked 08.03.2018).
[117] Case T-670/16, Digital Rights Ireland v Commission, filed 16.09. 2016; and Case T-738/16, La Quadrature du Net and Others v Commission, filed 09.12.2016. [2015], at 73.

the level of protection in the US under Privacy Shield still does not seem to be *essentially equivalent* to the protection level in the EU.[118]

2. Adequate Safeguards according to Article 26 (2) DPD

The ECJ did not address *adequate safeguards* in the *Schrems* case, and consequently the WP29 issued a Statement declaring "Standard Contractual Clauses and Binding Corporate Rules can still be used"[119]. This was before Maximilian Schrems was able to alternate his original complaint before the Irish DPA, challenging Safe Harbour, into a challenge of the validity of Standard Contractual Clauses for EU-US data transfers according to Article 26 (2) DPD.[120] The Irish DPA, in May 2016, commenced legal proceedings before the Irish High Court and asked the Court to refer the matter to the ECJ for preliminary hearing, which the Court did on 3rd October 2017.[121]

In the *Schrems case* the ECJ put great emphasis on the protection of transferred data against interference by public authorities, especially on a generalized basis and without effective recourse mechanisms for the affected data subject. By nature, *adequate safeguards* are based on contractual relationships between private parties, to which public authorities are not a party. Such a contractual obligation cannot restrain intelligence or LEAs activities in third countries.[122] Legislation in the respective third country might easily even override them, due to their contractual nature. Adequate Safeguards thereby cannot provide sufficient protection against interference by US authorities.

3. Derogations according to Article 26 (1) DPD

Derogations according to Article 26 (1) DPD are only applicable where neither an adequacy decision nor adequate safeguards are in place. Their purpose is to fill the gap void and enable data transfers to third countries on a case-by-case basis. Derogations such as consent (Article 26 (1) (a) DPD) "to the proposed transfer" or "the transfer is necessary in order to protect the vital interests of the data subject" (Article 26 (1) (e) DPD) are not aimed at providing adequate

---

[118] Similar: David Meyer (German DPA): "If the agreement will meet the high level of the requirements the [CJEU] postulated in the Schrems ruling is rather doubtful." quoted by Gregory W. Voss, The Future of Transatlantic Data Flows: Privacy Shield or Bust? (May 1, 2016). Journal of Internet Law Vol. 19 No. 11 pp. 1, 9-18, May 2016, page 16; Opposing: Nadine Geppert, Could the 'EU-US Privacy Shield' Despite the Serious Concerns Raised by European Institutions Act as a Role Model for Transborder Data Transfers to Third Countries? (31.08.2016).

[119] Article 29 Working Party, Statement of the Article 29 Working Party, 16 October 2015.

[120] Mary Carolan, High Court reserves judgment in Facebook case, Irish Times, 15.03.2017, accessible under https://www.irishtimes.com/business/economy/high-court-reserves-judgment-in-facebook-case-1.3011853 (checked 08.09.2017).

[121] Irish High Court, Data Protection Commissioner v Facebook Ireland 2016/4809, filed 31.05.2016; Mary Carolan & Elaine Edwards, High Court asks ECJ to examine Facebook case, The Irish Times (October 2017), accessible under https://www.irishtimes.com/business/technology/high-court-asks-ecj-to-examine-facebook-case-1.3242468 (last checked: 09.03.2017).

[122] Christopher Kuner, Reality and Illusion in EU Data Transfer Regulation Post Schrems, German Law Journal Vol. 18 No. 04, 2017, page 908 f.

protection, but rather allow a very limited amount of third country transfers to take place because of special circumstances.

It is therefore not surprising that they are seen as the “weakest” legal bases with regard to the protection provided to the transferred data.[123] The *Schrems* case findings consequently also do not affect derogations according to Article 26 (1) DPD, since by definition derogations are not supposed to achieve an *essentially equivalent* to the protection level in the EU but rather provide a derogation from that requirement on a case-by-case basis.

Conclusion

To recall, the ECJ implicitly requires that the assessed legal bases establish a level of protection for transferred data to the US that is *essentially equivalent* to the protection of personal data guaranteed within the European Union.[124] The aforementioned assessment especially focuses on whether these former legal bases can mitigate or provide sufficient legal remedies for the data subject against interference by foreign authorities to personal data originating from the EU.[125]

As shown, none of the legal bases provided in the DPD, including Privacy Shield, can provide protection that is *essentially equivalent* to the protection level in the EU, since potential interferences by foreign authorities to personal data originating from the EU can neither be prevented nor mitigated by sufficient legal remedies. Therefore, the third sub-research question, asking to what extent the *Schrems* case affects the reliability of the former framework for third country transfers under the Data Protection Directive, can be answered as follows: The *Schrems* case affected the framework to the extent, that the former framework did not provide a reliable legal basis for third country transfers until its replacement by the GDPR. An exception might have been transfers based on *derogations* (Article 26 (1) DPD), since by definition such transfers are not dependent on the level of protection provided but aim to provide a “derogation” from the rule on a case-by-case basis.

[123] Christopher Kuner, Reality and Illusion in EU Data Transfer Regulation Post Schrems, German Law Journal Vol. 18 No. 04, 2017, page 908.
[124] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 73.
[125] Ibid., at 89.

Chapter 4: The current Legal Framework for third country transfers (GDPR) in light of the *Schrems* case

Introduction

The previous Chapters dealt with third country transfers under the former applicable EU data protection framework enshrined in Art. 25 f. Data Protection Directive. Chapter 3 pictured the *Schrems* case's relevance for adequacy decisions but also for the system of third country transfers under the current framework in general.

As of 25th May 2018, the Data Protection Directive was replaced by the General Data Protection Regulation (GDPR), which was initially proposed on 25 January 2012 and after long and intense discussions adopted in 27th April 2016.[126] This chapter aims to analyze the current framework for third country transfers under the GDPR and incidentally assess to which extent this new framework for third country transfers can establish a level of protection that is *essentially equivalent* to the protection of personal data guaranteed within the European Union.[127] To recall, the ECJ in the *Schrems* case especially criticized the fact that the legislation in the US authorizes a generalized storage of personal data that has been transferred from the EU to the US, as well as access to such stored data by the public authorities.[128] In order for the new framework to provide enough reliability for data transferring companies, it is therefore essential, that the framework can mitigate or provide sufficient legal remedies for the data subject against interference by US authorities to personal data originating from the EU.[129] The following assessment therefore will pay special attention to the key elements determined in Chapter 2 of the ECJ's Safe Harbour analysis.

Article 44 GDPR determines that third country transfers shall only take place if the conditions laid out in Chapter 5 - "Transfers of personal data to third countries or international organizations"- are met. Similar to the DPD[130], three legal grounds for such transfers of personal data are regulated by the GDPR: Adequacy Decision (Article 45 GDPR), Appropriate Safeguards[131] (Article 46 f. GDPR) and Derogations (Article 49 GDPR).

Before taking a more detailed look at these three legal bases, it can be pointed out in advance, that the EU legislator already acknowledged the Schrems Case to some extent, by incorporating

---

[126] For a brief summary of the new requirements brought the GDPR: Gregory W. Voss, European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting (January 5, 2017), Business Lawyer, Vol. 72, No. 1, pp. 221-233, Winter 2016/2017 (January 2017), page 221.
[127] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 73.
[128] Also acknowledged by the European Commission, see Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 90 and 93.
[129] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 89.
[130] Adequacy decisions by the European Commission (Article 25 DPD), adequate safeguards (Article 26 (2) DPD), and derogations (Article 26 (1) DPD).
[131] Article 26 (2) DPD refers to them as "Adequate Safeguards".

the definition of what constitutes "adequacy" into Recital 104 and Article 45 (2) GDPR. To recall the ECJ in Schrems Case defined an *adequate level of protectio*n as protection that is of *essential equivalence with EU law* in light of the Charter and EU primary as well as secondary law, especially the Data Protection Directive. Kuner[132] rightfully points out, the GDPR is "much more complex and provides rules in a number of areas not covered by Privacy Shield", such as the use of data protection impact assessments (Article 35 GDPR), data portability (Article 20 GDPR) and data protection by design and default (Article 25 GDPR). He subsequently suggests that Privacy Shield in light of the ECJ's definition of "adequacy" will need to be revaluated once the GDPR in May 2018 comes into force.[133] This is in line with recital 146 of the EU Commissions Implementing Decision (EU) 2016/1250 (Privacy Shield) stating that "the Commission will assess the level of protection provided by the Privacy Shield following the entry into application of the GDPR." The Commission accordingly conducted annual reviews of Privacy Shield. The latest and second review conducted in October 2018, summarized by the Commission December 2019 report, determined inter alia that the certification process for Privacy Shield as well as proactive oversight have been improved but also pointed out that the essential position of the Ombudsperson (see also 3.1 above) should be permanently filled. Thus far the US has left only appointed an acting Ombudsperson. The Commission set a deadline, that the position shall be permanently filled by 28th February 2019. Until now, the White House only announced its intention to soon nominate a permanent Ombudsperson.[134]

1. Adequacy Decision according to Article 45 GDPR

Similarly, to Article 25 (6) DPD, according to Article 45 (3) GDPR the EU Commission is again entitled to issue an adequacy decision, thereby allowing for data transfers from the EU to the respective country without any authorization requirements by the national or European DPAs (see Article 45 (1) GDPR).

The Commission adopts adequacy decisions by means of an implementing act (see Article 45 (3) GDPR). Contrary to so-called delegated acts, an implementing act can be adopted without the Parliament's direct involvement, which will speed up the process.[135] As already pointed out in Chapter 1, the European Commission is thus again afforded a predominant role in the evaluation of third countries' data protection level.

Article 45 (3) GDPR furthermore determines, that the EU Commission has to review its adequacy decisions every four years, and in case the level of protection in the respective country does not equal the EU protection level, shall repeal or suspend the respective decision (Article 45 (5)

---

[132] Christopher Kuner, Reality and Illusion in EU Data Transfer Regulation Post Schrems, German Law Journal Vol. 18 No. 04, 2017, page 902 ff.
[133] Ibid.
[134] Rebecca Hill, Looks like Uncle Sam has pulled its finger out and appointed a Privacy Shield ombudsperson, The Register, January 2019, accessible under https://www.theregister.co.uk/2019/01/22/privacy_shield_ombudsperson/ (last checked 15.02.2019).
[135] Paul Craig and Gráinne de Búrca, EU Law – Text, Cases, and Materials, 2011, p. 118.

GDPR). This is notable since periodic review of adequacy decisions by the EU Commission was also explicitly pointed out by the ECJ in its Safe Harbour Judgement.[136]

Finally, the EU Commission according to Article 45 (2) GDPR shall consider the following key points when determining the level of protection in a third country[137]:

- "[T]he rule of law, respect for human rights and fundamental freedoms"[138];
- Relevant legislation, case law and practice especially "concerning public security, defence, national security and criminal law and the access of public authorities to personal data"[139];
- […] "effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred"[140];
- the existence and effective functioning of an independent supervisory authority in the third country, including adequate enforcement powers;[141] as well as
- "the international commitments the third country or international organization concerned has entered into"[142].

As previously noted, the ECJ made massive and indiscriminate surveillance by public authorities the key element of its Safe Harbour analysis and decision in the *Schrems* case. Although, the new regulation of Adequacy Decisions in Article 45 GDPR seems to almost mirror the Court's requirements, a considerable amount of uncertainty remains. This is due to the fact that the ECJ in the *Schrems* case also considers the foreign legal system as independent factor from the vehicle used for the data transfer or its EU regulation. This effect is magnified by the ECJ's understanding of adequacy accounting to *essential equivalence* with EU law. The GDPR with its provisions concerning Privacy by Default entails still not fully developed data protection concepts that open the door for regulation by technology/code and thereby might increase the level of data protection from one day to another. One might consider for instance that an advanced algorithm with near artificial intelligence is developed in the future and hard wired to record any access to personal data by public authorities within the EU as well as only permits such access if a validation by a court or other judicial authority is provided. This fictional algorithm illustrates the idea behind privacy by design or default. If such a software would be made mandatory for all law enforcement and intelligence services within the EU but the US would reject its application, the shift in the level of data protection would be paradigm and thus immediately question any adequacy decision by the European Commission.

[136] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 76.
[137] Note: The key points reflect exactly the requirements determined by the ECJ in the Schrems Case (see also Chapter 2 and 3).
[138] Article 45 (2) (a) GDPR.
[139] Article 45 (2) (a) GDPR.
[140] Ibid.
[141] Article 45 (2) (b) GDPR.
[142] Article 45 (2) (c) GDPR.

The new framework for adequacy decisions according to Article 45 (2) GDPR is a step forward from the old framework under Article 25 DPD. With regard to its reliability for US companies to transfer personal data based on such adequacy decisions as Privacy Shield, it needs to be seen how the successor to Privacy Shield based on Article 45 (2) GDPR will be designed. Judging from purely from the provision itself, it seems possible that a new adequacy decision based on Article 45 (2) GDPR will provide reliability for US companies compared to the DPD framework.

2. Appropriate Safeguards according to Article 46 f. GDPR

Appropriate Safeguards, which are called Adequate Safeguards under Art. 26 (2) DPD, can also under the GDPR be used as a legal basis to transfer data to a third country. Contrary to rules applicable under the DPD, Article 46 (2) GDPR lists under (a) to (f) six vehicles that by default provide for appropriate safety and allow third country transfers without the need for specific authorization by a national DPA:

(a) "a legally binding and enforceable instrument between public authorities or bodies;"[143]
(b) "binding corporate rules […]"[144];
(c) "standard data protection clauses adopted by the Commission"[145];
(d) "standard data protection clauses adopted by a supervisory authority and approved by the Commission"[146];
(e) "an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply appropriate safeguards, including data subjects' rights; or"[147]
(f) "an approved certification mechanism […] together with binding and enforceable commitments of the controller or processor in the third country to apply appropriate safeguards, including data subjects' rights."[148]

The adoption of codes of conduct (Article 40 GDPR) as well as certification methods (Article 42 GDPR) is new. [149] These methods, even outside their applicability for third country transfers, are still not much assessed. It remains to be seen how these two vehicles will be applied in practice, when the GDPR comes into force. In light of the *Schrems* case, it seems difficult to imagine how a code of conduct or a certification method will prevent US authorities from accessing personal data transferred from the EU to the US. Not per se new are standard clauses by national DPAs.

[143] Article 46 (2) GDPR.
[144] Ibid.
[145] Ibid.
[146] Ibid.
[147] Ibid.
[148] Ibid.
[149] Rita Heimes, Top 10 operational impacts of the GDPR Part 9 Codes of Conduct and Certification, IAPP website/blog, 24th February 2016, accessible under https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-9-codes-of-conduct-and-certifications (checked: 14.09.2017).

Although the Data Protection Directive keeps silent about this matter, such clauses are already common practice.[150]

The GDPR gives special attention to Binding Corporate Rules (BCRs), in that besides Article 46 Article 47 GDPR deals explicitly with BCRs. That is a notable change, since in the Data Protection Directive BCRs were not even mentioned and it shows their importance in practice, especially post *Schrems*. Article 47 (1) GDPR lays down three cumulative fundamental requirements for BCRs:

(a) legally binding and applied to and are enforced by every member of the company;
(b) enforceable third party rights for the data subject
(c) fulfill requirements of Article 47 (2) GDPR.

Article 47 (2) GDPR than in detail determines the specific issues that the BCRs need to address. For instance, the structure and contact details of the company, categories of data and type of processing, the purpose of processing, the BCRs legally binding nature, application of general data protection principles, access rights for the data subject, liability commitments, information requirements, complaint procedure, audit mechanisms, cooperation mechanism with national DPAs and training for employees to raise awareness.

What can be said at this early stage is that codes of conduct bear similarities to contractual agreements as well as BCRs. As discussed in Chapter 3, contractual obligations and BCRs as vehicles for third country transfers post *Schrems* will only be reliable in so far as (and thereby provide certainty to companies) the US provides a similar level of protection to EU data subjects to the one provided in the EU.[151] Overall the legal basis of Appropriate Safeguards seems to be a significant improvement compared to the DPD and pays respect to the ECJ's requirements in the *Schrems* case, but does not provide for more reliability compared to the DPD framework.

3. Derogations according to Article 49 GDPR

As a third legal basis, the GDPR in Article 49 provides for derogations from the general prohibition of transfers of personal data to third countries. Derogations therefore are not supposed to achieve an *essentially equivalent* to the protection level in the EU but rather provide an exemption from that requirement on a case-by-case basis. [152] Article 49 GDPR explicitly clarifies that a third country transfer based on derogations is only permitted "if the transfer is not repetitive, [and] concerns only a limited number of data subjects".

[150] European Commission, Analysis and impact study on the implementation of Directive EC 95/46 in Member States, 2003, p. 32, accessible under http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf (checked: 18.09.2017).
[151] In essence similar, Sydow, Europäische Datenschutzgrundverordnung, second edition 2018, Article 46 at 9; also Ambrock NZA 2015, 1493, 1495; more optimistic Wybitul, Ströber and Reuß, ZD 2017, 503, 506.
[152] Similar, Article 29 Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, WP 114, 25 November 2005, page 7.

The stipulated grounds are almost identical to the grounds under the Data Protection Directive except for a few minor changes and clarifications. For instance the data subject now, if a transfer is based on consent, needs to give its consent explicitly and must furthermore be informed about the risks of the absence of an adequacy decision and appropriate safeguards.[153] This is very interesting in light of the *Schrems* case, as it clarifies that informed consent must essentially also highlight potential risks in the respective third country such as access to transferred data by law enforcement authorities or intelligence agencies on a generalized basis. Whether this proposed, perhaps rather radical line of interpretation will also be followed in practice remains to be seen. With regard to vital interests of the data subject, as another derogation ground, Article 49 (1) (f) GDPR clarifies that not only the data subject's interests but also the interest of another person, "where the data subject is physically or legally incapable of giving consent" can be considered. Article 49 (4) GDPR in line with WP29[154], now confirms that a transfer based on a public interest is only valid, if the respective public interest is "recognised in Union law or in the law of the Member State to which the controller is subject"[155], a point that was left open for discussion under the DPD framework.[156]

Last but not least any transfer based on Article 49 GDPR must be reported to the national DPA and requires the exporter to inform the data subject of the transfer and on the compelling legitimate interest pursued. Article 49 paragraph 6 GDPR requires the exporter to document then the transfer for potential audits by the DPA.

The GDPR clarifies and provides additional safeguards with regard to derogations. With regard to a reliable legal basis for transfers of personal data from the EU to the US, it should be reminded that derogations can only be used "if the transfer is not repetitive, [and] concerns only a limited number of data subjects"[157], which in consequence will not help companies such as Google and Amazon to legitimately transfer personal data between the EU and the US.

Conclusion

In conclusion, the GDPR is compatible with the Schrems Case and incorporates most of the ECJ's requirements into the legal framework. Unfortunately, what was determined in Chapter 3 for the Data Protection Directive, to a large extent also holds true for the framework under the GDPR, in that the assessed legal bases provided in the GDPR, cannot provide protection that is *essentially equivalent* to the protection level in the EU, since potential interferences by foreign authorities to personal data originating from the EU can neither be prevented nor mitigated by sufficient

[153] See Article 49 (1) (a) GDPR.
[154] Article 29 Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, WP 114, 25 November 2005, page 15.
[155] Article 49 (4) GDPR.
[156] Article 29 Working Party, Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, WP 114, 25 November 2005, page 15.
[157] Article 49 (1) GDPR.

legal remedies. Something else might hold true if the EU Commission decides to revise Privacy Shield based on the requirements laid out in Article 45 GDPR. Unfortunately, as of today, none of the aforementioned provisions establish a reliable legal basis for US companies to transfer personal data from the EU to the US.[158]

[158] Similar, Sydow, Europäische Datenschutzgrundverordnung, second edition 2018, Article 46 at 9; also Ambrock NZA 2015, 1493, 1495.

Chapter 5: Alternative Solutions

Introduction

The previous Chapters laid out the former and current EU framework for the transfer of personal data to a third country, as well as explain and analyze the extent to which the frameworks provide reliability in light of the ECJ's *Schrems* case. As a consequence of the *Schrems* case, almost all available legal bases for a transfer to a third country under the DPD and GDPR, *adequacy decisions* by the European Commission (Article 25/Article 45), *adequate/appropriate safeguards* (Article 26 (2)/Article46 f.), but not *derogations* (Article 26 (1)/Article49), need to be assessed with regard to the level of protection provided for the EU data subject in the third country. According to the ECJ, this level must be *essentially equivalent* to the protection level in the EU, provided by the Charter, primary and secondary EU law (DPD and GDPR).

As shown, as of today, none of the provided legal bases can guarantee such a level of protection in the US. Nonetheless, it can be argued that the framework has improved under the GDPR. In light of the aforementioned, this Chapter aims to propose and examine some alternative solutions in regards to the GDPR framework for third country transfers. It would be naïve to suggest a reconsideration of the level of protection required in or outside the EU, since this would require either the EU or the US to either lower or raise its historically developed protection of privacy and data protection on fundamental rights level. The following therefore concentrates rather on technical solutions to the problem.

1. Modification of the transferred data as such

A first alternative might be found, when the data to be transferred is looked at in detail. Anonymization and encryption are not new terms to the data protection field and might actually add value to the protection against access by public authorities in a third country. Personal data becomes anonymized data, "if all identifying elements have been eliminated from a set of personal data"[159]. This definition might become clearer, when looking into the definition of personal data. Personal data means "any information relating to an identified or identifiable natural person"[160]. Accordingly, all personal data becomes anonymized, when no element is left in the information that could re-identify the person concerned.[161] The moment personal data is anonymized, it is by definition not personal data anymore and thereby excluded from the scope of the Data Protection Directive, GDPR as well as Article 8 Charter.

Understandably, data in anonymized form can be transferred without any need for the aforementioned legal basis. On the downside, companies that especially find added value in personal data will not profit from this solution. Encrypted data, on the other hand, is still considered personal data and thus does not fall outside the scope of protection but might provide

---

[159] Handbook on European data protection law, 2014, page 44.
[160] Article 2 (a) Data Protection Directive.
[161] Recital 26 Data Protection Directive.

efficient protection against access to the data by public authorities. Encryption in its purest form means nothing else than the process of encoding information in such a manner that only the person with the description key, for instance a password, can access it. Encrypted data, when accessed without a description key, reveals nothing but scrambled information – often called *ciphertext*.[162] Kuner, therefore argued, that encryption would solve the issues of data transfers to third countries.[163]

In February 2016 the FBI compelled Google through several court orders to assist the authority in accessing data on a locked iPhone belonging to one of the shooters of the San Bernardino terrorist attack from 2015.[164] The data on the phone was encrypted and therefore not accessible to the FBI. Apple opposed the order and the FBI ultimately found another way to unlock the respective phone[165] but the dispute shows how encryption can mitigate the risk of generalized access by public authorities to personal data. On the downside, one might argue that certain countries might establish obligations for companies to cooperate in the decryption process or even build a backdoor into the encryption to allow public authorities to access the data. The evaluation of the required level of protection would ultimately again come down to an assessment of the legislation and practices in the respective country and thereby encryption would not necessarily provide for a reliable safeguard to transfer personal data from the EU to the US.

2. Modification of the place of data storage

A second alternative might be revealed when looking into the place where personal data is stored. Data in the Internet environment is usually stored on a server in a server-center, which is located for instance in Ireland, the US, Germany or another country of the world. A possible storage place which would restrict the access of US authorities to personal data would be storage within the EU.

If companies, instead of transferring the data to a third country, would keep the data on a server center based within the EU, a third country data transfer and thereby the aforementioned problems would not occur since there would be no transfer to begin with. This solution is discussed under the term *data localization* and has recently gained momentum, as countries such as Russia, China and to some extent Canada and Australia introduced laws requiring the storage

[162] C. Metz, Forgetxs Apple vs. The FBI: WhatsApp Just Switched On Encryption For A Billon People, Wired (2016), https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/ .
[163] Christopher Kuner, Transborder Data Flow Regulation and Data Privacy Law (1st Edition, Oxford University Press, 2013), p. 97.
[164] For a complete overview of the case see, Apple vs. the FBI: all the news on the battle for encryption's future, at the Verge, accessible under https://www.theverge.com/2016/2/17/11036306/apple-fbi-iphone-encryption-backdoor-tim-cook (checked: 15.09.2017).
[165] Danny Yadron, San Bernardino iPhone: US ends Apple case after accessing data without assistance, the Guardian, 29 March 2016, accessible under https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone (checked: 15.09.2017).

of personal data within their respective countries.[166] In reaction to the *Schrems* case some US providers have even publicly announced to store their data in the EU.[167]

The biggest advantage of data localization in the EU would be that foreign authorities can physically not access EU data subject's data anymore, by for instance seizing the server upon which the data is stored. On the downside, even if service providers such as Google or Microsoft would store their data in the EU, they could be forced by US authorities, at the companies' headquarters, to provide access to the data through a connected terminal. In that case, the data would not be transferred *per se* but would be accessed remotely from the US.

Such investigatory measures by foreign authorities raise a difficult sovereignty questions. For instance, does a remotely conducted investigation by country A on the territory of country B, infringe the letter country's sovereignty? Any exercise of State power in the territory of another State, potentially interferes with the affected State's sovereignty and would thus require a permissive rule derived from international custom or convention in order to not conflict with international law.[168]

In order for data localization to really provide an alternative solution to data transfers, it must therefore be assured that although the data is kept in the EU, foreign public authorities cannot remotely access the data and thereby circumvent the ECJ's *Schrems* ruling with to third country data transfers. What needs to be assessed though is whether the sovereignty principle is actually restricting a State's investigations in practice or just in theory.

Lately, the aforementioned problem with regard to sovereignty has been subject to several litigations in the US and EU (Belgium).[169] The cases do not involve remote access by authorities to foreign stored data but data protection orders, an investigatory measure through which law

---

[166] Anupam Chander & Uyên P. Lê, Data Nationalism, Emory Law Journal, Volume 64, Issue 3, 2015, accessible under http://law.emory.edu/elj/content/volume-64/issue-3/articles/data-nationalism.html (checked:18.02.2018); Christopher Kuner, Reality and Illusion in EU Data Transfer Regulation Post Schrems, German Law Journal Vol. 18 No. 04, page 881-918, 2017, page 913.

[167] European Commission, Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America Under Directive 95/46/EC Following the Judgment by the Court of Justice in Case C-362/14 (Schrems), COM (2015) 566 final, page 12 footnote 40.

[168] See SS Lotus - France v. Turkey Case (1927), PCIJ Ser A No 10, 18 (emphasis added): "[T]he first and foremost restriction imposed by international law upon a state is that – failing the exercise of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or convention."

[169] Paul de Hert & Monika Kopcheva, International mutual legal assistance in criminal law made redundant: A comment on the Belgian Yahoo! case, Computer & Security Review 27 (2011) 291-297; Russell Brandom, You can't use US law to search foreign servers, appeals court confirms, 24.01.2017, the Verge, accessible under https://www.theverge.com/2017/1/24/14370962/microsoft-warrant-case-ireland-server-search-stored-communications (checked: 18.02.2018); Alexander J. Martin, Belgian court fines Skype for failing to intercept criminals' calls in 2012, the Register, (2016), https://www.theregister.co.uk/2016/10/27/belgian_court_fines_skype_intercept_criminals_calls/ (last checked 18.02.2018).

enforcement authorities compel a service provider to produce the sought-after data. The question in regards to sovereignty stays the same since the only difference between remote access and a production order is that in the former the authorities themselves access the data whereas in the latter a private entity is forced to access it for the authorities. Considering that the private entities do not access the data voluntarily but are forced by the State, their actions ultimately also amount to an act of the State.

In the aforementioned context, the Microsoft Ireland Case is particularly interesting.[170] The case began in December 2013, when a magistrate judge at District Court for the Southern District of New York granted a warrant for search and seizure of information belonging to an email account hosted by Microsoft. [171] The magistrate ordered the service provider to hand over a variety of data, including content, belonging to the aforementioned email account.[172] Microsoft produced all relevant subscriber information and non-content data, which were hosted on servers based in the US, but tried to vacate the warrant concerning the disclosure of content data which was hosted on a server abroad in Ireland. The service provider argued that a US judge had no authority to issue a warrant for data stored abroad and must rather seek mutual legal assistance from Ireland.[173] Subsequently, the magistrate disagreed with Microsoft and rejected Microsoft's motion to vacate in April 2014.[174] The judge pointed out that the search does not involve the presence of US investigators abroad.[175] Microsoft unsuccessfully appealed to the District Court for the Southern District of New York and argued that the seizure of the content data in form of emails actually takes place abroad.[176] The US attorney's office, in line the district court judge, countered that the warrant only requires Microsoft to disclose data under its control regardless of where the data is stored.[177]

The case ultimately went on to the Court of Appeals for the Second Circuit.[178] The Second Circuit decided that a warrant is not enforceable when a service provider, such as Microsoft, stores the data outside US territory.[179] It argued that the respective provisions do not explicitly permit the issuing of a warrant with extraterritorial reach and therefore can only be used to issue domestic

[170] See brief summary and relevant case documents, see the website of the Electronic Frontier Foundation (EFF) under https://www.eff.org/cases/re-warrant-microsoft-email-stored-dublin-ireland (last checked 18.02.2018).
[171] Ibid.
[172] Ibid.
[173] In the matter of a warrant to search a certain e-mail account controlled and maintained by Microsoft Corporation, US District Court Southern District of New York, 13 Mag. 2814, 25.04.2015, page 1, accessible under https://www.eff.org/document/magistrates-opinion-denying-microsofts-motion-quash (last checked 18.02.2018).
[174] Ibid.
[175] Ibid., page 21.
[176] Microsoft's objections to the Magistrate's Order denying Microsoft's motion to vacate in part a search warrant seeking customer information located outside the United States, 13 Mag 2814, 06.06.2014, page 2 ff. and 7 ff. accessible under https://www.eff.org/document/microsofts-objection-magistrates-opinion (last checked 18.02.2018).
[177] Government's Brief in support of the Magistrate Judge's Decision to uphold a warrant ordering Microsoft to disclose records within its custody and control, 13 Mag 2814, 09.07.2014, page 4 ff., accessible under https://www.eff.org/document/governments-brief-support-magistrates-decision (last checked 18.02.2018).
[178] U.S. Court of Appeals for the Second Circuit, Microsoft v. United States, No. 14-2985 (2d Cir. 2016), 14.07.2016.
[179] Ibid., page 6 f.

warrants.[180] Notably the judges pointed out that it is “difficult to dismiss” the interests of the foreign State of Ireland to regulate the behaviour of service providers within its State borders “on the theory that the foreign sovereign’s interests are unaffected when a United States judge issues an order requiring a service provider to “collect” from servers located overseas and “import” into the United States data, possibly belonging to a foreign citizen, simply because the service provider has a base of operations within the United States”.[181]

In his concurring opinion, Judge Gerard E. Lynch additionally reasoned that “[we] live in a system of independent sovereign nations, in which other countries have their own ideas, sometimes at odds with ours and their own legitimate interests. The attempt to apply U.S. law to conduct occurring abroad can cause tensions with those other countries”.[182] Judge Lynch furthermore stated that “the Irish government and the European Union would have a considerable grievance if the United States sought to obtain the emails of an Irish national, stored in Ireland, from an American company which had marketed its services to Irish customers in Ireland”. [183]

The US Department of Justice (DOJ) petitioned for rehearing en banc, which was denied by the Second Circuit on the 24th January 2017.[184] In its last attempt to challenge the decision, the DOJ in June 2017 has formally asked the Supreme Court to hear its appeal in the case, which was granted by the Court October 2017.[185] While the case was pending[186] before the Court, the US Congress passed in March 2018 the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which now grants US law enforcement authorities the power to request data from US based service providers, even if such data is stored on servers abroad as long as such data is in “possession, custody, or control” of a US company (§2713 - 18 U.S. Code Chapter 121). For the present discussion on data localization, at least from the US perspective, it must be determined, that stored data in the EU seems not to be protected from access by public authorities.

A related point will also be, whether data localization can be afforded by smaller companies offering their service in the EU market and whether this would constitute a market entry barrier for smaller companies and thus interfere with competition law or WTO law. Although storage in the EU ultimately results in no transfers to the US and thereby provides strong reliability and certainty, it is more than questionable if such a solution would fit the business model of companies such as Google, Amazon, Yahoo, Skype and Microsoft as well as would even be possible in light of competition or WTO law.

---

[180] U.S. Court of Appeals for the Second Circuit, Microsoft v. United States, No. 14-2985 (2d Cir. 2016), 14.07.2016., page 39 ff.

[181] Ibid., page 42.

[182] Ibid., (Lynch, G.E., concurring), page 7.

[183] Ibid., (Lynch, G.E., concurring), page 15.

[184] U.S. Court of Appeals for the Second Circuit, Microsoft v. United States, No. 14-2985 (2d Cir. 2016), (rehearing en banc denied), 24.01.2017.

[185] Amy Howe, Court adds four new cases to merits docket, SCOTUS blog (October 2017), accessible under http://www.scotusblog.com/2017/10/court-adds-four-new-cases-merits-docket/ (last checked: 09.03.2018).

[186] Pete Williams, Supreme Court seems set to rule against Microsoft in email privacy case, NBC News (February 2018), accessible under https://www.nbcnews.com/politics/supreme-court/gov-t-battles-microsoft-email-privacy-case-supreme-court-n851216 (last checked: 09.03.2018).

Conclusion

Neither the technical modification of the data transferred nor the modification of the place of storage can provide valuable alternatives to the GDPR framework for third country transfers. A modification of the place of storage will bring no added value to companies whose business model explicitly requires the data to be physically available in the US, since data localization would require the data to remain in the EU and also be only accessed and processed by the respective company in the EU. Ultimately US companies would have to set up headquarters in the EU in order to use the respective data. And finally, due to the introduction of the CLOUD Act, US authorities can still access data that is even stored in Europe, as long as these data is in possession, custody or control of a US company.

A technical modification of the data transferred, especially via encryption, could constitute a valuable alternative, as long as US legislation does not force companies to hand over the encryption key. Ultimately the evaluation of the required level of protection according to the Schrems Case would again come down to an assessment of the legislation and practices in the US.

Conclusion

The purpose of this thesis was to take a closer look at the transfer of personal data between the EU and the US inspired by the *Schrems* case the ECJ decided in 2015. As already pointed out, the last time the ECJ had addressed the data flow to a third country, such as the US, was its *Bodil Lindqvist*[187] ruling dating back to 2003. Back then services that dominate our daily life such as Google Search, Facebook or Amazon either did not exist or were still in their infant shoes.

Working from the hypothesis that the *Schrems* case has repercussions - beyond Safe Harbour- for the framework of third country transfers itself, I asked the question: *to what extent reliable solutions exist to transfer personal data within the law from the EU to the US after the ECJ Schrems case?* In order to answer this overarching question, I have formulated several sub-questions which were answered respectively in five separate chapters.

To establish a fundament against which the impact of the *Schrems* case can be measured Chapter 1 assessed the question: *to what extent can personal data be transferred between the EU and the US under the former European Data Protection framework?* The assessment focused on secondary European law namely the Data Protection Directive and its three legal bases for third country transfers: *adequacy decisions* by the European Commission (Article 25), *adequate safeguards* (Article 26 (2), and *derogations* (Article 26 (1)). I concluded that only *adequacy decisions* by the European Commission (Article 25) allowed for a comprehensive and unrestricted transfer of personal data between the EU and the US, followed by standard contractual clauses based on *adequate safeguards* (Article 26 (2), which allowed for unrestricted transfer within a contractually bound and limited scope. BCRs and contractual clauses (not standardized) require approval by the Data Protection Authorities which makes their actual use rather cumbersome. Finally, a transfer based on *derogations* (Article 26 (1) DPD) was limiteded by the number of data subjects affected by the transfer and can also not be conducted receptive, which was not be of much use for companies that transfer large numbers of personal data, from a variety of data subjects on a daily basis to the US.

As a logical next step, I needed to determine and assess how the *Schrems* case is relevant for the Data Protection framework in regards to third country transfers in itself. Chapter 2 therefore analyzed the *Schrems* case and especially filtered out the ECJ's requirements that need to be considered when data is transferred to the US. The ECJ determined that the level of protection for transferred personal data in the US must be of *essential equivalence* with the protection level in the EU law. Thereby the Court acknowledged that besides the actual legal basis permitting the third country transfer, the level of protection for the transferred personal data in the respective country, based on its legal system and practices, must also be taken into consideration, when assessing a transfer of personal data to a third country. In order for companies to estimate the legitimacy of any third country transfer, it is therefore essential to assess whether the respective legal bases, namely *adequacy decisions* by the European Commission, *adequate safeguards* and

[187] Case C-101/01 *Bodil Lindqvist* [2003].

derogations, can themselves establish a level of protection that is *essentially equivalent* to the protection of personal data guaranteed within the European Union.[188] This would be the case, according to the ECJ, if the respective legal basis can mitigate or provide sufficient legal remedies for the data subject against interference by US authorities to personal data originating from the EU.[189]

Chapter 3 went on to assess *the extent to which the Schrems Case affects the reliability of the framework for third country transfers under the Data Protection Directive*. I concluded that since none of the legal bases provided in the DPD, including Privacy Shield, could not provide protection that is *essentially equivalent* to the protection level in the EU, the former framework for third country transfers under the DPD did not possess a reliable legal ground to the transfer of personal data to the US, without risking repercussions by the national Data Protection Authorities.

Chapter 4 extended the assessment conducted in Chapter 3 to General Data Protection Regulation (GDPR) which replaced the DPD framework as of May 2018. I argued that the new framework considered the requirements laid out in the *Schrems* case but that potential interferences by foreign authorities to personal data originating from the EU can still neither be prevented nor mitigated by sufficient legal remedies, except if the EU Commission decides to revise Privacy Shield according to the new provision for Adequacy Decision in Article 45 GDPR. Consequently, I also concluded that the new GDPR framework for transfers of personal data to third countries, does not yet possess a reliable legal ground to transfer personal data to the US.

To provide for a bigger picture of the problem, I addressed in Chapter 5 the question of whether valuable alternative solutions exist to the GDPR framework for third country transfers. I concluded that none of the discussed approaches, i.e. neither technical modification of the data transferred nor the modification of the place of storage can provide valuable alternatives to the GDPR framework for third country transfers.

The key question of this thesis was: *From a pure legal perspective, should companies continue to transfer personal data from the EU to the US after the ECJ Schrems case?* I conclude that currently no reliable legal ground or alternative option exists to transfer personal data from the EU to the US. A company that nonetheless transfers data to the US without a valid legal ground can be subjected to administrative fines up to 20 000 000 Euro or up to 4% of the total worldwide annual turnover.[190] I therefore finally conclude that companies, from a pure legal perspective, should not continue to transfer personal data from the EU to the US, and urge the European Commission to revise Privacy Shield in accordance with the requirements determined by the ECJ in the Schrems Case.

---

[188] Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], at 73.
[189] Ibid., at 89.
[190] Article 83 (5) (c) GDPR.

Bibliography

Legislation & Fundamental Rights Codifications

European Commission, Decision 2000/520/EC (Safe Harbor)

European Commission, Decision 2001/497/EC, Annex

European Commission, Decision 2002/2/EC

European Commission, Decision 2004/915/EC

European Commission, Decision 2010/87/EU

European Commission, Implementing Decision 2016/1250 (Privacy Shield)

Directive 95/46/EC (Data Protection Directive)

Regulation (EU) 2016/679 (General Data Protection Regulation)

Charter of Fundamental Rights of the European Union (EU Charter)

European Convention on Human Rights (ECHR) - EU

Cases & Opinions

Article 29 Working Party, First orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy, 26 June 1997

Article 29 Working Party, Model Checklist: Application for approval of Binding Corporate Rules, WP 102, 25 November 2004

Article 29 Working Party, Opinion 15/2011 on the definition of consent, WP187, 13 July 2011

Article 29 Working Party, Statement of the Article 29 Working Party, 16 October 2015
Article 29 Working Party, Working document 01/2014 on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor", WP 214, 21 March 2014

Article 29 Working Party, Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995, WP 114, 25 November 2005

Article 29 Working Party, Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules, WP 155, 07 Febuary 2017

Article 29 Working Party, Working document on transfers of personal data to third countries: applying Article 26 (2) of the EU Data Protection Directive to binding corporate rules for international data transfers, WP 74, 03 June 2003

Article 29 Working Party, Working Document Setting up a framework for the structure of Binding Corporate Rules, WP 154, 24 June 2008

Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 153, 24 June 2008

Case C-101/01 *Bodil Lindqvist* [2003]

Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015]

Case T-738/16 La Quadrature du Net and Others v Commission [2016]

Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data protection, 2002

European Commission, Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America Under Directive 95/46/EC Following the Judgment by the Court of Justice in Case C-362/14 (Schrems), COM (2015)

Government's Brief in support of the Magistrate Judge's Decision to uphold a warrant ordering Microsoft to disclose records within its custody and control, 13 Mag 2814, 09.07.2014, accessible under https://www.eff.org/document/governments-brief-support-magistrates-decision (last checked 18.09.2017).

In the matter of a warrant to search a certain e-mail account controlled and maintained by Microsoft Corporation, US District Court Southern District of New York, 13 Mag. 2814, 25.04.2015

Irish High Court, Data Protection Commissioner v Facebook Ireland 2016/4809

Microsoft’s objections to the Magistrate’s Order denying Microsoft’s motion to vacate in part a search warrant seeking customer information located outside the United States, 13 Mag 2814, 06.06.2014

Neil M Richards, Report of Professor Neil Richards in Data Protection Commissioner v. Facebook ('Schrems 2'), Irish High Court 2017., Washington University in St. Louis Legal Studies Research Paper (February 2018)

SS Lotus - France v. Turkey Case (1927), PCIJ Ser A No 10, 18

U.S. Court of Appeals for the Second Circuit, Microsoft v. United States, No. 14-2985 (2d Cir. 2016), 14.07.2016

Literature

Alexander J. Martin, Belgian court fines Skype for failing to intercept criminals' calls in 2012, the Register, (2016), https://www.theregister.co.uk/2016/10/27/belgian_court_fines_skype_intercept_criminals_calls/ (last checked 18.09.2017)

Amy Howe, Court adds four new cases to merits docket, SCOTUS blog (October 2017), accessible under http://www.scotusblog.com/2017/10/court-adds-four-new-cases-merits-docket/ (last checked: 09.03.2018)

Anupam Chander & Uyên P. Lê, Data Nationalism, Emory Law Journal, Volume 64, Issue 3, 2015, accessible under http://law.emory.edu/elj/content/volume-64/issue-3/articles/data-nationalism.html (checked:15.09.2017)

Ariel Teshuva, Why Has the EU Made So Few Adequacy Determinations?, Law Blog (January 2017), accessible under https://www.lawfareblog.com/why-has-eu-made-so-few-adequacy-determinations (last checked: 07.03.2018)

Boris P. Paal and Daniel A. Pauly, DS-GVO BDSG, 2nd edition 2018 (Commentary – German)

Christopher Kuner, Reality and Illusion in EU Data Transfer Regulation Post Schrems, German Law Journal Vol. 18 No. 04, page 881-918, 2017

Christopher Kuner, Transborder Data Flow Regulation and Data Privacy Law (1st Edition, Oxford University Press, 2013)

Danny Yadron, San Bernardino iPhone: US ends Apple case after accessing data without assistance, the Guardian, 29 March 2016, accessible under https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone (checked: 15.09.2017)

Electronic Frontier Foundation (EFF), In re Warrant for Microsoft Email Stored in Dublin, Ireland, website of the Electronic Frontier Foundation (EFF), accessible under https://www.eff.org/cases/re-warrant-microsoft-email-stored-dublin-ireland (last checked 18.09.2017)

Eugen Ehmann and Martin Selmayr, Datenschutz-Grundverordnung, second edition, 2018 (Commentary – German)

European Commission, Analysis and impact study on the implementation of Directive EC 95/46 in Member States, 2003, accessible under http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf (checked: 18.09.2017)

European Union Agency for Fundamental Rights, Handbook on European data protection law, 2014 (citied as Handbook on European data protection law)

Fanny Coudert, Schrems vs. Data Protection Commissioner: A Slap on the Wrist for the Commission and New Powers for Data Protection Authorities, Europen Law Blog (October 2015), accessible under http://europeanlawblog.eu/2015/10/15/schrems-vs-data-protection-commissioner-a-slap-on-the-wrist-for-the-commission-and-new-powers-for-data-protection-authorities/ (last checked: 07.03.2018)

Gernot Sydow, Europäische Datenschutzgrundverordnung, second edition, 2018 (Commentary – German)

Gregory W. Voss, European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting, Business Lawyer, Vol. 72, No. 1, pp. 221-233, Winter 2016/2017 (January 2017)

Gregory W. Voss, The Future of Transatlantic Data Flows: Privacy Shield or Bust? (May 1, 2016). Journal of Internet Law Vol. 19 No. 11 pp. 1, 9-18, May 2016

Irena Nesterova, Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards, European Society of International Law (ESIL) 2016 Annual Conference (Riga) (January 2017)

Jens Ambrock, Nach Safe Harbor: Schiffbruch des transatlantischen Datenverkehrs?, NZA 2015, 1493-1496.

Joris Toonders, Data Is the New Oil of the Digital Economy, Wired (July 2017), https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/ (last checked: 07.03.2018)

Jürgen Kühling and Benedikt Buchner, DS-GVO BDSG, second edition, 2018 (Commentary – German)

Mary Carolan & Elaine Edwards, High Court asks ECJ to examine Facebook case, The Irish Times (October 2017), accessible under https://www.irishtimes.com/business/technology/high-court-asks-ecj-to-examine-facebook-case-1.3242468 (last checked: 09.03.2017)

Mary Carolan, High Court reserves judgment in Facebook case, Irish Times, 15.03.2017, accessible under https://www.irishtimes.com/business/economy/high-court-reserves-judgment-in-facebook-case-1.3011853 (checked 08.09.2017)

Metz, Forgetxs Apple vs. The FBI: WhatsApp Just Switched On Encryption For A Billon People, Wired (2016), https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/

Nadine Geppert, Could the 'EU-US Privacy Shield' Despite the Serious Concerns Raised by European Institutions Act as a Role Model for Transborder Data Transfers to Third Countries? (31.08.2016)

Owen Bowcott, Mass surveillance exposed by Snowden 'not justified by fight against terrorism', The Guardian (December 2014), accessible under https://www.theguardian.com/world/2014/dec/08/mass-surveillance-exposed-edward-snowden-not-justified-by-fight-against-terrorism (last checked 08.03.2018)

Paul Craig and Gráinne de Búrca, EU Law – Text, Cases, and Materials, 5th Edition, 2011

Paul de Hert & Monika Kopcheva, International mutual legal assistance in criminal law made redundant: A comment on the Belgian Yahoo! case, Computer & Security Review 27 (2011) 291-297

Pete Williams, Supreme Court seems set to rule against Microsoft in email privacy case, NBC News (February 2018), accessible under https://www.nbcnews.com/politics/supreme-court/gov-t-battles-microsoft-email-privacy-case-supreme-court-n851216 (last checked: 09.03.2018)

Peter Swire, US Surveillance Law, Safe Harbor, and Reforms Since 2013, Georgia Tech Scheller College of Business Research Paper No. #36 (December 2015)

Gabe Maldoff and Omer Tene, 'Essential Equivalence' and European Adequacy after Schrems: The Canadian Example, Wisconsin International Law Journal, 2017, Vol. 32 Issue 2 (January 2017)

Rebecca Hill, Looks like Uncle Sam has pulled its finger out and appointed a Privacy Shield ombudsperson, The Register, (2019), https://www.theregister.co.uk/2019/01/22/privacy_shield_ombudsperson/ (last checked 15.02.2019).

Rita Heimes, Top 10 operational impacts of the GDPR Part 9 Codes of Conduct and Certification, IAPP website/blog, 24th February 2016, accessible under https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-9-codes-of-conduct-and-certifications (checked: 14.09.2017)

Russell Brandom, You can't use US law to search foreign servers, appeals court confirms, 24.01.2017, the Verge, accessible under https://www.theverge.com/2017/1/24/14370962/microsoft-warrant-case-ireland-server-search-stored-communications (checked: 18.09.2017)

Sergio Carrera & Elspeth Guild, Safe Harbour or into the storm? EU-US data transfers after the Schrems judgment, No. 85 CEPS Paper in Liberty and Security, page 1-5, 2015

Tim Wybitul, Lukas Ströber and Marian Reuß, Übermittlung personenbezogener Daten in Drittländer, ZD 2017, 503-509.

Tobias Bräutigam and Samuli Miettinen, 'Data Protection, Privacy and European Regulation in the Digital Age', Helsinki Legal Studies Research Paper 46 (December 2016)