UNIVERSITY
OF TWENTE.

Bachelor Thesis

An analysis of the EU data protection policy and the significance of the Maximillian Schrems case

July 2019

words:18190

Harpo Vogelsang (s1834371)

Faculty of Behavioural management and Social Science

Public Governance across Borders

First Supervisor: Dr. Claudio Matera

Second Supervisor: Prof. Dr. Ramses A. Wessel

Abstract

The transfer of personal data from EU citizens to third countries requires an adequate level of data protection. In 2013, the revelations by Edward Snowden about mass surveillance practices by US intelligence services attracted a lot of attention. Subsequently, the Austrian privacy activist Maximillian Schrems did not believe that an adequate level of protection of his personal data transferred to the US could be longer guaranteed. Thus, he demanded the suspension of the transfer of his data to the US. The following trial went through all judicial instances, before the European Court of Justice. Ultimately, the Court supported Schrems opinion, declaring the legal basis for the transfer of personal data from the EU to the US invalid. The judgement and its underlying principles directly challenged the EU data protection frame work. Since the judgement in 2015, the Data Protection Directive got replaced by the General Data Protection Regulation and the Commission has announced further policy changes.

The purpose of this study is to answer the research question: *To what extent do the EU data protection policies reflect the principles upheld in the judgement of the Schrems case?* Therefore, a systematic overview of the European data protection framework is given. Initially, the framework before the trial is presented. Afterwards, the judgement and its underlying principles are analyzed. Finally, the current framework and upcoming changes are depicted and the significance of the Schrems case for these legal developments is evaluated.

Table of Content

1. Introduction ... 1

1.1 Research design ... 4

1.2 Scientific and social relevance ... 5

2. The EU data protection framework before 2015 ... 6

2.1 The Data Protection Directive ... 9

2.2 The *Safe Harbor* Agreement ... 12

2.3 The ePrivacy Directive ... 14

2.4 Conclusion of the Chapter ... 17

3. The Schrems Case ... 18

3.1 Background ... 18

3.2 The Trial ... 21

3.3 The Judgement ... 22

3.4 Conclusion of the Chapter ... 24

4. The EU data protection framework after 2015 ... 25

4.1 The Privacy Shield ... 27

4.2 The GDPR ... 30

4.2.2 Obligations for data controllers and processors ... 33

4.2.3 Application and enforcement ... 36

4.2.4 Data transfer to third countries ... 37

4.3 The ePrivacy Regulation ... 38

4.3 Conclusion of the Chapter ... 41

5. Conclusion ... 42

6. References ... 45

Abbreviations

CFR	Charter of Fundamental Rights of the European Union
CFSP	Common Foreign and Security Policy
DOC	US Department of Commerce
DPA	Data Protection Authority
DPC	Data Protection Commissioner
DPD	Data Protection Directive
ECJ	European Court of Justice
EDPB	European Data Protection Board
ePD	ePrivacy Directive
ePR	ePrivacy Regulation
FTC	Federal Trade Commission
GDPR	General Data Protection Directive
NSA	National Security Agency
OECD	Organization for Economic Cooperation and Development
OTT	Over-the-top services
UDHR	Universal Declaration of Human Rights

1. Introduction

With the rise of new communication technologies in the past decades the discussion about data protection and privacy received more attention. Especially the handling of personal data by big technology companies concern a growing number of people. They fear the misuse of new and existing technologies while the complexity of the issue gets more confusing. Thus, policy makers were required to enable laws, which protect the privacy of the citizens. In regard to the EU, the first legislation concerning this topic was the Data Protection Directive (DPD). It was applicable from 1994 until 2018, when it got replaced by the General Data Protection Directive (GDPR). In this time period information technologies experienced a rapid growth, today they are indispensable in virtually every aspect of modern life and with recent innovations like self-driving cars, virtual assistants or the internet of things there is no end in sight for this development. However, with new technologies new problems and challenges emerged, on the one hand companies began to collect data from their customers, e.g. for advertisement or personalized services, which led some economists to rate the potential of data so high that they call it "the oil of the 21st century". On the other hand governments started collecting data of their citizens in the name of security (The Economist, 2017). But, the right to privacy is enshrined in Article 12 of the Universal Declaration of Human Rights (UDHR):

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

Given the fact that the UDHR is not legally binding to states or persons, other legally binding laws such as the DPD or the GDPR are necessary to ensure that this right is not violated and personal data gets exploited. However, it is almost impossible for the lawmakers to keep up with the enormous pace of evolving technologies and the resulting new possibilities to collect personal data (Moses, 2007, pp. 247). Hence, data protection regulations needed to be adapted gradually, often after scandals which gained public attention and lead to demands by privacy activist and Non-Governmental Organizations. In this process the EU took a leading role in the protection of privacy rights, setting today a global standard (Carnevale, 2018). This

paper is going to examine this legal development of data protection legislation in the EU.

The DPD's aims were to protect the rights and freedoms of people while processing personal data as well as to regulate data processing within the EU and data transfers to third countries (Art. 1 DPD). Accordingly, data transfers to third countries were only allowed if third countries guaranteed an "adequate level of protection" (Art. 25 DPD). In the year 2000, the European Commission made the decision, that the United States principles of data protection did comply with the EU Directive, this decision is commonly known as *Safe Harbor* decision. However, in the following years big (American) technology companies like Google or Facebook were continuously covered in the news, due to controversial practices regarding privacy and data protection.

In 2010, after a Wall Street Journal report, Facebook admitted that its most popular game applications shared private user data and contact details of friends with external companies, which used the data for advertisement. According to the American newspaper the data breach affected tens of millions of users, even those who had activated Facebook's strictest privacy settings (Steel & Fowler, 2010). Another example for a violation of privacy rights became public in 2011 when security researchers discovered a hidden file inside Apples mobile devices which stored a complete collection of locations visited by their user in the past year (Arthur, 2011a). In the aftermath, Google and Microsoft had to admit that they collected the same kind of user location data on their mobile systems too (Arthur, 2011b). These practices meant a constant monitoring of millions of individuals without their knowledge and thus an infringement of their privacy rights.

After the revealings about mass surveillance practices by the American National Security Agency (NSA) by whistleblower Edward Snowden in 2013, public attention was drawn to privacy and the laws which should protect it. The Guardian reported, that the NSA collected the telephone records of millions of Americans. Furthermore, the NSA tapped directly into the servers of several internet firms, including Facebook, Google, Microsoft and Yahoo, to track online communication with a surveillance programme known as *PRISM*. In the following month more details became public exposing a global surveillance network, which also monitored EU citizens (MacAskill & Dance, 2013).

In the same year, the Austrian privacy activist Maximilian Schrems handed in a list of complaints against Facebook Ireland Ltd. to the Irish Data Protection Commissioner (DPC), as Facebook has its European headquarters in Ireland[1]. The complaints aimed at prohibiting Facebook to transfer data from Ireland (EU) to its servers in the US, since Schrems did not believe, in the light of the recent revealings, that Facebook could guarantee an adequate level of protection for the data of European citizens stored in the US. This accusation was intensified by Facebook's involvement in the NSA scandal. The DPC Mr. Billy Hawkes rejected the complaint on the ground that the complaint was "frivolous and vexatious" (Fioretti, Nasralla, & Murphy, 2015). Subsequently, Schrems requested a judicial review of the DPC's rejection at the Irish High Court, which was accepted. On 18th June 2014, the Irish High Court shunted the case to the European Court of Justice (ECJ). The responsible judge Mr. Gerard Hogan reasoned the step arguing that Irish privacy law had been pre-empted by European law. In the following trial (case C-362/14 (Schrems vs. Data Protection Commissioner)) the ECJ reviewed the adequacy decision on *Safe Harbor*, concluding *Safe Harbor* to be insufficient in meeting EU standards.

The most direct consequence of the Schrems judgment is the new legal framework for EU-US data transfers: The *Privacy Shield*, which was introduced in February 2016 and adopted by the European Commission on the 12th of July 2016 and replaced *Safe Harbor* (Kuner, 2016, p. 19 and Monteleone & Puccio, 2017, p. 16). Furthermore, the Commission discussed ways to align and alter the DPD to contemporary developments, which finally resulted in the adoption of the GDPR. The Regulation has been adopted in April 2016 and became effective on the 25th of May 2018, after a two-year transition period (Hustinx, 2013, p. 27). Moreover, the Commission has announced further adjustments to the data protection framework (Hoffmann, 2017, p. 36). These recent developments of the EU data protection policy framework raise the question: *To what extent do the EU data protection policies reflect the principles upheld in the judgement of the Schrems case?*

[1] Facebook has its European headquarters in Ireland due to two main reasons (as many big American technology companies): The first one can be described as technological, as Ireland is the closest point of the EU to the North American coast. The second one can be summarized as legal. The Irish tax law grants big technology companies many advantages (Garcia-Bernado, Fichtner, Takes, & Heemskerk, 2017, S. 6 pp.). Furthermore, Ireland was considered to have relatively low privacy standards after implementing the DPD.

1.1 Research design

The above stated research question will be answered by making use of a legal analysis, which shall provide the reader with a holistic picture of the Schrems case, its principles as well as the relevant EU data protection legislation. In the following chapter, the applied research design and the methodology are depicted and their choice is explained.

The main research question (RQ) can be categorized as an explanatory, hermeneutic and logic type of legal research. In the second chapter, an illustration of the EU data protection policy framework before the Schrems Case will be provided. This step is necessary, to subsequently analyze the changes of the current legal framework and to examine to what extent the principles upheld in the Schrems case are reflected. This chapter is based on an explanatory approach. Subsequently, the principles, which emerged from the Schrems case are presented in chapter three. For this purpose, the judgment of the ECJ is presented at length and interpreted, hence this chapter is based on a hermeneutical method. In chapter three the GDPR and the other relevant legislation, which was implemented after 2015, are analyzed and compared to the previous framework, as well as to principles from the Schrems case. Here, an explanatory and logical approach is applied. Finally, the main research question is answered with the use of the results of the previous chapters (Matera, 2016, p. 5). To answer the main RQ the following sub questions (SQ) have been identified:

SQ 1: What was the data protection regulatory framework in the EU before the Schrems case?

To answer the first sub question all relevant EU data protection laws, which were effective before 2013 are presented. A special focus is put on the framework, which regulated the EU-US data transfer, since it is crucial for the Schrems case. Thus the aim of this chapter is to explain the law, it applies an explanatory legal approach (Matera, 2016, p. 5). For the chapter mainly EU documents, such as the DPD and the *Safe Harbor* Agreement, as well as scientific articles examining the data protection policy framework before the law suit of Schrems are used.

SQ 2: Which principles and rules emerged from the Schrems case?

The second sub question discusses the Schrems case and the implications of its judgement. This sub question is based on an explanatory and hermeneutic method

(Matera, 2016, p.5). First, the case is presented at length, afterwards, the judgement of the ECJ is analyzed and the principles upheld in the case are identified. This methodology can be described as a case study and literature review. The literature, which is used for the second chapter are mainly the ECJ case C-362/14, articles which analyze the consequences of the judgment as well as reactions to it from the EU institutions presented in position and policy papers.

SQ 3: What are the innovations brought by the new European data protection policies to the data protection framework of the EU?

To provide an answer to the last sub question, it is necessary to first identify to which extent the data protection legislation has changed since the Schrems-judgement in 2015. Afterwards this new framework is depicted in a detailed manner, by making use of an explanatory approach. Subsequently, a hermeneutical approach is applied in order to highlight innovations brought by the new framework (Matera, 2016, pp. 5-6). The last chapter is also based on literature reviews. The sources for this chapter are mainly the Privacy Shield, the GDPR and official EU statements about proposed changes to the data protection law as well as scientific articles which analyze the development of the legislation.

In the conclusion an evaluation of the principles upheld in the Schrems case, which have been pointed out in chapter three, and the data protection policy framework of the EU, described in chapter two and four, is conducted. Therefore, the principles of the Schrems case and the current European data protection policies are reviewed on their coherence and underlying rules. By using this logic approach the RQ is finally answered (Matera, 2016, p. 5-6) Hitherto, the scope of the research question and the sub questions have been identified. Furthermore, the methodological approach applied in order to answer those questions has been illustrated. The next section justifies the scientific and social relevance of the RQ.

1.2 Scientific and social relevance

This research is of exceptional social and scientific relevance. First, the fact that the right to privacy is enshrined in Art. 12 UDHR underlines the importance of the issue. Second, the protection of privacy and the freedom of information is an issue of paramount importance for liberal societies. In April 2018, *The Guardian* and *The New*

York Times revealed that 50 million Facebook profiles were harvested by the British data analysis company *Cambridge Analytica*. Later, this number rose to 87 million affected Facebook profiles. The obtained data could be used to generate "psychographic" profiles of the users and show personalized advertisements or (fake) news stories to influence the user's political views and ultimately their voting decision. The newspapers accused the organizers of the Trump presidency campaign that they have used the service provided by *Cambridge Analytica* (Cadwalladr & Graham-Harrison, 2018). This major data scandal showed - once again - that data protection is current and socially relevant issue, which not only affects individuals personally, but also societies and democracies as a whole. Especially, the data transfer of the EU to the US is important in this context, since the EU is generally considered to have a high standard of data protection and many of the big technology companies, which handle personal data, have their head offices and servers in the US.

Given the rapid development of new (communication) technologies, this study is also highly relevant from a scientific point of view. It is for this reason, that legislation, which regulates its use needs to be adjusted and updated regularly (Moses, 2007). Afterwards, these new policies can be analyzed in terms of their effectiveness by researchers and thus constitutes a constant reciprocal process. Since the newest EU data protection policy is relatively new, only little of research on this topic has been conducted yet. Therefore, this study will help to understand the current EU data protection *acquis*. Moreover, this paper is going to contribute to the scientific discussion about European data protection regulations.

2. The EU data protection framework before 2015

In this chapter the first SQ: *What was the data protection regulatory framework in the EU before the Schrems case?* is answered. Therefore, the development of data protection policies in the EU is fist summarized, afterwards the relevant legislation, which composed the framework before the judgement in 2015, is identified and the choice is reasoned. Finally, the selected laws are analyzed and their central provisions and principles are presented.

The first step of data protection policy in Europe was done 1973 by the Council of Europe, which adopted the resolutions (73)22 and (74)29 on the protection of personal

information stored in electronic data banks in the private sector and respectively in the public sector. Ultimately, this led to the Convention 108 on Data Protection in 1981 (Honduis, 1983, p. 103-105). Today, the convention is ratified by 54 states (Council of Europe, 2019a). The Convention aims at protecting the individual against the misuse of personal data. Besides granting the individual certain rights in relation to the processing and collecting of personal data, it prohibits "the processing of "sensitive" data, on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards" (Council of Europe, 2019b). Moreover, it grants the individual's right to know which information is stored about him or her and to have it corrected if it is incorrect. Restrictions to the rights enshrined in the Convention are only possible when they are in conflict with vital state interest like national security or defense. Furthermore, the Convention establishes restrictions on data transfer between states where the data protection law does not provide an equivalent level of protection (Council of Europe, 2019b).

Nevertheless, as the Council of Europe "was less successful in terms of ensuring sufficient consistency across its Member States", further legislative action was needed (Hustinx, 2013, p. 9). In October 1994 the EU adopted the directive 95/46/EC – more commonly known as DPD – which was based on a recommendation of the OECD (Hustinx, 2013, pp. 9 & 33). The DPD regulates data processing within the EU and data transfer to third countries. Thereby, companies processing personal data were given restrictions, e.g. by the principle of purpose limitation, while data subjects obtain rights, as the right to object the processing of their individual data (Art. 6 DPD). Data transfer to third countries are regulated in Art. 25 DPD as data transfer outside the EU/EEA are only allowed if the third country ensures an "adequate level of protection" (Art. 25 (1) DPD). This principle is the basis for the *Safe Harbor* Decision, which regulated the data transfer to the US until 2015. The adequacy is discussed much, as it offers a wide scope for interpretation (Hustinx, 2013, p. 11). Furthermore, the Charter of Fundamental Rights of the European Union (CFR), adopted six years later (in 2000), contains provisions on data protection: Art. 7 CFR states that "everyone has the right to respect for his or her private […] life" and Art. 8 CFR explicitly guarantees "the right to the protection of personal data".

In some policy areas the main EU law – before 2015 the DPD and today the GDPR – is complemented by specific legislation. Before 2015 these were in particular:

- The Regulation [45/2001/EC] on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data
- The Directive [EU/2016/680] on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
- The Directive [2002/58/EC] concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (also kwon as ePrivacy Directive (ePD))

The Regulation No. 45/2001 deals with the processing of personal data by the organs and institutions of the EU, and aims at the protection of the fundamental freedoms and fundamental rights of the citizens. It corresponds in its structure and content in wide parts of with the DPD, hence the EU organs must respect in general the same principles laid down in the DPD (Hoffmann, 2017, pp. 24). One important consequence of the Regulation is the creation of the European Data Protection Supervisor in 2004, which serves as an independent data protection authority. His main tasks are to monitor the protection of personal data in the EU and to advise the EU institutions about this topic (European Union, 2019).

The Directive No. 2016/680 regulates the data processing of legal authorities, where special rules apply. Both legislations are untouched by the ramifications of the Schrems case, and are only applicable for the specific institutions and its bodies, rendering them irrelevant for this research.

Consequently, the relevant data protection framework before 2015 consists of the DPD, the *Safe Harbor* decision and the ePD. In the following, the provisions and principles of the legislations are discussed.

2.1 The Data Protection Directive

The directive is designed to protect the rights and freedoms of people while processing personal data (Art. 1 DPD). The main goal of the DPD was a harmonization of the data protection law of the EU Member States (Schwartz, 1994, p. 481).

It applies whenever personal data is processed, whether by state authorities or private individuals/companies. However, it does not apply if the data is processed solely for personal or family purposes or if the data is required for public security, national defense or state security reasons (Art. 3 DPD).

According to the DPD personal data is all information about an individual which makes him or her identifiable. A person is considered identifiable if he/she can be identified directly or indirectly, for example by a user number assigned to the name (Art. 2 DPD). The person whose data is being collected is defined by the DPD as the data subject and the person, company or organization who collects the data is called data controller. A data processor does not collect the data himself or herself, he/she just processes already collected data (Art. 2 DPD).

On the one hand the DPD ensures the data subject comprehensive rights: First, it defines key criteria for making data processing legal, according to those processing of personal data is forbidden in general and only allowed if the affected data subject has explicit agreed to it, or the processing is necessary for the following reasons:

1. for the performance of a contract or to enter one
2. for compliance with a legal obligation
3. in order to protect the vital interest of the data subject
4. for the performance of a task carried out in the public interest
5. for the purposes of legitimate interests pursued by the controller or by a third party to whom the data are disclosed, except where such interests are in conflict with fundamental rights and freedoms of the data subject (Art. 7 DPD).

The data subject has the right to object the processing in the last two cases or if the controller processes the data solely for direct marketing (Art. 14 DPD).

Furthermore, the DPD establishes principles relating to data quality, which must be respected when transferring personal data. According to those principles data processing is only legal if the personal data is collected for a specified, explicit and legitimate purpose. It must be processed in a fairly and lawful manner. Furthermore,

the collected data must correspond to the original purpose, be relevant for it and is not allowed to go beyond it. In addition, the collected data has to be correct and kept up to date where necessary. Moreover, the data may be saved only for the purpose for which it was raised and saved no longer than necessary (Art. 6 DPD).

The DPD protects in particular special categories of personal data from which racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership can be deduced as well as data about health or sexual life. The processing of such data is also forbidden in general, but the standards for processing this special kind of data are more restricted and exceed the provisions in Art. 6 DPD (Art. 8 DPD).

Moreover, the data subject enjoys comprehensive information rights additional to those mentioned in Art. 6 DPD: The data subject has the right to retrieve the following information from the data controller:

1. The Identity of the controller
2. The purposes of the processing
3. The recipients of the data
4. The category of the data (Art 10,11 DPD)

Additionally, the Member States have to guarantee that every data subject has the right to access the information relating to him or her from the controller and to get information about possible third parties to whom the data have been transmitted (Art. 12 DPD).

On the other hand, the DPD determines obligations for the data controller. He/She have to ensure the security of the data processing; therefore, they must take suitable measures to guarantee an effective protection of the data. Furthermore, the controller has to protect the "data against accidental or unlawful destruction", loss, changes as well as against unauthorized access (Art. 17 DPD). Nevertheless, the DPD does not define concrete measures how the controller should ensure this level of protection (Art 16, 17 DPD). Moreover, controllers must notify any planned automatic data processing to the national supervisory authority in advance. This body then checks whether there are risks to the rights and freedoms of the persons concerned. Exceptions to this obligation are possible, if the company "appoints a personal data protection official" (Art. 18 DPD).

The transfer of collected personal data to third countries is only allowed if the concerned country ensures an equivalent level of protection. The commission has to acknowledge this. Exceptions to this are possible if conditions similar to those in Art. 7 DPD are fulfilled (Art. 25, 26 DPD).

Each member state commits to establish an independent national supervisory authority (Data protection authority (DPA)), which controls the compliance of the directive (Art. 28 DPD). Furthermore, Member States must provide judicial remedies for those affected by a violation of their rights and ensure that the data subject is entitled to get a compensation from the data controller, in the case of unlawful data processing (Art. 22, 23 DPD). In addition, the so-called "Article 29 Data Protection Working Party" as an independent intergovernmental body with an advisory role is established, to promote a consistent application of the directive in the EU and to provide expert recommendations to the EU institutions and the Member States regarding data protection (Art. 29 DPD).

For the case of a violation of the provisions of the DPD, the Member States have to implement “suitable measures” and define sanctions to guarantee a compliance to the directive (Art. 24 DPD).

Finally, the Member States may restrict the data protection principles of the directive for the following reasons: the security of the country, the national defense, the public security, the prevention or investigation of criminal offences, an „important economic or financial interest of a member state or of the European Union“ or for the protection of the affected person or the rights and freedoms of other people (Art. 13 DPD).

EU directives are not legally binding for individuals, instead they are addressed to the Member States. Directive 95/46/EC foresaw the transfer of its guidelines into national law by the end of 1998, with which all Member States complied. (European Commission, 2003).

As Art. 25 DPD stated, the DPD required a recognition of the data protection standards of a third country by the Commission. For EU-US data exchange this was done in the so-called *Safe Harbor* Agreement. Since the trans-atlantic data transfer was the main subject of the Schrems case and *Safe Harbor* was declared invalid subsequent to the process, the agreement and its principles are depicted in the following.

2.2 The *Safe Harbor* Agreement

The European Union and the United States have substantial different data protection regimes, as the US has a significant lower standard of data protection (Greenleaf, 2012, pp. 70-72). After the DPD entered into force in 1995, these fundamental differences threatened the transfer of personal data between the EU and the US, since the DPD in general outlaw the transfer of personal data from EU Member States to states which data protection did not have an equal level of protection (Art. 25 DPD). Though, stopping the digital data transfer would have had harsh economic consequences for both parties, as the EU and the US are each other's most important investment and trade partners (European Commission, 2019). Subsequently, the cross-border data transfer between both economic areas is the highest in the world (Meltzer, 2014, pp. 5-6).

Given that the unhampered flow has been identified as mutual interest, EU and US officials negotiated how US companies can meet the required "adequate level of protection". This resulted in the *Safe Habor* Privacy Principles which were first published in 1999, together with 15 legally binding FAQ's, by the US Department of Commerce (DOC) (WP 27 2000/520/EC). In 2000, the Commission decided that these principles comply with the required level of protection for the personal data of EU citizens (2000/520/EC).

First, according to the Notice Principle, the data subject must be informed about the collection of data and the intended purpose, as well as about potential third parties to whom the data is accessible, by the data controller. Furthermore, the data subject must have the opportunity to make inquiries and complaints to the controller about the use of their personal data (Annex I *Safe Harbor* Decision).

Second, to ensure data integrity, the collected data must be relevant for the original purposes. Moreover, the controller should take reasonable measures to ensure that data is relevant for the purpose, correct, complete, and current (Annex I *Safe Harbor* Decision).

Third, the data subject must have the choice if his or her data is disclosed to a third party or is used for a purpose other than the original purpose for which the data was collected. The standards for sensitive personal data, like the one defined in in Art. 6

DPD, are even higher. Here the data subject hast agree unambiguously to the processing (Annex I *Safe Harbor* Decision).

Fourth**,** the Transfer to third parties is only legitimate when it is necessary for the original purpose and only if adequate protection is guaranteed. When controllers transfer data to a third party, they must respect the already described principles. (Annex I *Safe Harbor* Decision).

Fifth, he processed data must be stored secure and be protected against loss, misuse, unauthorized access, alteration and destruction (Annex I *Safe Harbor* Decision).

Sixths**, t**he data subject must have the possibility to access the data, correct it and delete it where it is inaccurate, except where the expense for the controller to do so would be disproportionate to the risks to the privacy of the individual or where the rights of others would be violated. Furthermore, the *Safe Harbor* principles may be limited when national security, public interest, or law enforcement requirements are at stake (Annex I *Safe Harbor* Decision).

Finally**,** to enforce the previous principles effective means should be established to ensure the compliance. For the case of violations of the principles severe sanctions should be applied (Annex I *Safe Harbor* Decision).

Under *Safe Harbo*r, a US company could self-certify to the DOC that it adheres the seven basic principles. Participation in Safe Harbor was open to any US organization/company which was regulated by the Federal Trade Commission (FTC) and to American airline companies which are regulated by the Department of Transportation (DOT) (Weiss & Archick, 2016, p. 6). This excluded in particular financial institutions and telecommunication companies, including internet service providers, but also non-profit organizations and journalists, where special rules for data transfer apply (*Safe Harbor* FAQ 3-4).

After opting in, a company had to provide a description of its activities with respect to personal data. Furthermore, "the organization […] declare its commitment to cooperate with the EU authority" (*Safe Harbor* FAQ 6). Moreover, it had to conduct an appropriate employee training for the handling of personal data in compliance with the principles and implement an effective internal dispute mechanism for the settlement of possible conflicts. Companies had to self-recertify annually that they still comply to the EU-US *Safe Harbor* principles. It was either possible to perform a self-

assessment to verify the compliance, or to commission a third-party to perform the assessment (*Safe Harbor* FAQ 7).

The US government did not regulate the *Safe Harbor* Agreement, which was self-regulated through the companies which obliged to it and the dispute resolution bodies they established. The FTC observed the system under the oversight of the DOC. The FTC was committed to review all complains of potential violations from EU member state authorities. (*Safe Harbor* FAQ 11).

To enforce the *Safe Harbor* principles, violations could be penalized by the FTC with sanctions of up to $16,000 per day (US International Trade Administration, 2015). Until 2015 the FTC has penalized 40 companies with violations of the *Safe Harbor* principles (Weiss & Archick, 2016, p. 6). If an organization failed to comply with the *Safe Harbor* principles it must notify the Department of Commerce as soon as possible, otherwise it could be prosecuted under the "False Statements Act" (*Safe Harbor* FAQ 11). "Persistent failure to comply would result in withdrawal of *Safe Harbor* status, a fact that would be indicated on the *Safe Harbor* website, and also, potentially, by regulatory action" (Weiss & Archick, 2016, p. 6)

The *Safe Harbor* principles could be however limited to the extent necessary for national security, public interest, or law enforcement requirements (Annex I *Safe Harbor* Decision).

The agreement existed between the EU and the US until it was declared invalid by the ECJ in 2015 in consequence of the Schrems case (Weiss & Archick, 2016, p. 1).

Communication technologies were evolving rapidly in the late 90s and early 2000s due to new developments. Thus, the processing of personal data in the communication sector increased constantly. Therefore, the EU had to complement the DPD in this regard. This effort resulted in the ePD, which deals with new issues of electronic communication like confidentiality of information, treatment of traffic data, spam mails and web cookies. In the following the principles of the ePD are summarized.

2.3 The ePrivacy Directive

The Directive [2002/58/EC] entered into force on the 31st of July 2002. It aims at the protection of fundamental rights in the electronic communication sector and

complemented the DPD in this field. It should, on the one hand strengthen the protection of privacy rights and on the other hand it should make and unhindered data exchange in the EU possible by further harmonizing the existing law. In contrast to the DPD, which protects only natural people the ePD also protects the rights of legal entities (Art. 1 ePD).

The ePD applies when personal data is processed via public communications networks for publicly available electronic communications services, this includes e.g. telecommunications services and radio or television services (Art. 3 ePD). The ePD does not apply for services that offer their content via electronic communications networks like e.g. Facebook and YouTube or which are under editorial control like news websites.

First, the ePD requires Member States to ensure the confidentiality of all messages and the related data transmitted over public communication networks and publicly available communication services (Art. 5 ePD). To ensure the confidentiality of electronic communication, the ePD obliges electronic communications service providers to guarantee security standards for data processing. Service providers operating publicly available electronic communication services in public communication networks are required to take appropriate measures to ensure the security of their services, if necessary, in cooperation with the network operator. The level of security must be adequate, considering the cost of security measures against the risks at stake (Art 4 ePD). Providers are only allowed to grant access to personal data to police or authorized persons for prosecution (Art. 1 & 11 ePD).

Providers who offer publicly available electronic communications services over the internet, like e-mail services, must inform users about possible measures to protect transmitted data, e.g. the use of special software or encryption tools. Furthermore, they have to notify the responsible national supervisory authority in the case of a possible violation of the principles defined by the ePD. Moreover, the service provider must immediately inform the data subject about a possible data breach that could put his or her privacy rights at risk (ePD Preamble 20).

The ePD not only protects the confidentiality of communication, but also so-called "traffic data" related to electronic communication. Traffic data is data which is “processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof” (Art 2 ePD). These include, e.g.

information about who communicated with whom, when, and how long. Traffic data must be deleted or anonymized as soon as it is no longer required for communication or billing purposes, unless the user concerned has consented to the traffic data being used for another purpose, e.g. marketing or to provide "value added services" (Art. 6 ePD)

According to the ePD location data (which is not traffic data) is only allowed to process when the data is anonymized, or with the consent of the users. The user has to have possibility to withdraw their consent for the processing of location data (Art. 9 ePD).

In principle, the ePD prohibits the use of web cookies unless the user has given his consent after being informed comprehensively and in particular about the intended purpose of the processing of the collected data (Art. 5 ePD). Web cookies are a small data files which are created on a user's devices while browsing the internet. They are sent from a website to remember information, like personal preferences or items added in the shopping cart in an online store or to record the user's online activity. This kind of data is often used for commercial purposes (WebWise Team, 2012).

An important objective of the ePD is to protect users from unwanted advertising. Thus, it prohibits sol called SPAM messages, which are often made using automatic call machines or sent by fax or to growing extend by e-mail. Such messages are only allowed if the user explicitly agreed to it (Art. 13 ePD).

Just as the DPD, the ePD allows Member States to restrict rights and obligations in the name of state security, national defense, public security or the prosecution of criminal offenses. The use of electronic communications systems has to be compatible with a democratic society. However, Member States and respectively their legal authorities have to act appropriate to the risk at stake (Art. 15 ePD).

With regard to remedies, liability and sanctions, the ePD refers to the provisions of the DPD. Thusly, the remit of the Art. 29 Working group is broadened to include the protection of rights, freedoms and legitimate interests in in relation to electronic communication (Art. 15 ePD)

The ePD had to be transferred into national law by 31.10.2003. In 2009 it was adapted in the context of the review of the regulatory framework for electronic communications. With the first publication of the GDPR the Commission has announced a review of the ePD for 2019, to ensure consistency between the GDPR

and the ePD. On 10th of January 2017, the Commission presented a proposal for a Regulation concerning the respect for privacy and the protection of personal data in electronic communications, which would replace the ePD[2] . The last chapter deals with this proposal in detail.

2.4 Conclusion of the Chapter

After having examined the relevant data protection law, the first SQ*: What was the data protection regulatory framework in the EU before the Schrems case?* is answered.

The data protection framework before 2013 consisted of the resolutions (73)22 and (74)29 as well as the Convention 108 on Data Protection by the Council of Europe. Moreover, the CFR, the Regulation [45/2001/EC], the Directives [2016/680/EC], [1995/46/EC] (DPD), and [2002/58/EC] (ePD) as well as the *Safe Harbor* Agreement form the regulatory framework before 2013. The legislation of the Council of Europe are not relevant for this research as they are no EU legislation. As depicted above, the Regulation [45/2001/EC] and the Directive [2016/680/EC] have not been examined in detail as their analysis do not provide an added value to this work.

Overall, the DPD, the *Safe Harbor* Agreement and the ePD set a high standard for data protection in the EU. First, every individual has to consent to the processing of his or her personal data. Second, personal data has to be secured against potential threats and collected personal data can only be used for the originally intended purpose. Additionally, data transfer to third parties or states is generally considered to be illegal. Exceptions to this rule are only possible if an adequate level of protection is guaranteed and has been acknowledged by the European Commission. In addition, every individual has the right to get full information about the data stored and processed about himself or herself. Beyond this, each individual has also the right to withdraw the consent for processing of personal data at any time. Exceptions to the regulations can only be made if state security or vital national interest are at risk.

However, after having depicted the relevant legislation, a number of weaknesses are identified. First, as already described above, the nature of the DPD and the ePD (being

[2]COMMISSION STAFF WORKING DOCUMENTIMPACT ASSESSMENT Accompanying the document Proposal for REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

directives) leave the concrete implementation of the provisions up to the Member States. Second, if information about a person are protected depends solely on whether or not the processed data are defined as personal data. Data such as financial information and location data are not inevitable classified as personal data. Third, the monitoring role of the national DPAs, defined in the Safe Harbor agreement, remains unclear. Fourth, the fact that an adequate level of protection is only investigated once poses a problem. Hence, the Adequacy Decision by the Commission cannot take altered circumstances in the third country, as for example the NSA scandal, into account. Moreover, sanctions are not clearly defined in the DPD and the ePD leaving a lot of scope for interpretation. Also, this also applies to other provisions of the directive as the discovered differences in national implementations indicate (Robinson, Graux, Botterman, & Valeri, 2009, p. 26).

3. The Schrems Case

In 2013, the European data protection framework came suddenly into public focus, when details about mass surveillance programs by the American NSA were exposed by Edward Snowden. These revelations had far-reaching consequences. The most direct one – at least for the European data protection framework – was a claim by Maximilian Schrems in front of the ECJ, who wanted to prevent Facebook from transferring his personal data to servers based in the US.

The following chapter aims at answering the *SQ 2: Which principles and rules emerged from the Schrems case?* For this purpose, the Schrems case and the circumstances which lead to the process are presented in detail. Subsequently the principles, which underlie the judgement are discussed.

3.1 Background

As already described in the previous chapter the commission acknowledged the adequacy of the *Safe Harbor* principles in the adequacy decision from 2000. This allowed a free flow of data between EU and US.

By 2015, approximately 4,500 American companies had joined the *Safe Harbor* Agreement, including Microsoft, Amazon, Google and Facebook (Weiss & Archick, 2016, p. 6). In June 2013 the perspective on the EU-US data exchange was changed abrupt when whistleblower Edward Snowden revealed details about the mass surveillance program *PRISM* by the NSA. Snowden had worked as a system administrator for the NSA at the Kunia Regional SIGINT Operations Center in Hawaii on behalf of the US consulting firm Booz Allen Hamilton (Grennwald, MacAskill, & Poitras, 2013).

On May 20th 2013 Snowden flew to Hong Kong requesting asylum. Between June 1st and June 6th, he handed Guardian reporters Glenn Greenwald and Ewen MacAskill and documentary filmmaker Laura Poitras his collected NSA documents. In an interview, he stated that he had collected estimated 1.7 million documents from the internal data network of the NSA (Poitras, 2014).

Subsequently, The Guardian and the US newspaper The Washington Post published documents and information about the hitherto unknown US programs monitoring global Internet communications, *PRISM* and *Boundless Informant*.

On June 23rd, Snowden, coming from Hong Kong, arrived at Sheremetyevo airport in Russia, where he stayed in transit for several weeks in a hotel and was granted asylum subsequently (Poitras, 2014).

In the months following his revelations more and more details about the surveillance practices of the NSA and other allied intelligence services became public: It became clear that the NSA had obtained unrestricted access to personal data of EU citizens stored on US servers (MacAskill & Dance, 2013). Moreover, most companies involved in the PRISM program appeared to be *Safe Harbor* certified (Weiss & Archick, 2016, p. 9)

Thus, the Commission evaluated the *Safe Harbor* agreement and judged that the self-verification mechanism is in transparent and not sufficient. According to the Commission the *Safe Harbor* agreement became "one of the conduits through which access is given to US intelligence authorities to collecting personal data initially processed in the EU" (Commission Communication p. 16). The member of the EU Parliament Jan Phillip Albrecht, who became later the rapporteur at for the GDPR, and Jacob Kohnstmann, the Chairman of the Article 29 Working Party, stated that there

was a "substantial likelihood" that the Safe Harbor principles were violated (Commission Communication p. 5).

Furthermore, the Commission recommended closer control of the enforcement of the the provisions established in the *Safe Harbor* Agreement. Moreover, it demanded in particular "the provision of information to individuals about potential further transfers to US intelligence services" and a comprehensive information to individuals about their privacy rights (Coudert, 2015).

The privacy scandal attracted the attention of privacy activist and NGOs. Especially the Austrian activist Maximilian Schrems, who started his activities in 2011, when he demanded that Facebook provides him all data stored about him. Facebook gave him over 1,200 pages, which also contained data he had already deleted (Pidd, 2011). Subsequently, the Irish DPA agreed with Facebook on changes to their privacy policy, which should enable European Facebook users to have more control over their personal data (O'brien, 2012). Since then Schrems has been suing Facebook multiple times.

Due to the new evidence of mass surveillance practices by the NSA, he complaint to the Irish DPC. He demanded the stop of the transfer of his personal data by Facebook Ireland to the mother company Facebook Inc., which is located in the US, since in his opinion the adequate level of protection could be no longer guaranteed (Coudert, 2015).

Though, the Irish DPC argued that it was not responsible for the case, since national DPAs would have "no competence to challenge the validity of an Adequacy decision" (Coudert, 2015). Subsequently Schrems complaint against this opinion to the Irish High Court.

The Irish High Court shared Schrems concerns, that fundamental privacy rights of EU citizens' could be affected. First, the Court wanted to ascertain whether the Adequacy decision by the Commission prevents a national DPA from investigating a complaint about the insufficient level of protection of personal data in a third country. Furthermore, the judges at the court believed, in the light of the revelations by Mr. Snowden, that it would be impossible for US companies to satisfy the requirements of

Articles 7[3] and 8[4] CFR. Hence, the case was submitted to the ECJ according to Article 267 TFEU (Coudert, 2015). There the case was negotiated under the name: "Maximillian Schrems v. Data Protection Commissioner, C-362/14" in front of the Grand Chamber.

3.2 The Trial

During the Trial the ECJ first answered the question, of the competences of the national supervisory authorities: The Advocate General Mr. Yves Bot emphasized the independence of the DPAs and stated that "the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection" of personal data (Final Opinion of Advocate General II. 63.). With his assessment the Advocate General reiterated that the existence of the adequacy decision of the Commission did not restrict the competences of the national DPAs. Thus the DPAs do have the power to suspend data transfers in a third country.

Subsequently, the Court evaluated the validity of the Safe Harbor decision: In his Final Opinion Mr. Bot found that the Commission did not consider the domestic law and circumstances of the US in the Adequacy Decision. Furthermore, he criticized the lack of effective monitoring and control mechanisms and of effective judicial protection against violations of privacy rights. Moreover, he complaint about the unlawful restriction of the competences of the national DPAs (Final Opinion of Advocate General C-362/14). In his entire argumentation the Snowden revelations played a major role. As a consequence, the Court finally annulled the *Safe Harbor* Agreement at the 06.10.2015.

[3] **Art. 7 CFR:** Everyone has the right to respect for his or her private and family life, home and communications.

[4] **Art. 8 CFR:** 1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

3.3 The Judgement

With the judgment the ECJ followed the final Opinion of the Advocate General entirely. First it strengthened the role of the national DPAs, as it clarified that the existence of an Adequacy Decision, in fact increases the competences of the national DPAs. In its judgement the ECJ explicitly referred to Article 16 (2) TFEU and Article 8 (3) CFR which oblige the DPAs to monitor independently the compliance with EU law on the protection of individuals with regard to the processing of personal data (Hoffmann, 2016, pp. 10-11). Therefore, the DPAs "must be able to examine, with complete independence, any claim concerning the protection of a person's rights and freedoms in regard to the processing of personal data relating to him" (Judgement C-362/14 l. 99).

As the General Advocate in his Final Opinion, the ECJ decided that the Commission did not evaluated the circumstances in the US sufficiently (Judgement C-362/14 l. 97). In its decision the Commission just considered the Safe Harbor Principles and did not take American data protection laws into account. However, according to Art. 25 (6) an Adequacy Decision has to be made on the basis of the "domestic law or of the international commitments [a country] has entered into". Consequently, it was impossible for the Commission to acknowledge that the US did indeed ensure an adequate level of protection, hence Art. 1 of the *Safe Harbor* Decision was judged to be invalid (Hoffmann, 2016, p. 11). Moreover, the ECJ criticized that the Commission Decision does not take into account the circumstances that have arisen after thae adoption of the decision (Judgement C-362/14 l. 77). Which can be interpreted as a clear reference to the revelations by Mr. Snowden.

Furthermore, the ECJ criticized the self-certification mechanism of *Safe Harbor* and emphasized the importance of effective monitoring and control mechanisms, which allow authorities to identify and prosecute any violations to privacy rights. Nevertheless, the ECJ did not rule out an Adequacy Decision on the basis of self-certification mechanisms in general. The Court rather points out, that the control mechanisms of a third country can differ to these applied in the EU and a system of self-certification does not infringe the requirements of Art. 25 (6) DPD inevitable (Judgement C-362/14 l 81).

Moreover, the ECJ condemned that the *Safe Harbor* decision makes fundamental rights violations possible (Judgment C-362/14 l. 87). In particular in the right to

privacy laid down in Art. 7 CFR and the fundamental right to protection of personal data guaranteed by Art. 8 CFR are at risk. A violation of these rights is possible as the decision allows exceptions to the *Safe Harbor* principles when national security, public interest or criminal prosecution is at stake. Consequently, *Safe Harbor* certified companies are obliged to ignore the principles of the agreement if they could conflict with these exceptions. The court stressed, that the Adequacy Decision did not include a statement whether there were any US regulations which limit such interventions (Judgment C-362/14 l. 89). Additionally, the Commission itself found, in its Communication concerning the *Safe Harbor* Agreement, that the US authorities processed personal data of EU citizens in a way which was incompatible with the principle of purpose limitation and was not proportionate to the protection of national security (Hoffmann, 2016, p. 12). This statement is also a harsh condemnation of the surveillance practices by the NSA, which according to the judges misused the exceptions of *Safe Harbor*.

According to the ECJ, a law which restricts the fundamental rights guaranteed by the CFR has to provide clear and precise rules for the requirements and the application of such an intervention. This is necessary to effectively protect personal data against misuse and unauthorized access. The court explicitly points out that the risk of a violation is much higher when personal data is processed automatically (Judgment C-362/14 l. 91). Furthermore, the court stressed that, the protection of privacy rights "requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary" (Judgment C-362/14 l. 92). Therefore, a general monitoring and storage of personal data, as the NSA demonstrably did, is illegal (Judgment C-362/14 l. 93). Such practice does not make any differentiation, restriction or exception on the basis of the objective pursued. Neither does it contain a provision which would limit the access of authorities to personal data, moreover the access is not limited for a specific purpose, which could justify such interventions. Consequently, it is a violation of Art. 7 CFR (Hoffmann, 2016, pp. 12-13). This assessment by the court can be also understood as a clear critique of the surveillance practices by the NSA.

Additionally, the Court criticized that in the *Safe Harbor* Decision the Commission failed to establish effective judicial protection against possible infringements of privacy rights. The monitoring instruments by the FTC "are limited to commercial

disputes" and the *Safe Harbor* principles "cannot be applied in disputes relating to the legality of interference with fundamental rights that results from measures originating from the State" (Judgement C-362/14 l 89). In the light of the revelations by Mr. Snowden this can be understand as a reference to the surveillance programs by the NSA. Furthermore, there are in fact no judicial possibilities for individuals who are affected by a violation of their rights to access correct or delete their personal data. This deficit was also observed by the Commission in its Communication (Judgement C-362/14 l 90.). This means an infringement of the access principle enshrined in Art. 12 DPD and the *Safe Harbor* Agreement. Moreover, a provision which does not provide such possibilities is incompatible with Article 47 CFR, which guarantees the right to an effective remedy and to a fair trial (Judgement C-362/14 l 95).

Moreover, the ECJ annulled Art. 3 of the *Safe Harbor* Decision (Judgement C-362/14 l 102-104) on the grounds that it limits the requirements for intervention by the national DPAs in the case of an infringement, such as the suspension of data transfers to a third country. The Court pointed out that, these powers are necessary for the DPAs to fulfill their duties in accordance with Art. 28 DPD and Art. 8 CFR (Judgment C-362/14 l. 99). Furthermore, it stressed that Article 25 (6) DPD did not authorize the Commission to restrict the powers of national DPAs. Consequently, the Commission exceeded its competence (Hoffmann, 2016, pp. 13-14). With this assessment the ECJ again underlined the independence of the national supervisory authorities.

Finally, the court annulled the entire Safe Harbor Decision. It found that the invalid Art. 1 and 3 are inextricably linked to Art. 2 and 4 and to the Annex of the *Safe Harbor* Decision, which consequently makes a further existence of the Agreement impossible (Judgment C-362/14 l. 105).

3.4 Conclusion of the Chapter

After having analyzed the Schrems case in detail, the principles and rules emerging from the ECJ judgment are summed up in the following. First, the EJC judgement emphasizes the independence of the national DPAs and strengthens their competences. Second, the court stresses that for a sufficient Adequacy Decision, domestic law and international commitments a country has entered have to be considered in the decision-making process. Third, the need for effective monitoring and control of the self-

certification mechanism is underscored. According to the judgement, the NSA scandal also emphasized the necessity of effective restrictions of unauthorized access to personal data and other fundamental rights violations. Finally, the Court demands the establishment of a framework ensuring effective legal protection of the privacy rights of European citizens.

With the judgement the ECJ sets a high standard for the transfer of personal data to third countries. The court defines clear guidelines on how to ensure sufficient guarantees for effective data protection. Thus, it has made an unambiguous statement that an effective and adequate protection of personal data of EU citizens to a third country requires more than a self-certification mechanism.

Taking into account the results from the previous chapter, the court addresses the identified weaknesses of the data protection framework, such as the unclear role of the DPAs or the insufficient control mechanisms, as well as the soft rules for sanctions of the legal framework.

The judgement - with its resulting implications – has challenged the data protection framework of the EU. Thus, the existing framework needed to be revised. Already during the trial, EU and US authorities began to negotiate a replacement agreement, which resulted in the *Privacy Shield*. On July 12th 2016, the European Commission adopted the *Privacy Shield*. This agreement has been the initial step for many developments within the European data protection framework since the judgement. In this regard, the replacement of the DPD by the GDPR has been the most discussed as it has gained much public attention. In addition, the Commission announced its intention to revise the ePD. In the next chapter, the current data protection framework of the EU is analyzed to evaluate the impact of the judgement C-362/14 l 81.

4. The EU data protection framework after 2015

Before the main RQ can be finally answered it is necessary to answer the last *SQ 3: What are the innovations brought by the new European data protection policies to the data protection framework of the EU?* Therefore, the current framework and proposals for upcoming changes are presented at length and analyzed in this chapter.

Since the judgment, the EU data protection framework was significantly changed. Already in 2003, a review of the EU Member States data protection law, according to the DPD, revealed many different possibilities of national interpretation (Hustinx, 2013, pp. 24-25). In addition, developments like the Schrems case showed the need for innovation.

In comparison to the previous framework described in chapter two, three changes are striking: First, as mentioned before, the *Safe Harbor* Agreement was replaced by the *Privacy Shield*. Second, the DPD got replaced by the GDPR and third, the EU also announced to replace the ePD with a regulation, the so called ePrivacy Regulation (ePR). The other laws, which composed the data protection framework before 2015, are unchanged since the judgment and still applicable. Moreover, no additional privacy laws were enacted in the EU after 2015, thus it is, for the purpose of this paper, sufficient to analyze the three changes uttered above. However, it is worth mentioning that in December 2018 the Directive 2018/1972 has been adopted, setting up a European Electronic Communications Code (EECC). The Directive deals with technological provisions and takes recent market and technology changes in the electronic communications sector into account; thus, the ePR is linked to the EECC.

The immediate consequence of the judgement was the abolition of the *Safe Harbor* Agreement and the implementation of the new *Privacy Shield*, which regulates the data transfer from the EU to the US today. Furthermore, the Commission worked more than four years to improve the DPD, which resulted in the General Data Protection Regulation adopted in April 2016 and being effective from the 25thof May 2018 onwards (Hoffmann, 2017, p. 5). The GDPR harmonizes the various data protection legislation in the EU Member States, since the legal form of a regulation does not allow any discretion for the Member States but only the application of common EU law.

Moreover, the Commission presented a proposal for a Regulation concerning the respect for privacy and the protection of personal data in the electronic communications sector (the ePR) which should replace the ePD. In the following, first the principles of the *Privacy Shield* are presented, subsequently the GDPR and the proposal of the ePR are summarized and analyzed.

4.1 The Privacy Shield

Already during the beginning of the Schrems case, in November 2013, the European Commission published a recommendation to improve the *Safe Harbor* Agreement. The recommendation aimed at: "enhancing transparency; ensuring redress; strengthening enforcement; and limiting the access of US authorities to data transferred under Safe Harbor" (Weiss & Archick, 2016, p. 9). Subsequently, the EU and US officials began to negotiate a new agreement. In February 2016, the *Privacy Shield* and its supporting documentation were released. The new framework is substantially longer and more detailed than the preceding *Safe Harbor* Agreement.

As *Safe Harbor*, the *Privacy Shield* consists of a set of regulations: the agreement itself and an Adequacy Decision by the European Commission. Moreover, it includes guarantees by the US federal government that are published in the US Federal Register. Even though the principles remained basically the same compared to the *Safe Harbor* Agreement, the provisions to enforce these principles are now much stricter and described in more detail:

First, according to the Notice Principle, the data controller must still inform the subject about the collection of data and the intended purpose, as well as about potential third parties to whom the data is accessible. In contrast to *Safe Harbor* the controller is now obliged to inform the data subject about his rights, in particular the right to access and the right of choice. Furthermore, companies are required to make their privacy policies public (Privacy Principles 20).

The provisions of the Data integrity and Purpose Limitation Principle stayed basically the same (Privacy Principles 23). The same applies for the Choice principle. Furthermore, collected personal data must be still stored securely by the data controller. However, the *Privacy Shield* extends this provision to third parties to whom the data might get transferred, in this case the data controller must conclude a contract with the third party guaranteeing the same level of security (Privacy Principles 24).

Additionally, under the *Privacy Shield* data subjects have the right to obtain information from the data controller, if personal data relating to them were processed within reasonable time. Furthermore, data subjects must still be "able to correct, amend or delete personal data where it is inaccurate or has been processed in violation of the Principles" (Privacy Principles 25). In contrast to the *Safe Harbor* Agreement the

Privacy Shield relates directly to US law in the context of automated processing of personal data, which can be used to take decisions affecting the data subject. The Access principle acknowledges that under "U.S. law individuals have the right to be informed of the specific reasons underlying the decision" (Privacy Principles 25). A close coordination in the regard of automated decision-making between EU and US authorities is announced (Privacy Principles 25).

Next, according to the Recourse, Enforcement and Liability Principles, companies and organizations which commit to adhere to the principles of the *Privacy Shield* have to guarantee compliance with the principles, therefore they need to implement "robust mechanisms". Moreover, participants of the *Privacy Shield* must put in place effective redress mechanisms to deal with complaints of data subjects and subject themselves to the investigatory and enforcement powers of the FTC, the DOT or another US authorized body that will ensure compliance with the principles (Privacy Principles 26). These redress mechanisms include determined timelines by which US companies must respond to complaints and grant the data subject the ability to report complaints directly to the responsible national EU data protection authority. In case complaint is not resolved in this way, the *Privacy Shield* requires companies to commit to binding arbitration in order to resolve the complaint of the data subject (Privacy Principles 42).

Finally, the onward transfer of personal data is, as defined in the *Safe Harbor* Agreement, only allowed "(i) for limited and specified purposes, (ii) on the basis of a contract […] and (iii) only if that contract provides the same level of protection as the one guaranteed by the Principles" (Privacy Principles 28). If personal data is transferred to a third party the subject has to be informed about it and according to the Choice Principle has to have the opportunity to contradict the transfer (Privacy Principles 28). Anyhow, the *Privacy Shield* extends the obligation to provide the same level of data protection as required by its Principles to all third parties data is transferred to, as well as to further third parties which receive the data from the first third party. In all cases, a contract with the third party recipients must ensure that every third party involved in the processing of the data will ensure the same level of data protection as granted by the *Privacy Shield*. Moreover, the third parties have to notify the *Privacy Shield* registered organization, from which they received the data, if they make any change to their handling of personal data, which could be in conflict with the principles of the *Privacy Shield*. (Privacy Principles 29).

Similar to the *Safe Harbor* Agreement, American companies have to register themselves to comply with the *Privacy Shield* in order to transfer data from EU citizens to the US. In contrast to the old agreement, the verification process is supervised by an Ombudsperson who should advise companies, which would like to register for the agreement, in meeting the requirements (Annex A).

In case of a possible infringement of privacy rights or any other conflict, EU citizens can ask the newly established Ombudsperson at the US Department of Sate to investigate whether a company has violated the principles of the *Privacy Shield*. All investigations of the Ombudsperson are publicly available in the US Federal Register (Annex A). The Ombudsman is a US State Department official, he is supposed to cooperate closely with other independent supervisory authorities on US and EU side, including the bodies which are responsible for overseeing the American intelligence agencies (Annex A). Moreover, EU citizens have also the right to contact US companies directly. Complaints have to be dealt with within 45 days. Additionally, citizens can also turn to their national DPA, which has to investigate complaints in cooperation with the FTC (Privacy Principles 45).

Furthermore, the American side has guaranteed, for the first time in written form, the European Commission to take effective supervisory measures against any violation of the principles of the *Privacy Shield* (Privacy Principles 125). Moreover, the US offials have given assurance to the EU authorities that access to personal data of EU citizens of intelligence services for national security purposes should be subject to clear restrictions, guarantees and oversight mechanisms (European Commission, 2016).

Another innovation of the *Privacy Shield* is that the European Commission has to produce an annual report on the functioning of the *Privacy Shield* and forward it to the European Parliament and the European Council. The review is published by the Commission together with the US DOC. In the review process experts from the US and the European DPAs should be involved (Privacy Principles 145-148). On the basis of the annual review, the Commission publishes a report to the European Parliament and the Council (Privacy Principles 149).

In conclusion, the new agreement promotes several new innovations wich have been presented in detail. In the following, the latter change to the EU data protection framework – namely the replacement of the DPD by the GDPR - is analyzed.

4.2 The GDPR

The GDPR has been adopted in 2016 and became effective from the 25th of May 2018, after a two-year transition period. One main reason for the reform of the DPD was the different implementation and application in the Member States, which led to different standards of data protection (Hustinx, 2013, pp. 24-25). By changing from a directive to a regulation, the EU wanted to reduce the existing legal uncertainty (Preamble 13 GDPR). As, in contrast to the DPD, the GDPR does not require implementation into national law.

The GDPR develops the terminology and policies of the DPD further. Like the DPD, it applies to the processing of personal data; it uses the same definitions for personal data, processing, data subject, and data controller (Art. 4 GDPR). However, it introduces new terms such as profiling and pseudonymisation. Profiling is any form of automated processing of personal data, in particular data concerning work performance, wealth, health, personal interests and movements, which allows to create a profile of the data subject (Art. 4 (4) GDPR). These profiles can be used to analyze or predict the behavior of the subject. Pseudomynisation means that the personal data is processed in a manner in which the data can no longer be attributed to a specific data subject without the use of additional information. Therefore, this required information must be kept separately and secure against unauthorized access (Art. 4 (5) GDPR).

In general, the GDPR applies whenever personal data is processed in the entire private and public sector in the EU. However, it does not apply to the processing of personal data for private or family purposes. Moreover, it does not apply to data processing by EU Member States in the context of the Common Foreign and Security Policy, by police and judiciary which is regulated in the Directive [(EU) 2016/680] and for processing by the EU institutions, in that regard Regulation [(EC) No 45/2001] applies (Art. 2 GDPR). The conditions for exceptions for the provisions of the GDPR are the same as for the DPD described in chapter two.

As defined in the DPD, the processing of personal data is only allowed if it is based on a legal basis. This is the case, if one of the provisions of Art. 6 GDPR is fulfilled (Art. 6 GDPR). The conditions for a legal transfer of personal data enshrined in Art. 6 GDPR remained the same as in Art. 7 DPD. Additionally, the legal basis can now also be derived from other Union law or national law, insofar as the GDPR refers to it (Art. 6 (3) GDPR). Also the principles of Art. 6 DPD are still applicable, as personal data

may only be collected for specified and legitimate purposes and it is only allowed to process the data according to the original purpose (Art 5. (1) GDPR). Furthermore, the GDPR uses the same definition for special categories of personal data as the DPD, but adding genetic and biometric information to these categories. This kind of data has a special level of protection; in the case of processing such data the same provisions as described in chapter 2.1 apply (Art. 9 GDPR).

Additionally the GDPR emphasizes the importance of consent for the transfer of personal data, as two articles are dedicated to this topic: Consent must be given voluntarily, informed and unambiguous for a specific case (Art. 4 (11) GDPR). Moreover, the data subject must have the opportunity to withdraw the consent at any time (Art. 7 (3) GDPR). The consent has to be given by an explanation or another clearly confirming act (Art. 4. (11) GDPR). The conditions for a voluntary consent have been redefined. Accordingly, it is essential to consider whether the performance of a contract depends solely on the consent to the processing of personal data (Art. 7 (4) GDPR). Thus, consent is not given voluntarily if a data controller makes the performance of a contract inextricably linked to the granting of consent, even though the data processing is not necessary for the performance of the contract.

According to the GDPR, the data controller is required to be able to demonstrate the consent of the data subject (Art. 7 (1) GDPR). Witten consent statements must be transparent and clearly understandable (Art. 7 (2) GDPR). Finally, the GDPR considers children to be capable of consent only from the age of sixteen onwards. However, the Member States can lower this age to thirteen years. Providers of internet services which address children directly are only allowed to process data from younger children if they first obtain parental consent (Art. 8 (1) GDPR).

4.2.1 Rights of data subjects

Like the DPD the GDPR grants the data subject's rights to transparent information about the collection of his or her personal data (Art. 12, 13, 14 GDPR). In the case of automated decision making, explicitly including profiling, the data subject has the right to be informed about the logic of the processing and the consequences for him or her (Art. 13 (2), 14 (2) GDPR). Moreover, the data subject has the right to be informed about any potential data breach which could put his or her privacy rights at risk (Art.

34 (1) GDPR). Furthermore, he or she enjoys the same information rights as granted before - by the DPD (Art. 15 GDPR). Consequently, the data subject may still demand from the controller the immediate correction of incorrect data, or the supplementation of incomplete data (Art. 16 GDPR).

Moreover, the GDPR introduces the "right to be forgotten". According to that, the data subject is entitled to demand his or her personal data to be deleted, if the data is no longer necessary for processing purposes, if there is no legal basis for the processing because it was based on a consent which the data subject withdrew or if he/she has objected to the processing of his or her data for direct marketing purposes (Art. 17 (1) GDPR). The data must also be deleted, if the data processing violated the principles of the GDPR or if the data controller is legally obliged by Union or Member State law to delete it (Art. 17 (1) GDPR).

Additionally, he/she has – under certain conditions – the right to demand that the controller restrict the processing of his or her data (Art. 18 GDPR). If the data controller processed the data for a legitimate reason stated in Art. 6 GDPR, the data subject has the right to object to the processing of his or her data for personal reasons. However, if the data controller has compelling reasons for the processing, such as public interest or the exercise of official authority, he/she is allowed to process the data, if he/she demonstrates legitimate grounds, which outweigh the interests, rights and freedoms of the data subject, or if the data is needed for legal claims (Art. 21 (1) GDPR). If personal data is processed for direct marketing purposes, the data subject can object to the processing of his or her data at any time and without restriction (Art. 21 (2) GDPR).

What's more, the GDPR provides the opportunity for data subjects to file a complaint directly to the supervisory authorities, if he/she is concerned that the processing of their personal data by a data controller/processor violates the principles of the GDPR (Art. 77 (1) GDPR). Accordingly, the data subject has the right to contact the DPA of the Member State where he/she lives, no matter in which Member State the possible infringement was committed (Art. 77 (1) GDPR). In addition, the data subject has the right to an effective judicial remedy against a supervisory authority or data controller and processors, in case of a legal conflict (Art. 78, 79 GDPR). Moreover, the GDPR allows, in cases of legal complaints or judicial remedies, the EU-wide legal

representation of the affected data subject by certain non-profit organizations such as consumer associations (Art. 80 (1) GDPR). Furthermore, the GDPR introduces the possibility for such organizations to file collective claims in the name of the data subjects (Art. 80 (2) GDPR). In case a data subjects suffers damage caused by a violation of his or her privacy rights, he/she has the right to receive a compensation by the responsible controller/processor. The GDPR explicitly incudes immaterial damages to this compensation right (Art 82 (1) GDPR).

Additionally, the GDPR introduces another new right with the right to data portability (Art. 20 GDPR); whenever data processing is automated or based on consent or contractual relationship, the controller must – at request of the data subject – provide the data to the data subject or, if desired and technically feasible, directly to another controller (Art. 20 GDPR). However, the right does not exist if the processing is carried out in public interest or in exercise of official authority (Art. 20 (3). GDPR).

Furthermore, the GDPR addresses explicitly automated processing and profiling; the data subject may refuse to be subjected to a decision – based on automated processing including profiling – which has legal effects on him or her (Art. 22 (1) GDPR). Exceptions apply, if the decision is permitted by Union or Member State law or is necessary for the performance of a contract or if the person concerned explicitly agreed (Art. 22 (2) GDPR). In these cases, the data controller must take appropriate measures to protect the rights, freedoms and interests of the persons concerned (Art. 22 (3) GDPR).

4.2.1 Obligations for data controllers and processors

As the DPD the GDPR contains obligations for the data controllers and processors. First, they have to obey the same principles as defined in Art. 6 DPD (Art. 5 (1) GDPR). However, from now on the data controller is responsible for demonstrating compliance with those principles (Art. 5 (2) GDPR). This obligation requires the data controller to submit comprehensive documentation to the national DPAs. If he/she cannot proof the compliance, high fines are at risk (Art. 83 (5) GDPR). Furthermore, according to the principle of data integrity and confidentiality, the GDPR obliges data controllers and processors to take appropriate technical and organizational measures to ensure a sufficient protection of personal data (Art. 5 (1) GDPR). In contrast to the

DPD, the GDPR specifies these safety measures (Art 32 GDPR). Accordingly, personal data should be pseudonymised and encrypted (Art. 32 (1) GDPR). Additionally, controllers and processors must ensure the confidentiality, integrity, availability and resilience of their systems and services on a permanent basis and are required to restore data availability and access in the event of an incident as fast as possible (Art. 32 (1) GDPR). Moreover, they must implement procedures for a regular review of their security measures (Art. 32 (1) GDPR).

In addition, all data controllers and processors with at least 250 employees are required to maintain a record of all their data processing activities and make it available to supervisory authorities upon request (Art. 30 (1, 2, 4) GDPR). This includes the purposes of processing, the categories of personal data, data subjects and recipients and the security measures taken to protect the data (Art. 30 (1), (2) GDPR).

In comparison to the DPD the GDPR provides a much more comprehensive catalog of information which the data controller must provide to the data subject (Art. 13, 14 GDPR). Foremost, the controller must provide the data subject with the contact details of him or her and of the responsible data protection officer (Art. 13 (1), 14 (1) GDPR). Furthermore, the controller has to be able to present the legal basis of the data processing and – if this is the case – of the transfer of the data to a third country (Art. 13 (1), 14 (1) GDPR). If the data is collected directly from the data subject, the controller may also have to indicate his legitimate interests, which is the basis for the processing (Art. 13 (1) GDPR). If the data is collected from the data subject indirectly, the controller must provide additional information about which data categories he/she processes (Art. 14 (1) GDPR). In both scenarios the controller must provide further information, about the nature of the processing and the rights of the data subject, to the extent which is necessary for fair and transparent data processing (Art. 13 (2), 14 (2) GDPR). If the data is not collected from the data subject directly the controller must also indicate the source of the data (Art. 14 (2) GDPR). Additionally, if the data is obtained directly, the data subject may have to be informed why he/she is obliged to provide the data and what would be the consequence of non-providence (Art. 13 (2) GDPR). However, if the data processing is based on a given consent, the controller must clarify this and inform the concerned person that he/she has the right to withdraw the consent (Art. 13 (2), 14 (2) GDPR). Moreover, information has to be provided if the original purpose of the processing is changed by the controller (Art. 13 (3), 14 (4)

GDPR). If the personal data is collected indirectly from the data subject, these provisions may be waived if the expenses are disproportionate, if the data is confidential or if legislation specifically requires the collection of the data (Art. 14 (5) GDPR). All provided information must be available in written form and communicated in a clear and simple language (Art. 12 (1) GDPR).

A new feature of the GDPR is the obligation to inform the data subject and the responsible national DPA about data breaches, which could pose a threat to the privacy of the individual (Art. 33, 34 GDPR). A notification to the supervisory authority must be made in any case within 72 hours, otherwise the delay must be justified reasonably (Art. 33 (1) GDPR). The affected data subject has to be informed without any undue delay, if the data breach is likely to pose a risk to their privacy rights (Art. 34 (1) GDPR). In exceptional cases, reporting to the DPAs is not required, if the data controller can prove that, despite the data breach, there are no risk to the rights and freedoms of the data subject (Art. 33 (1) GDPR). The information of the data subject is not necessary if the controller can proof that he/she implemented appropriate technical measures which guarantee the security of the personal data (Art. 34 (1) GDPR).

Another innovation of the GDPR is the obligation for data controllers to carry out a data protection impact assessment in advance of the processing, if it is likely to put a high risk to the rights and freedoms of the affected persons (Art. 35 GDPR). Such an impact assessment must be carried out, in the case of automated data processing including "profiling", if a large scale of special categories of personal data should be processed (Art. 9 GDPR) or if an extensive video surveillance of a public area is planned (Art. 35 (3) GDPR). If the impact assessment concludes that the processing would put a risk to privacy rights, the controller must consult the responsible supervisory authority and take measures to mitigate the risk (Art. 36 (1) GDPR).

Additionally, the GDPR requires controllers and processors to appoint an internal data protection officer who monitors compliance with data protection obligations, advises the data controllers or processors and communicates with the supervisory authority (Art. 37, 39 GDPR). This obligation applies in particular to public bodies, but also to certain non-public bodies which mainly deal with the performance of data-processing operations (Art. 37 (1) GDPR). Moreover, the GDPR encourages data controllers and processors to implement a code of conduct for the handling of personal data in

accordance with the GDPR. These rules can be certified by the supervisory authorities or other independent accredited bodies and establish a legal basis for the processing of personal data (Art. 40, 41, 42, 43 GDPR).

4.2.2 Application and enforcement

Furthermore, the GDPR introduced innovations to ensure a unionwide application of the GDPR: First, the European Data Protection Board (EDPB) has been established as an independent EU body with legal personality (Art. 68 GDPR). It replaces the Art. 29 Data Protection Working Party and has more powers than the predecessor. The EDPB is composed of the head of a supervisory authority of each Member State and the European Data Protection Supervisor (Art. 70 GDPR). The main tasks of the EDPB is to advise the Commission on data protection issues and draw up guidelines, recommendations and procedures about the concrete application of the GDPR (Art. 70 GDPR). Thereby, the EDPB has the power to interpret the provisions of the GDPR and to determine the concrete application of it. Moreover, the EDPB also has a final decision-making right in certain disputes between national supervisory authorities (Art. 65 GDPR).

Second, as required by the DPD, each Member State must set up at least one data protection supervisory authority which is responsible for monitoring the compliance with the GDPR in the individual Member State (Art. 51 (1), 55 (1) GDPR). However, the role of the national supervisory authorities as an independent monitoring body is strengthened by the GDPR, as their tasks are now described in a more detailed way. From now on the DPAs need to inform the public about risks associated with processing of personal data in the EU and inform data controllers and processors about their obligations according to the GDPR (Art. 57 (1) GDPR). Furthermore, they must deal with complaints and enforce the GDPR if necessary (Art. 57 (1) GDPR). Moreover, they must investigate any possible violation of the GDPR upon request and should keep track of recent developments of information and communication technologies if they could pose a risk to privacy rights (Art. 57 (1) GDPR).To ensure consistent application, the national DPAs should cooperate with each other and with the Commission (Art. 51 (2) GDPR). Therefore, the GDPR includes an individual chapter on cooperation between the national supervisory authorities. Accordingly, new cooperation and coherence mechanisms are designed to ensure a unionwide

application of the GDPR and prevent the establishment of data protection loopholes (Art. 64, 65 GDPR). In case of a conflict the DPA where the data controller has its main place of business is responsible. Thus, in cross-border data processing, data controllers no longer have to deal with different jurisdictions in individual Member States.

Third, the possibility of imposing sanctions has been harmonized and is much stricter under the GDPR. In the event of a violation of organizational regulations, fines of up to EUR 10 million, or 2% of the global annual turnover, can be imposed (Art. 83 (4) GDPR). For violations of data protection principles, patent rights, the rules on the lawfulness of data processing or failure to comply with instructions from the DPAs, the fines may amount up to EUR 20 million or 4% of the worldwide annual turnover (Art. 83 (5), (6) GDPR).

4.2.3 Data transfer to third countries

Finally, the provisions for a data transfer to third countries were also reformed. The general principle for the transfer of personal data to third countries or to international organizations is still an adequate level of protection (Art. 44 GDPR). Accordingly, it has to be ensured that the level of data protection defined by the GDPR is not undermined. Therefore, the transfer of personal data to a third country shall continue to be authorized by the Commission in an Adequacy Decision. In this decision the Commission should take *inter alia* the domestic law and international commitments a country has entered into, the rule of law, the respect for human rights and the access of public authorities to personal data into account. Moreover the Commission should evaluate the existence and functioning of independent supervisory authorities (Art. 45 (2) GDPR). The GDPR requires the Commission to conduct a periodic review of their decision at least every four years, giving the EU officials the opportunity to react to relevant developments. In case of noncompliance the Commission can suspend the transfer of personal data (Art. 45 (3) GDPR). An adequacy decision is not needed, if there are other sufficient guarantees to compensate for the inadequate level of protection in the third country (Art. 46 GDPR). Such guarantees may arise from contractual arrangements between the data exporter and the data importer or binding corporate data protection regulations (Art. 47 (1), (2) GDPR).

As with the DPD and the ePD, the EU have had to complement the GDPR in the electronic communications sector. Since the implementation of the DPD new technologies have been developed. Thus, in 2017 the Commission published a proposal for the ePR which ought to adapt the provisions of the DPD to the altered reality. In the following, the principles and innovations of the ePR proposal are summarized.

4.3 The ePrivacy Regulation

On 10th January 2017, the Commission submitted a reform proposal for the ePD which should replace it with a "Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications" (Regulation on Privacy and Communication (ePR)). The proposal for the Regulation contains revised rules for the protection of fundamental rights and freedoms in the field of electronic communication, in particular the fundamental right for respect of privacy, the right of confidentiality of communication and the protection of personal data, which are *inter alia* granted by Art. 7 and 8 CFR.

With the proposal for the ePR the Commission aims at providing a consistent level of data protection across the EU Member States, for both natural and legal persons, while ensuring the free movement of electronic communications data, equipment and services (Art.1 ePR Proposal and 1.2. and 1.3. Context of the Proposal). As, the different implementation of the ePD in the individual Member States can be an obstacle for the free flow of communication data across the EU (3.1. Results of Ex-post Evaluations). Unlike the previous Directive, the new ePR will immediately apply without transition in Member State law and take precedence over any national laws. Additionally, the prospective Regulation should align the provisions in the field of electronic communication with the reformed EU data protection framework in order to avoid duplication and ensure coherence of EU legislation (1.2 and 1.3. Context of the Proposal). In this manner, the Commission intends to more effectively protect privacy and personal data (2.4. Legal Basis). Thus, the proposal for the ePR refers to various other legal acts, in particular the GDPR (e.g. Art. 4). Moreover, the aim of the Commission is to adapt the provisions of the ePD to the altered technical and economic

reality (1.1. Context of the Proposal). In the following the important provisions of the proposal are presented:

The Proposal uses similar definitions as the ePD and refers directly to terms used in other laws such as the GDPR and the EECC. Additionally the ePR introduces new definitions – central is the term of "electronic communications data" which includes both the "contents" and the "metadata" of electronic communications (4 (3) ePR Proposal). Electronic communications content refers to the actual content exchanged by means of electronic communications services, such as text, voice or videos. Electronic communications metadata means data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content, this includes e.g. data about the physical source and destination of a communication as well as the date, time and duration of a communication (Art. 4 (3) ePR Proposal).

The ePR will apply whenever electronic communications data is processed to provide electronic communication services in the EU. Moreover, it will apply for the protection of information about the end user (Art. 2 (1), (2) and Art. 3 (1) ePR Proposal). As the GDPR, the Regulation will also apply if the processing itself is carried out outside the EU. Thus, the only requirement for this protection is that the end-user is located in the EU (Art. 3 ePR Proposal). Accordingly, companies which are not based in the EU must designate a representative in the EU who acts as a contact person for customers and supervisory authorities (Art. 3 (2) ePR Proposal). In contrast to the ePD the Proposal includes Over-the-top (OTT) services services in the scope of the law. OTT services are service which provide a product over the Internet and bypass traditional distribution. OTT services are often related to media and communication. Examples include Netflix or similar video streaming services as well as Facebook, WhatsApp and Skype or similar services (1.3. Consistency with other Union policies)

Firstly, the ePR prohibits any interference of electronic communication, such as monitoring, storage, tapping or scanning of electronic communication (Art. 5 ePR Proposal). Accordingly, it should be prohibited to store files on the end users device which can be used to collect information about him or her (e.g. cookies) without the end user's consent (Art. 8 (1) ePR Proposal). In contrast to the ePD, end-users should not only be protected against cookies, but also against new tracking techniques that do

not require access to the end-user's device. Such tracking methods monitor data which is send from the end users device in order to connect to a service or network. In this way, individuals can be tracked which can pose a threat to their privacy (ePR Preamble 25).

Moreover, the new Regulation also strengthens protection against unsolicited direct communication known as Spam. In comparison to the ePD the term "direct mail" is extended to cover not only commercial advertising for the supply of goods or services, but also election advertising by political parties or advertising by non-profit organizations (ePR Preamble 32). Direct mail are only allowed if the user gave his or her prior consent, which must be easily revocable at any time. (Art 16 ePR Proposal).

Additionally, every service provider is obliged to inform the user about the privacy settings when using their service (Art 10 (2) ePR Proposal). As regulated by the GDPR the ePR will require the service providers to inform the users about any potential risk to their privacy (Art. 17 ePR Proposal).

According to the Proposal, the same national supervisory authorities will be responsible for monitoring and enforcing the GDPR and the ePR in all EU Member States. (Art 18 (2) ePR Proposal). Consequently, the EDPB established under the GDPR has the task of ensuring consistent application of the new Regulation. Moreover, it will advise the Commission on future amendments of the ePR and examine issues regarding the application of the Regulation (Art. 19 ePR Proposal). The remedies, the liability rules and the sanctions are also largely aligned with the corresponding regulations in the GDPR. Like the GDPR, the EPR contains tiered fines for diferent violations. For example, the penalties for less serious infringements should be regulated by the Member States (Art. 23 (4) ePR Proposal). In the event of violation of the cookie regulation or the prohibition of unsolicited communications, fines of up to EUR 10 million or 2% of worldwide annual turnover of the service provider can be imposed (Art. 23 (2) ePR Proposal). Infringements of the principle of communication confidentiality or the unauthorized processing of electronic communications data can be punished with penalties of up to EUR 20 million or 4% of the global annual turnover (Art. 23 (3) ePR Proposal). However, as previously stated, the ePR is yet not effective. It is expected to be implemented by the end of 2019 (Eickmeier, 2018).

4.3 Conclusion of the Chapter

After examining the European data protection frame work after 2015, the last SQ*: What are the innovations brought by the new European data protection policies to data protection framework of the EU?* can be answered.

Regarding the EU-US data transfer the *Privacy Shield* increased the transparency of the legal framework as official authorities are obliged to make reports publicly available. Second, with binding restrictions for US authorities to access personal data of EU citizens, the level of protection is increased in general. In the same light, the threshold for granting data transfer to third countries is increased as well. In this regard, the access right is revised and a dispute mechanism is newly established. Moreover, through a closer cooperation between the DOC and the European DPAs an effective enforcement of the principles laid down in the agreement ought to be ensured. Another new aspect of the Privacy Shield is the annual review mechanism which requires the Commission to periodically review its decision on an adequate level of protection, allowing to take altered circumstances into account.

All in all, the GDPR introduces a series of innovations. First, by the implementation of the GDPR technological developments are now taken into account and it is explicitly referred to new practices, such as profiling, which can pose a threat to the right to privacy of individuals. Second, the importance of unambiguous consent is underscored. Third, with the "right to be forgotten" and the "right to data portability", two new rights for data subjects are established. According to the GDPR, European citizens are also able to file direct complaints to companies which are required to respond to complains within 45 days. In case of conflict with the provisions of the Regulation, non-profit organizations are now able to present collective claims in front of court. Furthermore, the legal basis for compensation of immaterial damage is included. With the establishment of the GDPR, official authorities are now required to document all data breaches and to inform the DPAs as well as effected individuals immediately if such have occurred. In certain cases, data controller are also required to carry out a Data Protection Impact Assessment.

To improve the application and enforcement of the provisions of the GDPR, the EDPB as a new monitoring and advisory body has been established. Cooperation mechanisms between the monitoring bodies have been strengthened. In addition, the GDPR increases the leverage of the DPAs by paving the way for imposing harsh sanctions if

the principles of the Regulation are violated. Finally, the GDPR specifies that - regarding data transfer to third countries – for a sufficient Adequacy Decision a review is at least necessary every four years.

Finally, the ePR - in comparison to ePD – provides several innovations. By shifting from a directive to a regulation, consistent application of the rules regarding electronic communication across the Member States ought to be ensured. A significant change is the inclusion of OTT services, as these services have not been previously regulated under ePD. The usage of OTT services is constantly growing; hence, their inclusion to the provisions is of major importance for the general public. In addition, the cooperation between DPAs and the newly established EDPB ought to improve enforcement mechanisms on European level. Meanwhile, the application of sanctions is clearly defined.

5. Conclusion

After having provided answers to all SQs in the previous chapters, it now possible to answer the main RQ: *To what extent do the EU data protection policies reflect the principles upheld in the judgement of the Schrems case?*

The central principles of the EU data protection framework before the Schrems case were, *inter alia*, every individual had to consent to the processing of his or her personal data, the use of data was limited to the original purpose and personal data had to be stored secure against unauthorized access. In case of data transfer to a third countries, an adequate level of protection had to be ensured.

The judgement of the Schrems case demanded a strengthening of the competences of the DPAs, as well as strict monitoring and enforcement mechanisms to ensure legal protection of privacy rights. In addition, the Court stressed the necessity of evaluating the legal data protection framework of third countries for a sufficient Adequacy Decision. The importance of effective restrictions of unauthorized access to personal data and other fundamental rights violations has been underscored as well.

The analysis of the current data protection framework showed that the central principles of the data protection framework before the Schrems case are still the basis of the current legislative framework. Beyond these principles, the reforms which have

been conducted since the Schrems judgement introduced several innovations. With the introduction of the Privacy Shield, binding restriction for US authorities to access personal data of EU citizens are provided for the first time. Moreover, the provisions of the Privacy Shield are also applicable to all third party data transfers. Contractual agreements with these third parties ought to grant an adequate level of data protection.

With the implementation of the GDPR, the data protection standard in the EU has been further increased. The need for unambiguous consent has been stressed and the GDPR introduced new rights for the data subject. Furthermore, new dispute settlement mechanisms, strengthening the right of individuals, have been established. Moreover, data controllers are obliged to actively document compliance with the provisions of the GDPR. The competences of the DPAs are enhanced, as for example clear rules for imposing sanction in case of violations have been set up. In addition, infringements can be penalized with much harsher sanctions than it has been the case before. To be able to fulfill their task, the DPAs are supported by the new monitoring body, the EDPB.

With the upcoming ePR, the EU further fosters the reform of the data protection framework. A major innovation to the current framework is the inclusion of OTTs services, because they are of crucial importance as these are frequently used by the vast majority of European citizens.

Summing up, it is apparent that the European Commission has taken the principles upheld in the judgment of the Schrems case in the reforms of the European data protection framework into account. While the provisions of the data protection framework before the judgement of the Schrems case are still central today, the principles of the judgment have been implemented to a high extent. Thus, the Schrems case is significant for the current EU data protection framework.

However, the application of the principles of the Schrems judgement in practice is difficult to measure, due to the immense scope which the framework is covering. Huge companies like Amazon, Facebook or Google offer a wide variety of services subordinating them to different legislative provisions. This poses the risk of “watering down” the data protection standards upheld by the European data protection framework. Thus, a constant review of new technological developments as well as of the actual enforcement of the provisions is needed to ensure a defacto application of the principles emerging from the Schrems case. Finally, future developments will

determine whether, or not, the Schrems case can be considered a turning point for European data protection.

6. References

Arthur, C. (2011a, April 20th). *iPhone keeps record of everywhere you go*. Retrieved April 1st, 2019, from The Guardian: https://www.theguardian.com/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears

Arthur, C. (2011b, April 26th). *Windows Phones collect location data too, says Microsoft*. Retrieved April 1st, 2019, from The Guardian: https://www.theguardian.com/technology/blog/2011/apr/26/windows-phone-location-data

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17th). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. Retrieved April 1st, 2019, from The Guardian: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Carnevale, S. G. (2018, January 1st). *Europe's new data protection rules export privacy standards worldwide.* Retrieved April 1st, 2019, from POLITICO: https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/

Coudert, F. (2015, October 15th). *European Law Blog*. Retrieved April 28th, 2019, from Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for data protection authorities: 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/

Council of Europe. (2019a, April 8th). *Chart of signatures and ratifications of Treaty 108*. Retrieved April 8th, 2019, from Council of Europe: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=3HVyeWmJ

Council of Europe. (2019b, April 8th). *Details of Treaty No.108*. Retrieved April 8th, 2019, from Council of Europe: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

Eickmeier, F. (2018, February 2nd). *ePrivacy*. Retrieved July 2nd, 2019, from What does the ePrivacy Regulation mean for the online industry?: https://www.eprivacy.eu/en/about-us/news-press/news-detail/article/what-does-the-eprivacy-regulation-mean-for-the-online-industry/

European Commission. (2003). *Eur-Lex*. Retrieved April 27th, 2019, from First Report on the implementation of the Data Protection Directive (95/46/EC): https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:EN:HTML

European Commission. (2016, July 12th). *European Commission - Press release*. Retrieved June 23rd, 2019, from European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows: http://europa.eu/rapid/press-release_IP-16-2461_en.htm

References

European Commission. (2019, April 15th). *Countries and regions*. Retrieved April 28th, 2019, from United States: http://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/

European Union. (2018, 01 29). *europa.eu*. Retrieved 01 29, 2018, from https://europa.eu/newsroom/highlights/special-coverage/enlargement_en

European Union. (2019). *European Data Protection Supervisor*. Retrieved April 27th, 2019, from About: https://edps.europa.eu/about-edps_en

Fioretti, J., Nasralla, S., & Murphy, F. (2015, October 7th). *reuters.com*. Retrieved May 9th, 2019, from Max Schrems: the law student who took on Facebook: https://www.reuters.com/article/us-eu-ireland-privacy-schrems/max-schrems-the-law-student-who-took-on-facebook-idUSKCN0S124020151007

Garcia-Bernado, J., Fichtner, J., Takes, F. W., & Heemskerk, E. M. (2017, July 24th). Uncovering Offshore Financial Centers: Conduits and Sinks in the Global Corporate Ownership Network. *Scientific Reports*, 1-10.

Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. *International Data Privacy Law, Volume 2*(No. 2), 68-92.

Grennwald, G., MacAskill, E., & Poitras, L. (2013, June 11th). *The Guardian*. Retrieved May 11th, 2019, from Edward Snowden: the whistleblower behind the NSA surveillance revelations: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Hoffmann, A. (2016, April). „Privacy Shield“: Kein ausreichender Datenschutz im unsicheren Hafen USA. *cepStudie*, 1-62.

Hoffmann, A. (2017). EU-Datenschutzrecht - Ein Überblick über die bestehenden Vorschriften auf EU-Ebene und die aktuellen Reformbestrebungen der Kommission. *cepStudie*, 1-57.

Honduis, F. W. (1983, August). A Decade of International Data Protection. *Netherlands International Law Review, Volume 30*(Issue 02), 103-128.

Hustinx, P. (2013). EU Data Protection Law: The Review of directive 95/46/EC and the Proposed General Data Protection Regulation. *Collected courses of the European University Institute's Academy of European Law, 24th Session on European Union Law*, 1-12.

Kuner, C. (2016, November). The language of data privacy law (and how it differs from reality). *International Data Privacy Law, 6*(4), 259–260. doi:https://doi.org/10.1093/idpl/ipw022

MacAskill, E., & Dance, G. (2013, November 1st). *NSA Files: Decoded*. Retrieved April 1st, 2019, from The Guardian: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

Matera, C. (2016). *Writing a bachelor thesis in law in the EPA program at the University of Twente.* Enschede: University of Twente.

References

Meltzer, J. P. (2014). The Importance of the Internet and Transatlantitic Data Flows for U.S. and EU Trade and Investment. *Global Economy & Development, Working Paper 79*, 1-26.

Monteleone, S., & Puccio, L. (2017). *From Safe Harbour to Privacy Shield. Advantages and shortcomings of the new EU-US data transfer rules.* European Parliamentary Research Service.

Moses, L. B. (2007). Recurring Dilemmas: The Law's Race to Keep up with Technological Change. *Journal of Law, Tecnology & Policy, Volume 7*, 239-285.

O'brien, K. J. (2012, April 12th). *The New York Times*. Retrieved May 11th, 2019, from Facebook Offers More Disclosure to Users: https://www.nytimes.com/2012/04/13/technology/facebook-offers-more-disclosure-to-users.html

Pidd, H. (2011, October 20th). *The Guardian*. Retrieved May 11th, 2019, from Facebook could face €100,000 fine for holding data that users have deleted: https://www.theguardian.com/technology/2011/oct/20/facebook-fine-holding-data-deleted

Poitras, L. (Director). (2014). *Citizenfour* [Motion Picture].

Robinson, N., Graux, H., Botterman, M., & Valeri, L. (2009). Review of the European Review of the European. *RAND Europe*.

Schwartz, P. M. (1994). European Data Protection Law and Restrictions on International Data Flows. *80 Iowa L. Rev. 471*, 471-496.

Steel, E., & Fowler, G. A. (2010, October 18th). *Facebook in Privacy Breach*. Retrieved April 1st, 2019, from The Wall Street Journal: https://www.wsj.com/articles/SB10001424052702304772804575555848407523696 8

The Economist. (2017, May 6th). *The world's most valuable resource is no longer oil, but data.* Retrieved April 1st, 2019, from https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

US International Trade Administration. (2015, June 3rd). *export.gov*. Retrieved April 27th, 2019, from Instructions for Self-Certified Organizations on the Use of the U.S.–EU Safe Harbor Framework Certification Mark: https://2016.export.gov/safeharbor/eu/eg_main_018362.asp

WebWise Team. (2012, October 10th). *BBC*. Retrieved April 28th, 2019, from What are cookies?: http://www.bbc.co.uk/webwise/guides/about-cookies

Weiss, M. A., & Archick, K. (2016). U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield. *Congressional Research Service*.

Legal Documents

Charter of Fundamental Rights of the European Union

Data Protection Directive

ePrivacy Directive

Final Opinion of Advocate General in the case C-362/14

General Data Protection Regulation

Judgment C-362/14

Privacy Shield

Proposal for electronic Privacy Regulation

Safe Harbor Agreement

Treaty on the Functioning of the European Union

Universal Declaration of Human Rights