University of Twente
Faculty of Behavioral, Management and Social Science
Public Governance across Borders

First Supervisor: Dr. Claudio Matera
Second Supervisor: Dr. Martin Rosema

Bachelor Thesis

The European Commission's Strategy on Big Data and Human Rights and the Data Economy.

A case study on the significance of the Maximillian Schrems case.

Mischka Walten

5 July 2017
word count (text only): 22,458
word count (total): 25,182

KEY WORDS: Big Data, Data Protection, Right of Privacy, Digital Single Market, Data Economy, Maximillian Schrems

ABSTRACT

In times of digitalization big data becomes an increasingly more relevant topic for the European Union (EU) and its institutions as new technologies demand new regulations and reactions. The growing use of big data offers new chances and opportunities for businesses which may cause economic growth. At the same time, big data usage rises concerns regarding the privacy of individuals. The EU, known for high standards in the field of human and civil rights, follows the aim of ensuring privacy and safety and empowering the economy at the same time.

The research will analyze the relationship between the big data strategy of the European Commission (EC), the Digital Single Market (DSM) including the data economy, as well as the impact of the right of privacy on this field. The research is based on a case study which encounters the debate of big data usage and the infringement of the right of privacy. The case deals with the exchange of Facebook data between the EU and the United States of America (US) and has been brought to court by a private individual. The engagement with the US elaborates the difficulties of a transnational topic and dives into the idea of cross-border data flow and its effects. Through the investigation of the case study, the research enters into the current policy and regulatory framework and guides through the analysis of the compatibility of the EC's strategy on big data, human rights and the data economy. Once the internal strategy of the EU has been identified, the EU's external relations are analyzed with a focus on trade and partnership agreements with third countries. Next to the case study, the research is based on literature reviews and follows an explanatory, hermeneutic research design.

Table of Content

ABBREVIATIONS 5

1. INTRODUCTION.....6

1.1 Research question and subquestions 7

1.2 Body of knowledge, methodology, theory and conceptualization.....9

1.2.1 Body of knowledge 9

1.2.2 Methodology and theory 10

1.2.3 Conceptualization 11

1.2.3.1 Big data, the digital single market and the data economy.....11

1.2.3.2 Human rights and the right of privacy and data protection.....13

1.3 Social and scientific relevance 15

2. THE PRINCIPLES EMERGING FROM THE MAXIMILIAN SCHREMS CASE ON HUMAN RIGHTS AND THE DATA ECONOMY 16

2.1 The Safe Harbor Decision, the EU-US Privacy Shield and cross-border data transfers to third countries 16

2.2 The Maximillian Schrems case 20

2.3 Conclusion on the impact of the Maximillian Schrems case on the data economy 22

3. THE RELATIONSHIP BETWEEN THE EUROPEAN COMMISSION'S BIG DATA STRATEGY AND THE DATA ECONOMY 24

3.1 The European Commission's big data strategy, the Digital Single Market and the data economy.....24

3.1.1 The European Commission's communication from 2014 25

3.1.2 The European Commission's communication from 2017 27

3.2 The EU's interest in a data economy regarding relations to third countries.....28

3.3 Conclusion on the relationship between the European Commission's strategy on big data and the data economy 30

4. BIG DATA AND THE DATA ECONOMY THROUGH THE LENSE OF THE RIGHT OF PRIVACY 31

4.1 The general framework of the right of privacy and data protection 31

4.1.1 The General Data Protection Regulation 33

4.1.2 The proposal on the Regulation on Privacy and Electronic Communications 34

4.1.3 The Charter of Digital Fundamental Rights of the European Union 35

4.2 Unsolved privacy concerns and the data economy 37

4.3 Conclusion on privacy and data protection in the context of big data 38

5. THE EUROPEAN UNION'S INTERNAL STANDARDS IN REGARD WITH TRADE AGREEMENTS CONCERNING DATA-TRANSFERS WITH THIRD COUNTRIES 40

5.1 The European Union's internal standards and principles on trade relations with third countries 41

5.2 Recent Trade and Partnership Agreements with Third Countries 43

5.2.1 The EU-South Korea Free Trade Agreement 44

5.2.2 The Comprehensive Economic Trade Agreement between the European Union and Canada (CETA) 45

5.2.3 The EU-Singapore Free Trade Agreement (EUSFTA) 47

5.2.4 The EU-Japan Free Trade Agreement 48

5.2.5 The Transatlantic Trade and Investment Partnership between the European Union and the United States of America (TTIP) 49

5.3 Conclusion on the European Union's internal standards in regard with trade agreements concerning data-transfers with third countries 50

6. CONCLUSION ON THE EUROPEAN COMMISSION'S STRATEGY ON BIG DATA AND HUMAN RIGHTS AND THE DATA ECONOMY 51

BIBLIOGRAPHY 55

ABBREVIATIONS

AFSJ	Area of Freedom, Security and Justice
CCP	Common Commercial Policy
CDFREU	Charter of Digital Fundamental Rights of the European Union
CETA	Comprehensive Economic and Trade Agreement
CFREU	Charter of Fundamental Rights of the European Union
CIA	Central Intelligence Agency
CJEU	Court of Justice of the European Union
DESI	Digital Economy and Society Index
DPA	Data Protection Authority
DPD	Data Protection Directive
DSM	Digital Single Market
EC	European Commission
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EP	European Parliament
EU	European Union
EUR	Euro
EUSFTA	EU-Singapore Free Trade Agreement
FTA	Free Trade Agreement
GATS	General Agreement on Trade in Services
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
IDPC	Irish Data Protection Commissioner
LIBE	Civil Liberties, Justice and Home Affairs committee of the European Parliament
NSA	National Security Agency
PIPEDA	Personal Information Protection and Electronic Documents Act
RPEC	Regulation on Privacy and Electronic Communications
SHD	Safe Harbor Decision
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TTIP	Transatlantic Trade and Investment Partnership
UDHR	Universal Declaration of Human Rights
US	United States of America

1. INTRODUCTION

'Digital technologies are going into every aspect of life. […] We need to be connected, our economy needs it, people need it[1]', stated Jean-Claude Juncker, president of the European Commission (EC), on the 14 September 2016, and emphasized the growing need of interconnectedness in the digital age. The digital age is characterized by a shift towards an economy based on digital technologies and devices. Being connected with people on the other side of the globe has never been as easy as it is nowadays. New driving forces and technologies of the internet industry have risen the growth from a human society towards a cyber society[2]. The use of digital technologies is more and more integrated in our every day life. Through the increasing use of digital technologies immense amounts of data are generated. This data has been described as a 'goldmine of information[3]'. It is collected, stored and shared and is generally called 'big data'. Gathering the data retrieved, with meaningful information and patterns about the user's behavior and habits, it can be utilized to provide the user with services adjusted to his or her (consumer) preferences[4]. However, this is only one option for the use of big data. Big data usage can be found in all different kinds of environments: finance, health, e-commerce, security, household, agriculture and many more. In all these areas, the applications share the processing of huge data emerging in short intervals[5].

The following research investigates the degree to which big data impacts the data economy and human rights referring to the Maximillian Schrems case as a benchmark. The study focuses on the regulatory and human rights challenges related to big data regulation. In the recent report of the Civil Liberties, Justice and Home Affairs committee of the European Parliament (LIBE) it is emphasized that there is 'unprecedented insight into human behavior, private life and our societies[6]' because of the growing use of big data, new devices and communication technologies. This statement points out the perspective of a private individual focussing on the risk and fear of big data. Therefore, the approach of the LIBE committee is rather citizen-oriented. Anyhow, the businesses and economists focus mostly on the potential of technologization and digitalization and the growing market of big data usage. The trend turns towards a data-driven economy: an economy that is more and more based on data and in need of regulatory frameworks.

One of the strategies that aims on the integration of the digitalization into the European Union (EU) policy framework is the EC's digital single market strategy, which emphasizes the potential of data-driven technologies and big data usage as a positive influence on the economic growth and thus, the digitalization and innovation potential of the EU. The EC expects an almost 1.9

---

[1] European Commission (2016a), '*A Digital Single Market for Europe*', available at https://ec.europa.eu/commission/publications/digital-single-market-two-years_en.

[2] H. Mohanty, P. Bhuyan & D. Chenthati, '*Big Data - A Primer'*, Studies in Big Data, Volume 11, Springer India.

[3] European Commission (2015a), '*Digital Single Market: driving economic growth*', available at https://ec.europa.eu/digital-single-market/en/economy-society-digital-single-market#Article.

[4] H. Mohanty, P. Bhuyan & D. Chenthati, *supra* 2.

[5] H. Mohanty, P. Bhuyan & D. Chenthati, *supra* 2.

[6] A. Gomes, '*Report on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law enforcement*', Document LIBE/8/07753.

percent growth in the overall economy of the EU due to big data usage[7]. Moreover, individuals can profit: big data may enable intelligent traffic control, easy accessible e-governance products or a better adjusted and flexible healthcare program. The following research aims on providing a holistic overview of big data that identifies privacy concerns and needs for action regarding the EU institutions.

1.1 Research question and subquestions

As outlined before, most perspectives focus rather on the chances or on the risks of big data, but do not give a holistic picture. This research shall provide a study emphasizing possible opportunities and hazards and their relationship to offer the reader a more diverse picture of big data. The study focuses on the relationship between a data-driven economy and human rights standards regarding the EC's strategy on big data. This takes both approaches — the citizen-friendly and the business-oriented — into consideration. The research is based on one main research question (RQ):

RQ: To what extent does the strategy of the European Commission on big data promote a data-driven economy whilst respecting human rights standards?

The main research question comprises the characteristics of an explanatory, hermeneutic and logic type of research[8]. To answer the main question the EC's strategy itself is presented to analyze its influence (*section 3*). This part is based on an explanatory approach. Throughout the research, different aspects of the impact of a data-driven economy are analyzed with a focus on conflicting areas regarding human rights standards (*section 4*). This relationship is based on an explanatory and logic research. In order to answer the research question, its scope is limited to a case study of Maxmillian Schrems (*section 2*). Furthermore, the EU's internal standards on trade agreements with third countries are identified as the field of the EC's big data strategy cannot be limited to the EU due to the transnational character of big data (*section 5*). This section is based on an explanatory and logic approach. The main research question is answered in chapter six using the previous results and interpreting possible outcomes through a hermeneutic approach. The following subquestions (SQ) help providing answers to the main research question and are analyzed in chapter two, three, four and five:

SQ 1: What are principles that emerge from the Maximillian Schrems case on the relationship between human rights protection and a data-driven economy?

The first subquestion focuses on the case study on Maximillian Schrems. This subquestion is based on an explanatory, logic and hermeneutic typology[9]. First, the general frameworks applied

---

[7] European Commission (2015a), *supra* 3.

[8] C. Matera, '*Writing a bachelor thesis in law in the European Public Administration program at the University of Twente*', p. 5.

[9] C. Matera, *supra* 8.

in the Maximillian Schrems case are presented and analyzed, based on an explanatory, hermeneutic approach (*section 2.1*). Afterwards, the Maximillian Schrems case itself is identified at lengths based on a hermeneutic approach (*section 2.2*). The last section addresses the relationship between the Maximillian Schrems case and a data-driven economy and applies the emerging principles from the first section to answer the first subquestion of the study (*section 2.3*). This follows the typology of an explanatory and logic approach. This chapter presents and evaluates the general principles and legislative and political framework of the case as the case study is used as a fundament in the on-going research. Thus, an extensive analysis and interpretation is necessary.

SQ 2: How is the big data strategy of the European Commission related to the data economy?

The second subquestion follows the typology of a logic, explanatory and hermeneutic question[10]. First, the EC's big data strategy is presented with a focus on the digital single market (DSM) and the data economy (*section 3.1*). Additionally, the study analyzes the EU's interest in a data economy, taking the competitive character with third countries into consideration (*section 3.2*). Is the EU seeing itself as a pioneer and fears to fall behind? Is data the new currency and causes economic growth needed to maintain the EU's economic position? These questions are answered in chapter three in order to provide an integral image of the data economy and the EC's interest in the field of big data (*section 3.3*).

SQ 3: To what extent are human rights torn in between big data and the data economy?

The third subquestion is asked in a logic, explanatory and hermeneutic manner[11]. First of all, human rights are broken down to the right of privacy and data protection. It is differentiated between the right of privacy and data protection and focused on the regulatory frameworks concluded in the area of human rights, data protection and the right of the right of privacy with a focus on its relationship to big data and the data economy (*section 4.1*). This section is based on the explanatory character of the question. The intersections of the right of privacy, big data and the data economy are interpreted including the risks of privacy due to data fragmentation (*section 4.2*). This part focuses on the hermeneutic and logic characteristics. The final section of the fourth chapter reifies the interaction between the right of privacy and the data economy and stresses the interests of the opposing angles of the topic *(section 4.3*).

[10] C. Matera, *supra* 8.

[11] C. Matera, *supra* 8.

SQ 4: To what extend are big data, the data economy and human rights considerations, in the sense of data protection, placed in the relationship of the EU and its external relations?

The fourth subquestion is relevant as it incorporates the transnational characteristics of big data and the data economy into the research. It explicitly refers to the EU's current policy and regulatory framework regarding trade relations with third countries. This subquestion comprises the characteristic of an explanatory and logic approach[12]. It aims on presenting the EU's internal standards (*section 5.1*), based on an explanatory research approach. To limit the subquestions scope, it focuses on the recently negotiated trade agreements between the EU and third countries (*section 5.2*). Thus, the trade agreements between the EU South Korea (*section 5.2.1*), the EU and Canada (*section 5.2.2*), the EU and Singapore (*section 5.2.3*), the EU and Japan (*section 5.2.4*) and the EU and the United States of America (*section 5.2.5*) are analyzed. In the end, a conclusion on the EU's internal standards on externally concluded trade agreements with third countries is made (*section 5.3*). In the sixth chapter, the main research question is answered.

1.2 Body of knowledge, methodology, theory and conceptualization

The following section introduces into the methodology and theory used to tackle the research question, the current body of knowledge and the conceptualization of terms. The first section propounds the body of knowledge, afterwords, the study introduces into the methodology and theory, whereas the last section focuses on the conceptualization of terms.

1.2.1 Body of knowledge

The study is searching for whether competences of institutions ask for a technology neutral or technology specific regulation in the field of big data[13]. Regarding the current competences, the study focuses on one European institution, the EC. To understand the situation, the system itself has to be understood, therefore, this section introduces into the meta-structures of the study.

The meta-structures rely on the EU's integration, the EU's human rights protection and the EU's international relations. The EU's integration is represented through the data economy, evoking the supranational approach of the EU and the competition, the EU founds itself in with third countries. The right of privacy serves as an example for the EU's human rights protection, whereas the scope of the EU's international relations is presented through the internal standards shaping the EU's interactions with third countries on trade agreements. Coming from these meta-structures, the study is based on the interconnectedness of consumer law, personal data processing, the general data protection regulation and competition law. Therefore, it addresses the idea of a growing economy and the individual privacy concerns of consumers[14]. The study

---

[12] C. Matera, *supra* 8.

[13] D. J. B. Svantesson, '*A Legal Method for Solving Issues of Internet Regulation; Applied to the Regulation of Cross-border Privacy Issues',* EUI Working Papers, Law 2010(18).

[14] G. Buttarelli, '*EDPS Opinion on coherent enforcement of fundamental rights in the age of big data*', Opinion 8/2016.

identifies the current challenges and difficulties of big data regulations and missing competences, responsibilities and regulatory frameworks with a focus on the European Commission.

1.2.2 Methodology and theory

The study is based on one main research question limiting the field of digitalization to the area of big data. The approach on how to tackle the research question is an explanatory, hermeneutic research design[15], based on argumentation and interpretation as the topic displays actuality and no general provisions have been concluded up until now.

To answer the research question, several subquestions are answered previously. First of all, the Maximillian Schrems case is presented at length, comprising its principles and relationship to the human rights protection and a data-driven economy (*SQ 1, section 2*). As the case builds the fundament of the study it is presented first. In the next chapter, the focus is on the big data strategy of the EC to identify its current policy framework (*SQ 2, section 3*). In this section, the data economy and the general economic principles of the EC are identified. This section answers the first part of the main research question: *'to what extent does the strategy of the European Commission on big data promotes a data-driven economy*'. The third subquestion integrates the field of human rights protection and the right of privacy in the research and therefore, focuses on the last part of the main research question: '*whilst respecting human rights standards' (section 4)*. The fourth subquestion includes the transnational character of digitalization into the study and analyzes the EU's approach in concluding trade agreements with third countries (*section 5*). Afterwards, the main research question can be answered.

This study is based on a case study and literature reviews. The case has been chosen as it stresses the debate of the interconnectedness of the area of big data and privacy concerns. Additionally, it connects the topic of big data to the transnational sphere and arouses the difficulties regarding the engagement of third countries. As law making is rather reactive than active[16], the study emphasizes what has happened in the past to conclude possible improvements and developments. The literature used refers to position papers and policy papers. A policy paper brings a proposal of an institution on a policy to light, whereas a position paper states a concrete sentiment on one or more topics, mostly written by one person. Position papers often comment on policy papers, which usually introduce new contemplates or policies. Additionally, the study relies on existing legislation, previous court decisions and other institutional papers, which can all be filed as qualitative data.

The variables conceptualized in the next section and their facets are used to indicate the main terms. So far, the extent of the research question and the subquestions have been identified. The next section introduces into the individual concepts of the study and aims on the clarification of terms.

---

[15] C. Matera, *supra* 8.

[16] D. J. B. Svantesson, *supra* 13.

1.2.3 Conceptualization

In the following, the main analytical concepts and terms of the research are discussed. In times of the digital age, the EU and its institutions are confronted with the impact of new technologies in the digital sphere. Therefore, the EU's institutions have to address the concerns due to the on-going digitalization process in their strategies. The research's scope is limited to the field of big data, which is the first concept that needs to be clarified in the following section.

1.2.3.1 Big data, the digital single market and the data economy

First of all, terms connected to the technological age will be explained: big data, the digital single market and the data economy.

Many researchers and scientists have approached a definition of 'big data'. However, a clear conceptualization is difficult, as the term is used to cover a technical phenomenon rather than being used as an analytical concept. It depends on the researcher's scope what to include in the term 'big data', therefore, three definitions from literature reviews are presented.

In the recent report on fundamental rights implications of big data, privacy, data protection and non-discrimination of the LIBE committee of the European Parliament

> 'big data refers to the collection, analysis and the recurring accumulation of large amounts of data, including personal data, from a variety of sources, which are subject to automatic processing by computer algorithms and advanced data-processing techniques using both stored and streamed data in order to generate certain correlations, trends and patterns[17]'.

Other authors have defined big data 'as a holistic approach to manage, process and analyze volume, variety, velocity, veracity and value in order to create actionable insights for sustained value delivery, measuring performance and establishing competitive advantages[18]'. The series 'Studies in Big Data' only refers to three of the features mentioned above in order to describe 'big data': velocity, variety and volume[19].

In the next section the term 'digital single market' is conceptualized to clarify the individual parts of the research question and the subquestions. The Digital Single Market (DSM) is a strategy of the EC[20] encouraging trade between the EU Member States by removing digital barriers and encouraging the free movement of goods, services and people[21]. The DSM follows

---

[17] A. Gomes, *supra* 6.

[18] S. Fosso Wamba, S. Akter, A. Edwards, G. Chopin & D. Gnanzou, '*How big data can make big impact: Findings from a systematic review and a longitudinal case study*', International Journal Production Economic, 2015(165), 234-246.

[19] H. Mohanty, P. Bhuyan & D. Chenthati, *supra* 2.

[20] European Commission (2016a), *supra* 1.

[21] T. Wessing (n.n.), '*The Digital Single Market*', available at https://united-kingdom.taylorwessing.com/en/digital-single-market.

the aim of improving the 'access for consumers and businesses to digital goods and services across Europe[22],' to shape 'the right environment for digital networks and services to flourish[23]' and to create 'a European Digital Economy and society with growth potential[24]'. It has been created to build a digital connected continent all over the EU and ease the flow of data among member states[25].

To sum up, the DSM strategy of the EC aims on improving internet access, creating a good business environment, driving economic and employment growth. As the DSM is a strategy of the EC, the implementation is based on the EU Member States agreements on draft legislations, therefore, the concrete realization cannot be dated[26]. Some companies and businesses fear an exclusion of local markets through the DSM as it may encourage the business of multinational companies[27].

The DSM is separated in three policy areas and sixteen different initiatives, one of them being the 'data economy'. As the study reflects the degree to which big data impacts the economy and human rights standards, the data economy is one of the key concepts of the study. In order to capture the different contexts in which the concept 'data economy' is applicable its facets have to be identified. The issues raised through the term 'data economy' are for example the localization of data liability and standardization of regulation to identify the actions needed[28]. Data economy includes data for research, innovation and new business opportunities as well as new promising technologies, such as cloud computing and the Internet of Things[29]. The data economy is part of the EC's strategy on the DSM and new policy and legal solutions to unleash the EU's data economy have been published on 10 January 2017. The data economy aims on resolving unnecessary restrictions on the free movement of data across borders. To implement the data economy, the EC engages in dialogues with EU Member States and offers different pioneer projects. These actions shall encounter 'further evidence on the nature of […] restrictions and their impact on businesses […], startups, and public sector organizations[30]'. As the data

---

[22] European Commission (2015b), '*Why we need a Digital Single Market?'* available at https://ec.europa.eu/commission/publications/why-we-need-digital-single-market_en.

[23] European Commission (2015b) *supra* 22.

[24] European Commission (2015b) *supra* 22.

[25] European Commission (2015a), *supra* 3.

[26] T. Wessing, *supra* 21.

[27] Diana Lodderhose critiques that the DSM disadvantages small companies, indie businesses, associations and institutions in the film industry as the market stability of multinational companies and productions, such as Google, Apple, Netflix, Amazon and Hollywood may increase through the DSM. Other players are excluded as they cannot compete in the international dominated market and depend stronger on the local market and access regulations. ('*Europe's Digital Single Market: What you need to know & how it may kill indie biz*', available at http://deadline.com/2016/11/europe-digital-single-market-what-you-need-to-know-how-it-could-kill-the-indie-business-1201857973/.)

[28] European Commission (2016a), *supra* 1.

[29] European Commission (2016a), *supra* 1.

[30] European Commission (2017a), '*Commission outlines next steps towards a European data economy*', available at http://europa.eu/rapid/press-release_IP-17-5_en.htm.

economy's foundation is build on trust, a strong affiliation to human rights can be identified. Therefore, the next section includes the right of privacy and data protection.

1.2.3.2 Human rights and the right of privacy and data protection

The second sub-section defines the necessary legal provisions for three other key concepts related to the technical area of big data: human rights, right of privacy and data protection.

Whilst the concept of 'human rights' can be defined as

> 'rights inherent to all human beings, whatever our nationality, place of residence, sex, national or ethnic origin, color, religion, language or any other status. […] These rights are all interrelated, interdependent and indivisible. […] International human rights law lays down obligations of government to act in certain ways or to refrain from certain acts, in order to promote and protect human rights and fundamental freedoms of individuals or group[31]',

for the purpose of this research only a specific right is taken into consideration. The focus is on the 'right of privacy' as it is often discussed in relation with big data usage. Additionally, the chosen case is based on the infringement of the right of privacy. In 1890, Samuel D. Warren and Louis D. Brandeis published an article on the right to privacy and examined 'that the individual shall have full protection in person and in property is a principle as old as common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection[32]'. Coming from this point, the study analyzes the right of privacy and data protection and its development through new technologies. Therefore, in the following, legal provisions of the right of privacy are given. First of all, the right of privacy is defined in international public law in article 12 of the Universal Declaration of Human Rights (UDHR):

> Article 12
> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks (UDHR, 1948).

in article 8 of the European Convention of Human Rights (ECHR):

---

[31] Office of the High Commissioner (n.n.), '*What are human rights?*', available at http://www.ohchr.org/EN/Issues/Pages/WhatareHumanRights.aspx.

[32] S. D. Warren & L. D. Brandeis (1890), '*The Right to Privacy*', Harvard Law Review, Vol. IV, No. 5.

> Article 8 – Right to respect for private and family life
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others (ECHR, 1950).

and in article 7 of the Charter of Fundamental Rights of the European Union (CFREU):

> Article 7 – Respect for private and family life
> Everyone has the right to respect for his or her private and family life, home and communications (CFREU) 2000).

The articles provide a basis for the conceptualization of the right of privacy. Article 6 of the Treaty on European Union (TEU) states that the rights of the CFREU are recognized and the identified values shall be promoted.

The study analyzes the challenges linked to protecting the right of privacy in connection with big data and a data-driven economy. In the following, the concept of 'data protection' is defined, as it is strongly interconnected with the right of privacy in regard with big data usage. The CFREU defines personal data protection in article 8:

> Article 8 – Protection of personal data
> 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 (CFREU, 2000).

As identified in the previous section article 6 TEU recognizes the CFREU. Additionally, article 16 of the Treaty on the Functioning of the European Union (TFEU) ensures the data protection through its provision:

> Article 16 (ex Article 286 TEC)
> 1. Everyone has the right to the protection of personal data concerning them.
> 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. […] (TFEU, 2012).

The articles provide a conceptual basis for the term 'data protection' used later in the study to interpret the right of privacy and its impacts in the digital sphere. The previous definitions are given to start from the same level of understanding of terms for the upcoming analysis of the challenges linked to protecting privacy and data in the context of big data and the data economy.

1.3 Social and scientific relevance

In the context of globalization, digitalization has become a more and more important subject. In the field of digitalization, the concept of big data covers a wide scope as it compromises a plurality of electronically received data from various sources. An interesting feature of big data is that modern businesses and startups are embracing these developments as they may cause a growing economy and new flourishing business fields. Contradictory, many citizens and more traditional businesses fear new technologies due to the unidentified limits of big data usage and unpredicted control through modern businesses over the economic market which causes the 'glass human being', also known as the 'transparent citizen'. As fear does neither harm the businesses' usage of new technologies, nor does it empower the citizens in promoting their rights, the study emphasizes the strengths and the weaknesses of big data to elaborate a broad picture that enables the reader to understand why big data and its regulation are important for our future. A more confident approach on big data regulation may limit abuses and eliminate the fear of technology. However, to be confident about big data one has to be informed about the opportunities and risks. This gives the study sufficient social relevance to investigate this field. As the topic is very recent and continuously evolves, not a lot of research has been done on the effects of big data and possible infringements of human rights, explicitly the right of privacy and data protection. Therefore, this study helps understanding the regulatory and human rights challenges related to big data regulation. Diving in to a mostly undetected field of research ensures scientific relevance and offers opportunities to fill knowledge gaps.

2. THE PRINCIPLES EMERGING FROM THE MAXIMILIAN SCHREMS CASE ON HUMAN RIGHTS AND THE DATA ECONOMY

After having outlined the background of the study, this chapter answers the first subquestion of the research: What are principles that emerge from the Maximillian Schrems case on the relationship between human rights protection and a data-driven economy? The case emphasizes the interconnectedness of the area of big data and privacy concerns and links big data to the transnational sphere, which arouses the difficulties regarding the engagement of third countries. Therefore, this chapter focuses on the emerging principles of the Maximillian Schrems case in the field of data protection, the right of privacy and the data economy. The first section introduces into the relevant frameworks of the Maximillian Schrems case, such as the Safe Harbor Decision (SHD), the EU-US Privacy Shield and the cross-border data transfer to third countries. At the end of the section, emerging principles are presented (*section 2.1*). Afterwards, the Maximillian Schrems case itself is described and the problems raised are analyzed (*section 2.2*). The last section of this chapter addresses the impact of the Maximillian Schrems case on a data-driven economy and thus, answers the first subquestion of the study (*section 2.3*). The determined principles are applied in the following chapters to the individual concepts, thus, this chapter serves as a benchmark for the study.

2.1 The Safe Harbor Decision, the EU-US Privacy Shield and cross-border data transfers to third countries

Already in 1995, the European Union (EU) concluded a Directive on Data Protection (DPD)[33], which entered into force in October 1998. The Directive applies to all countries of the European Economic Area (EEA), which includes all EU Member States and Iceland, Liechtenstein and Norway. Once personal data is transferred to countries outside the EEA special precautions need to be taken.

Article 25 DPD states that personal data can only be transferred to third countries when an adequate level of protection is ensured. The European Commission (EC) has made several decisions on the adequacy of the protection of personal data in third countries, including the SHD and the EU-US Privacy Shield[34]. The general principle for the transfer of personal data to a third country resolving from this section is, that the recipient has to ensure an adequate level of protection, similar to the EU standards, which may not be violated. Questionable is, what is an adequate level of protection?

Often the adequacy is determined through similar data protection standards to the EU. However, the DPD states that the EC has the power to determine the adequacy of protection. The process on how the adequacy is considered is laid down in article 25 (6) DPD. There are different jurisdictions on how the adequacy has been assessed. Member states of the Convention 108 are

---

[33] Directive 95/46/EC.

[34] European Commission (n.n.a), '*Data transfers outside the EU*', available at http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm.

seen has having an adequate, or sometimes even equivalent level of data protection[35]. In this case, equivalent is used to emphasize that the regulative framework corresponds to the principles of the EU. Adequacy only determines that a suitable and appropriate level is given, however it is not identical to EU law[36]. In Andorra the assessment took place on the base that the national law (Qualified Law 15/2003 on the protection of personal data) complies with the DPD. Moreover, the state has a Parliamentary Co-Principality with the President of the French Republic[37]. In Switzerland it has been assessed that the Swiss Data Protection Act complies with the DPD[38]. In Canada the Personal Information Protection and Electronic Documents Act (PIPEDA) had to enter in force to receive the status of an adequate level of protection[39]. It can be identified, that the adequacy is usually assessed on the basis of the national law of the third country.

A new Directive on Personal Data entered into force on the 5 May 2016 and the EU Member States have to include the Directive into national law by the 6 May 2018[40]. Moreover, a new Regulation entered into force on the 24 May 2016 and applies on the 25 May 2018[41]. Both frameworks shall reform the data protection in the EU. The later is repealing the former DPD and thus, responsible for data protection, the processing of data and the free-movement of data, and therefore, relevant for this study.

According to the DPD, to transfer data with third countries, such as the United States of America (US), the EC had to conclude agreements. In 2000 the SHD was concluded between the EU and the US. Facing the decision, the EC considered the US as having an adequate level of protection of personal data[42] and thus, the EC concluded this decision, instead of determining an adequate level of protection. The decision was based on the self-commitment of US-companies. The SHD[43] is the fundament for the transfer of personal data from the EU to the US. In order to transfer data from the EU to the US, mother companies based in the US have to comply with the DPD and join the Safe Harbor Program to have access to the person-related data from the EU's citizens. Here, one can see a link between the SHD and the idea of a data-driven economy. Moreover, the nature of the agreement of the SHD is a private-public deal. In October 2015, the SHD has been declared as invalid by the Court of Justice of the European Union (CJEU). The

---

[35] Convention 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data).

[36] European Data Protection Supervisor (14.07.2014), '*The transfer of personal data to third countries and international organizations by EU institutions and bodies',* Position paper, available at https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf.

[37] 2010/652/EU on the adequate protection of personal data in Andorra.

[38] 2000/581/EC on the adequate protection of personal data provided in Switzerland.

[39] 2002/2/EC on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act.

[40] Directive 2016/680/EU, this Directive is focusing on the use of data in criminal areas and therefore, less relevant for this study.

[41] General Data Protection Regulation EU 2016/679

[42] European Commission (n.n.b), '*Digital Single Market - Commission strengthens trust and gives a boost to the data economy*'.

[43] Safe Harbor Decision 2000/520/EG.

invalidity of the decision and the judgement of the CJEU is addressed while presenting the Maximillian Schrems case (*section 2.2*).

Since 2016, there is a new political and regulative framework, replacing the SHD: The EU-US Privacy Shield[44]. As the SHD was declared invalid in October 2015, a new agreement was needed to continue the business and thus, the transfer of data from the EU to the US. The EU-US Privacy Shield has been concluded by the EC and the US Department of Commerce. The three key features are: 'Strong obligations for companies' handling of EU citizens' data, clear safeguards and transparency obligations for US government agency access and new redress and complaint resolution mechanisms for EU citizens[45]'. The EU-US Privacy Shield is 'based on a system of self-certification for the transfer for commercial purposes to the US of personal data sent from the EU[46]'. In relation to the SHD, the EU-US Privacy Shield is based on the DPD and the requirements are stricter: companies may only transfer personal data to partners for limited purposes and with a contract providing at least the same standards. Moreover, they must take appropriate measures to protect data from loss, misuse, unauthorized access, disclosure, alteration and destruction[47]. EU citizens have opportunities to redress their data, to report complaints to local Data Protection Authorities (DPA) and there are clear safeguards and mechanisms limiting mass surveillance[48]. Nevertheless, the EU-US Privacy Shield has been criticized by a number of European data protection regulators and may end up in front of the CJEU in the future, but, one has to admit that it currently serves as a valid and accessible mechanism to enable data transfers from the EU to the US[49]. A principle emerging from the new agreement is, that privacy and data protection constraints are permanently developing, thus, a general framework cannot be found. Due to the strong dependence on the US-market, the EU is in need to conclude agreements on data transfers with the US. New complaints may reveal stronger data protection and privacy regulations, thus, one has to fight for EU standards and fundamental rights.

The new General Data Protection Regulation (GDPR), shortly introduced at the beginning of this chapter and adopted by May 2016 has to be implemented until May 2018. It interrelates with the EU-US Privacy Shield as both frameworks shall maintain data protection. The main difference between the two frameworks are the purposes: the GDPR came from the EU and is based on protecting its citizens and adapting new changes in technology, thus, the main reason for the GDPR was the privacy of the EU's citizens. Contradictory, the EU-US Privacy Shield replaces the SHD and focuses on the digital business between two countries with different

---

[44] EU-US Privacy Shield: Commission Implementing Decision 2016/1250/EU.

[45] ITI (2016), '*The EU-US Privacy Shield*', available at http://www.itic.org/safeharbor.

[46] European Data Protection Supervisor (30.05.2016), '*Opinion on the EU-US Privacy Shield draft adequacy decision*', Opinion 4/2016.

[47] T. Wessing (2016), '*EU-US Privacy Shield - What's new in comparison with Safe Harbor*', available at http://www.lexology.com/library/detail.aspxg=e02eccc0-9c26-4eb6-9293-00 fb41272693.

[48] P. Hastings, '*Five Ways that Privacy Shield is Different from Safe Harbor and Five Simple Steps Companies Can Take to Prepare for Certification'*, available at https:// www.paulhastings.com/publications-items/details?id=eaffe969-2334-6428-811c-ff00004cbded.

[49] T. Wessing (2016), *supra* 47.

cultures to privacy. There has been critique on the EU-US Privacy Shield due to the self-certification of businesses. As the GDPR is not in force yet, one cannot predict how the two frameworks will cooperate with each other, however, even though the EU-US Privacy Shield is stricter than the SHD, there is a lack of clarity and contradicting purposes that may cause court sanctions or fines as the complex legal procedure of transferring data across countries is not yet solved[50].

This section introduces into the transnationality of cross-border data transfers. Transnationality means going beyond nationhood and contradicting nationalism[51]. As the digital sphere crosses all borders, every state, region or association of states has to conclude individual agreements to ensure certain standards. In times of growing interconnectedness, transfers of personal data to third countries become more frequent, which can be seen in the augmenting agreements of the EU with third countries[52]. To ensure EU standards, the fundamental rights have to be taken into consideration regarding transfer of data to third countries. A new proposal for a Regulation on Privacy and Electronic Communications (RPEC)[53], presented in January 2017, strives at extending privacy rules to new communication services including online communication, namely WhatsApp, Facebook and Skype[54]. The new Proposal for a RPEC shows the urgent need of new frameworks to solve the difficulties occurring due to transnationality. Moreover, the communications frameworks need to be enlarged to the digital sphere and the field of electronic communications.

The SHD is an example of the interference of a transnational area, the digital sphere, and EU law. Thus, either way technological neutral or technological specific regulations[55] are demanded. The SHD has shown, that technological specific regulations may require frequent adjustments and have to be very detailed to not infringe the law of one or the other party. Questionable is, if there are chances to create technological neutral agreements on cross-border data flows. This requires either way a general acceptance of higher privacy and data protection regulation and therefore, less innovative use of data and technology or a higher degree of a data-driven economy and thus, less privacy protection for the individual. However, the interests of the countries involved are diverging and thus, the chances are high that individual agreements will be concluded in the future. As mentioned before, the current agreement on the EU-US Privacy Shield is in critique of European data protection regulators and may need adjustments to properly correspond to EU law. As the example has shown, transnational spheres cannot be easily

---

[50] T. Stretton & L. Grest, '*How will the new EU-US privacy shield fit with the upcoming General Data Protection Regulation*', available at https://www.scmagazineuk.com/how-will-the-new-eu-us-privacy-shield-fit-with-the-upcoming-general-data-protection-regulation/article/531527/.

[51] C. E. Bradatan, '*Transnationality as a fluid social identity*'.

[52] The impact on agreements concluded between the EU and third countries is highlighted in *chapter 5*.

[53] Proposal for a Regulation on Privacy and Electronic Communications 2017/0003 (COD).

[54] European Commission (2017b), '*Hearing: Respect for private life and protection of personal data in electronic communication*', available at http://www.europarl.europa.eu/news/de/news-room/20170411IPR71014/respect-for-private-life-personal-data-protection-in-electronic-communication.

[55] D. J. B. Svantesson, *supra* 13.

incorporated in prevailing agreements and contracts and thus, need regulations. Currently, they are based on technological specific regulations. Yet, once the digital sphere is more incorporated, there may be technological neutral regulations to conclude general agreements[56].

This section addresses the competences of the EC in concluding agreements with third countries on personal data transfers. The EC is the executive branch of the EU and responsible for proposing and enforcing legislation and implementing policies. Internationally, the EC negotiates agreements for the EU. Thus, the EC is responsible for agreeing on frameworks on transatlantic data flows. The SHD and the Privacy Shield were approved and concluded by the EC[57]. Regarding the procedures, the legitimacy of the agreements are criticized, as there have not been legislative procedures and not the European Parliament nor the Council had to agree on the decisions. Moreover, the EC is not elected by the citizens, thus, the democratic procedure is criticized. In general, one would concede a high degree of power to the EC, nevertheless, the agreements and thus, the Maximillian Schrems case presents, that the existence of a decision by the EC does not eliminate or reduce the internal standards. In this case, the powers have been regained and monitored by the CJEU which related to national supervisory authorities: the Charter of Fundamental Rights of the European Union (CFREU). Thus, the principle emerging is, that all institutions and branches are limited by the general principles and standards of the EU and cannot override them. Additionally, eligible concerns of the legislative and democratic procedure are raised, regarding the power of the EC in negotiating contracts with third countries.

The investigated principles focus on the human rights debate evolving through the transfer of personal data. Generally, they show the importance of frameworks and agreements being in accordance with the fundamental rights of the EU and the necessary control of legitimacy by the CJEU. Moreover, it represents the necessity of being an active EU citizen: using one's opportunities and claiming one's rights. Questionable is, if the US-market dependence and thus, the inadequately protected transfer of personal data, overrides the EU standards due to a data-driven economy[58]. As the current regulative framework presents, an assurance of the right of privacy and data protection cannot be guaranteed, consequently, the transnational trade of data as to be reassessed. In the next section, the benchmark of the study is analyzed, the Maximillian Schrems case. The previously presented frameworks are applied to the case and the main principles of the case are emphasized.

2.2 The Maximillian Schrems case

This section provides an introduction into the Maximillian Schrems case[59] and connects the case to the SHD and the DPD. The Maximillian Schrems case relates to the frameworks discussed in

---

[56] The transnational character of big data and a data-driven economy is extensively analyzed in *chapter 5*.

[57] European Commission (2016b), '*Protection of personal data*', available at http://ec.europa.eu/justice/data-protection/.

[58] The data-driven economy is highlighted in *chapter 3*.

[59] Maximillian Schrems case C-362/14.

the previous section and has a focus on the main concepts of the study: data economy, right of privacy and data protection in the area of big data usage.

Maximillian Schrems is an Austrian lawyer, author and privacy activist who became famous for claiming against Facebook for privacy violation. As a European Facebook user since 2008, Maximillian Schrems user contract is with Facebook Ireland Ltd, which again transfers user data to its servers in the US. Schrems complained in 2013 and asked the Irish Data Protection Commissioner (IDPC) whether the data transfers are adequately protected[60]. Schrems complaint was encouraged through Edward Snowden, a former Central Intelligence Agency (CIA) employee who leaked information without authorization from the National Security Agency (NSA). The IDPC, responsible as the server is located in Ireland, based his answer on the SHD. The SHD states that data transfers to US companies participating in the Safe Harbor scheme are adequately protected[61]. More than 4,600 US companies have used the SHD during that time for their data transfers, including Facebook[62]. Schrems reviewed the argumentation of the IDPC and claimed the invalidity of the decision due to its coincidence with fundamental rights stated in the CFREU and DPD.

At this point, Schrems referred to EU standards: the CFREU. As presented in the first chapter, the CFREU is recognized by the TEU and thus, builds the fundament of general EU standards. Regarding the transfer of personal data to a third country, article 7, 8 and 47 CFREU have to be taken into consideration. Article 7 provides the general basis for the right of privacy, whereas article 8 emphasizes data protection. Maximillian Schrems claimed the violation of both articles as his data was not adequately protected. He received an over 1,200 pages record about his Facebook data and was not able to adjust or erase the data. Moreover, there has not been a general accessibility for the data. The new proposal for RPEC addresses article 7 and 8 CFREU, and states that both articles can be applied to the digital sphere. Therefore, a clear violation through the Safe Harbor data transfers can be stated. Moreover, article 47 CFREU ensuring the right to a fair trial has been infringed as it was not possible to claim against the transfer of personal data to the US. This argumentation is the fundament of the judgement of the CJEU.

In October 2015 the Court of Justice of the European Union (CJEU) handed down a judgment in the case. The CFREU ensures the fundament for the right of privacy (article 7 CFREU), data protection (article 8 CFREU) and the right to a fair trial (article 47 CFREU). The DPD includes article 25 which ensures a strict regime for cross-border data flows. Data transfers with third countries are only realizable if the recipient ensures an adequate level of protection[63]. The CJEU declared the SHD of the EC as invalid. The argumentation is based on the legitimacy of data

---

[60] The background of the Maximillian Schrems case and further developments are available at http://europe-v-facebook.org/EN/en.html.

[61] R. Boardmann, A. Mole & G. Voisin, '*CJEU invalidates Safe Harbor*', available at https://www.twobirds.com/en/news/articles/2015/global/cjeu-invalidates-safe-harbor.

[62] F. Coudert, '*Schrems vs. Data Protection Commissioner: A Slap on the Wrist for the Commission and New Powers for Data Protection Authorities*', available at 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/.

[63] F. Coudert, *supra* 62.

processing for US national security, public interest and law enforcement requirements irrespective of the principles stated in the SHD[64]. In addition to that, the EC admitted that US authorities have access to the transferred data, even though it does not effect the national security and no controls on the adequacy have been taken. The importance of the replacement of the SHD by the EU-US Privacy Shield becomes visible taking into consideration that individuals were not able to access, adjust or erase the data relating to them during the Safe Harbor Decision[65]. Furthermore, the EC has not assessed in 2000 whether the US level of protection of fundamental rights is equivalent to EU standards, namely the DPD and the CFREU[66]. There have not been controls by the EC on an adequacy of protection. The Schrems case presents the occurring difficulties due to a transnational sphere: the standards of data protection and privacy do not correspond in the EU and US, thus, individual agreements have to be concluded. Nevertheless, the agreements have to be in accordance with the national standards of each party.

All in all, the Maximillian Schrems case caused major changes in cross-border data flows with the EU and the US. Maximillian Schrems as a privacy activist strongly promotes human rights including data protection and caused the invalidity of the SHD. The principle emerging from this case will be applied in the following chapters to answer the main research question in the end: To what extent does the strategy of the European Commission on big data promote a data-driven economy whilst respecting human rights standards? The Maximillian Schrems case is utilized as a precedential case representing the interconnectedness of the EC's strategy on big data, a data-driven economy and EU human rights standards. Thus, the Maximillian Schrems case is utilized as a benchmark in the following chapters. The next section focuses on the relationship between the Schrems case and the data economy.

2.3 Conclusion on the impact of the Maximillian Schrems case on the data economy

Having analyzed the Maximillian Schrems case and the emerging principles, this section clarifies the relationship between the Schrems case and a data-driven economy.

A data-driven economy is 'an ecosystem of different types of players interacting in a Digital Single Market (DSM), leading to more business opportunities and an increased availability of knowledge and capital[67]'. The EC has stated that a 'data-driven economy stimulates research and innovation on data, increases business opportunities and availability of knowledge and capital across Europe[68]'.

First of all, a general relationship between the Schrems case and a data-driven economy can be drawn: Facebook as a company represents the economy and the business model strongly relies on data. Facebook offers seemingly free access to the platform to the users, however, they do pay with their data. In today's society, data is often seen as the new currency and Facebook profits

---

[64] F. Coudert, *supra* 62.

[65] R. Boardmann, A. Mole & G. Voisin, *supra* 61.

[66] R. Boardmann, A. Mole & G. Voisin, *supra* 61.

[67] European Commission (02.07.2014), '*Towards a thriving data-driven economy*', available at https://ec.europa.eu/digital-single-market/en/news/communication-data-driven-economy.

[68] European Commission (02.07.2014), *supra* 67.

from the user's data. Facebook is located in the US, which are a forerunner country in the field of digitalization and have different standards regarding privacy and data protection than the EU.

Secondly, the EU encounters amicable relations with the US. In regard of commercial transfers of data, the US are the biggest trading partner of the EU[69]. The EC indicates 'a new industrial revolution driven by digital data, computing and automation[70]'. Big data technologies and services are expected to cause a worldwide growth, thus, the EU cannot afford missing the evoking potentials from this global trend[71], which means that the US as a trading partner cannot be eliminated without major economic damage.

As the judgement on the Schrems case is based on the DPD, the reform, which enters into force in May 2018 has to be taken into consideration. The GDPR has to be incorporated into the EU Member States national law by May 2018. However, to work in accordance with the GDPR, functioning mechanisms to assess and control the adequate protection of personal data in third countries, such as the US have to be ensured. The GDPR is a key enabler of the DSM (*section 3.1*) and therefore, closely relates to a data-driven economy. Citizens shall have control over their personal data and businesses shall benefit from the data economy[72]. The interconnectedness between the individual's privacy and the businesses data-driven economy is represented through the GDPR[73], the replacement of the SHD by the EU-US Privacy Shield and the Maximillian Schrems case.

The purpose of the chapter is to answer the first subquestion: What are principles that emerge from the Maximillian Schrems case on the relationship between human rights protection and a data-driven economy? This chapter clarifies that the data protection debate and the quest for a stronger data economy are closely linked in the Maximillian Schrems case. The principles emerging from the case explain that EU standards cannot be disregarded to achieve a flourishing data-driven economy. However, inaccuracies and the democratic deficit[74] cause missing protections of EU standards, thus, each EU institution is in need to control the other EU institutions. Moreover, the EU needs active citizens claiming their rights and complaining about grievances.

---

[69] European Data Protection Supervisor (30.05.2016), *supra* 46.

[70] European Commission (02.07.2014), *supra* 67.

[71] European Commission (02.07.2014), *supra* 67.

[72] European Commission (2016b), *supra* 57.

[73] The General Data Protection Regulation is extensively discussed in chapter 4, *section 4.1.1.*

[74] The 'democratic deficit' is a term arguing that the EU's decision-making procedures have a lack of democracy. EU voters do not feel their impact. As the European Parliament is the only EU institution that is legitimized by the EU citizens, the Lisbon Treaty (2009) aims on strengthening its financial, legislative and supervisory powers. Moreover, new technologies to emphasize the dialogue between the civil society and the EU institutions have been founded (EUR-Lex, available at http://eur-lex.europa.eu/summary/glossary/democratic_deficit.html)

3. THE RELATIONSHIP BETWEEN THE EUROPEAN COMMISSION'S BIG DATA STRATEGY AND THE DATA ECONOMY

Big data is becoming more relevant and concise in today's society. In order to meet the emerging needs the European Commission (EC) relates to its strategy on big data. This study focuses on the effects of the current strategy of the EC on big data. To assess the impact of the EC's strategy on big data on human rights and the data economy, the strategy itself has to be identified and analyzed. This chapter firstly, presents the EC's current strategy on big data, introduces into the relationship between the EC's strategy on big data, the Digital Single Market (DSM) and the data economy and focuses on the communication papers of the EC introduced in 2014 and 2017 *(section 3.1*). Secondly, the study points out the EU's interests in a data-driven economy in relations with third countries (*section 3.2*) and answers in the end of this chapter the second subquestion: How is the big data strategy of the European Commission related to the data economy (*section 3.3*)?

3.1 The European Commission's big data strategy, the Digital Single Market and the data economy

To introduce into the EC's strategy on big data it is important to take into consideration that policies on the data economy have been introduced before the era of big data has started. Thus, now the data economy policies have to be adjusted: The EC has included the data economy in its strategy on big data as new dimensions of data masses cause new political and regulative frameworks and adjustments. The next section introduces into the general principles of the EC's strategy on big data and its fragments.

The EC's big data strategy is under the head of the European Commissioner for Digital Economy and Society, previously the European Commissioner for Digital Agenda. Since the 1 January 2017, the office is held by Andrus Ansip, an Estonian politician[75]. He takes the view that 'data should be able to flow freely across borders and within a single data space. We need a coordinated and pan-European approach to make the most of data opportunities, building on strong EU rules to protect personal data and privacy[76]'. The EC's strategy on big data is laid down in the DSM, which encounters the general aim of opening digital chances for individuals and businesses and to strengthen Europe's position in the data economy. The DSM strategy was adopted on the 6 May 2015 and includes 16 initiatives. A European Single Market 'refers to the EU as one territory without any internal borders or regulatory obstacles to the free movement of goods, services, capital and persons. A functioning Single Market stimulates competition and trade, improves efficiency, raises quality and helps to cut prices[77]'. The DSM aims on realizing these goals in the digital sphere with a focus on creating a single market where the free

[75] Andrus Ansip is the Vice President of the EC and responsible for the DSM.

[76] European Commission (2017c), '*Building a European Data Economy*', available at https://ec.europa.eu/digital-single-market/en/building-european-data-economy.

[77] European Commission (n.n.c), '*The European Single Market*', available at https://ec.europa.eu/growth/single-market_en.

movement of goods, persons, services and capital is ensured and where citizens can fairly access online goods and services[78]. The strategy is built on three policy areas: access, environment and economy and society.

This study focuses on the last two pillars: environment, as this policy area focuses on the conditions needed for digital networks and innovative services and incorporates the aspects of the right of privacy and data protection (*chapter 4*), and the policy area of economy and society, as this pillar aims on maximizing the growth potential of the digital economy and thus, involves the data economy. In the following, the study shortly introduces into the policy area of environment and the regulative frameworks proposed by the EC. However, the field of privacy and data protection will be extensively discussed in chapter four. Afterwards, the second policy area, the area of economy and society is analyzed and the link between the EC's strategy on big data and a data-driven economy is made.

In the field of the environment policy, the EC mentions the General Data Protection Regulation (GDPR), the Data Protection Directive (DPD), and the proposed Regulation on Privacy and Electronic Communications (RPEC)[79]. The emerging frameworks are extensively discussed in the fourth chapter.

In the area of economy and society, the focus is on digitizing European industry and building a European data economy. In this study, the emphasis is on the European data economy. The data economy is based on two communications by the EC: The communication 'Towards a thriving data-driven economy' from July 2014[80] and the communication on 'Building a European data economy' from the 10 January 2017[81]. The next two sections introduce into the communication papers of the EC. Communication papers do not have a legislative status and do not serve as formal acts, however, communication papers are policy papers communicated by the EC focusing on the policy design of the EU. The communication papers of the European Commission on the data economy are presented in chronological order.

3.1.1 The European Commission's communication from 2014

Firstly, the study introduces into the communication 'Towards a thriving data-driven economy', which has been adopted in July 2014 and serves as an action plan involving all European Union (EU) Member States and EU institutions. The European Council has concluded in October 2013 to focus on innovation, services and data economy as they provide jobs and growth. Thus, the EC provided this policy paper outlining the components of a data economy[82]. First of all, the communication paper identifies the general impact of the technological age and the global trend towards big data usage. Afterwards, new opportunities emerging from the changes are presented and the potential and advantages of a data-driven economy for the EU are identified. Then,

---

[78] European Commission (2016a), *supra* 1.

[79] European Commission (2017d), '*Right environment for digital networks and services*', available at https://ec.europa.eu/digital-single-market/node/78516.

[80] European Commission (02.07.2014), *supra* 67.

[81] European Commission (2017c), *supra* 76.

[82] European Commission (02.07.2014), *supra* 67, page 1.

characteristics of the data economy and necessary framework conditions are presented. To enable a data-driven economy, the infrastructure has to be adapted as well as the cooperation among EU Member States and businesses and governments. The last section of the communication paper arouses concrete regulatory issues emerging through the adaption of a data economy.

The communication paper identifies that the technological age creates an enormous economic potential in various fields such as health, food, security and energy efficiency. Current data management tools and methods are not adapted to the large and complex data sets emerging through big data, thus, new methods, products and technologies on data collection and processing have to be promoted to enable a data-driven economy and to master new challenges occurring due to big data usage[83]. Thus, the communication paper identifies the need of action to compete in the global market, especially with the United States of America (US). 'To facilitate the implementation of the EU open data policy and legal framework, the Commission is preparing guidelines on recommended standard licenses […][84]' that can be adapted easily by the individual EU Member States and shall guide through the jungle of uncertainties in the digital sphere.

The communication criticizes the legal complexity which is made responsible for creating (unnecessary) barriers causing less data-related companies in the EU. The communication paper focuses on the use of big data only from the economy-driven site and does not enlighten possible risks. Nevertheless, the implementation of new regulative frameworks is seen as necessary[85].

Another important aspect is 'enabling the infrastructure for a data-driven economy[86]'. There are still many countries less connected than others in the EU and thus, not able to profit from this new field, which can be extensively analyzed in the Digital Economy and Society Index (DESI)[87]. Unsurprisingly, the DESI presents that the more developed countries in the EU have better access and more advanced digital economies. An overall improvement can be seen, nevertheless, the connectivity, human capital, use of internet by citizens and integration of digital technology is low in developing areas. Therefore, only the developed EU Member States can profit from the quick changes towards a data-driven economy, whereas others still found themselves in positions where broadband internet is a rare exception.

The communication presents that the EC recognizes personal data and consumer protection[88], however, data location requirements are seen as limiting the cross-border flow of information and thus, have to be reduced to a minimum[89]. All in all, the communication focuses on the economic profit and emphasizes the individual's well-being through economic flourish due to data-driven businesses based on big data.

---

[83] European Commission (02.07.2014), *supra* 67, page 2.

[84] European Commission (02.07.2014), *supra* 67, page 8.

[85] European Commission (02.07.2014), *supra* 67.

[86] European Commission (02.07.2014), *supra* 67, page 9.

[87] European Commission (2017e), '*The Digital Economy and Society Index*', available at https://ec.europa.eu/digital-single-market/en/desi.

[88] Data protection and the right of privacy are discussed in *chapter 4*.

[89] European Commission (02.07.2014), *supra* 67, page 12.

3.1.2 The European Commission's communication from 2017

Secondly, the communication on 'Building a European data economy', which has been adopted in 2017, is presented. Again, the first section of the communication focuses on the importance of a data-driven economy and strongly connects to the previous papers published by the EC to enable the free movement of data. The different existing regulative frameworks and emerging issues are introduced. Afterwards, individual topics are presented: the free flow of data, data access and transfer, different types of data and their current measurements. In the following, a rather inconcrete action-plan is presented. Necessary adjustments are mentioned, as well as the EU liability of data. Moreover, the communication has a section on the experimentation with new technologies and methods and a current research project is indicated.

Following the idea of the communication from 2014, the EC recognizes that coherent frameworks among EU Member States are needed. Thus, the communication focuses on the GDPR as a regulative framework providing 'one single pan-European set of rules contrary to 28 national laws[90]' and being applied to any personal data whether machine generated or otherwise until the data is anonymized. The framework ensures that EU standards and rules have to be acknowledged and applied by third countries which shall increase the consumer trust in the field of big data. As presented at the beginning of the study, many individuals station themselves reserved regarding big data usage. Moreover the RPEC shall ensure the confidentiality. It becomes clear, that the communication paper focuses stronger on the individual's privacy. Nevertheless, the data-driven economy is in the focus of this communication: unjustified restrictions on the free movement of data shall be minimized, privacy concerns should not be used by public authorities as a reason to restrict the free flow of data as the GDPR provides a high level of privacy and data protection for the EU and access to data by market players to flourish the market[91]. The communication proposes further voluntary or mandatory insurance schemes and risk-management approaches to asses the liability and compensate possible damage. As the communication is on the data economy, it mainly focuses on economic aspects. Nevertheless, in comparison to the first communication from 2014, the EC realized that individuals fear their privacy and data protection, thus, the communication has been adjusted and new frameworks have been concluded.

In general, the initiative of a European data economy aims on utilizing the potential of digital data to its fullest to benefit the society and economy. Therefore, it tackles barriers impeding the free flow of data which is a necessary condition to accomplish a European DSM with a coherent set of rules applicable for all EU citizens[92]. The data economy is described as 'an ecosystem of different types of market players […] collaborating to ensure that data is accessible and usable. This enables the market players to extract value from this data, by creating a variety of applications with a great potential to improve daily life[93]'. To accomplish the free flow of data,

---

[90] European Commission (2017c), *supra* 76, page 2.

[91] European Commission (2017c), *supra* 76, page 6-9.

[92] European Commission (2017c), *supra* 76.

[93] European Commission (2017c), *supra* 76, page 2.

the EC claims the elimination of mostly local restrictions, relating on the location of data storage or processing purposes. Through unjustified data location restrictions the freedom to provide services is impaired. Here, the EC sees an interference with secondary law, referring to the GDPR and the focus on the creation of a single market and thus, general guidelines relevant to all EU Member States. In order to remove unjustified data restrictions, the EC collects the individual evidence of the restrictions and assesses the impact to take justified and appropriate follow-up actions and address the issue. Local data restrictions in EU Member States should only be preserved if they are necessary to ensure the national security or similar objects[94].

Both communication papers serve as a basis for a dialogue with stakeholders to identify policy measures needed to realize a data economy in a DSM and to develop guiding strategies on the follow-up actions. In this section the importance of a data economy in the EC's strategy on big data became clear. The main actions claimed to achieve a DSM and thus, a data economy to successfully operate in times of big data, were examined. Moreover, a development regarding the implementation can be identified: While the strategy in 2014 mainly focused on the development towards a data economy, in 2017 privacy concerns are taken into consideration and the strategy is adjusted. However, the communication papers do not only propose actions, they also raise challenges. The realization of the communication papers is questionable as the demands are formulated rather inconcrete. Moreover, the different approaches regarding big data among the EU Member States and the environmental structure have to be adjusted. Thus, it is likely that it needs time to realize the DSM and a data-driven economy. Nevertheless, the rivals do not rest and the technological age is already in its heydays. To analyze the competitive situation, the next section emphasizes the EU's interests in a data economy, how the interests are related to third countries and the EU's position in the world economy.

3.2 The EU's interest in a data economy regarding relations to third countries

In the communication papers presented in the previous section, the enormous potential of a data economy are yield. This section emphasizes the EU's interest in a data economy and focuses on the competition with third countries. The increasing use of big data does not only offer chances to improve the individuals daily life, but also, to positively influence the EU's capital and overall gross domestic product (GDP). Implementing the proposed strategies, the EC expects an overall EU GDP growth of 3.17% by 2020, provided that the regulative frameworks are adapted towards a data economy. Through the growth of 3.17%, the value increases to 643 billion Euro (EUR) by 2020[95]. Thus, the EU has an internal interest in providing a data economy in their strategy on big data.

Still, the interest is not only based on internal demands: The EU founds itself in a constant competition with third countries. As a single market including 28 countries, the EU is a major trading partner in the world. In the international context, the EU is next to China and the US, the

[94] European Commission (n.n.b), *supra* 42.

[95] European Commission (2017c), *supra* 76, page 2.

third largest partner regarding international trade[96]. This emphasizes the enormous potential of the EU of maintaining its position as a forerunner. Moreover, it shows that the EU relates on the international trade and is therefore, in need of competing with economically strong countries.

The EC published a communication paper, stating that 'for Europe, knowledge, innovation, intellectual property, services and the efficient use of resources are now the keys to competitiveness. […] But the EU is losing ground in high technology areas[97]'. This citation shows the urgent need of becoming an active trading partner in the digital sphere to compete with the global developments. Moreover, the Europe 2020 Competitiveness Report reveals that 'the EU continues to underperform in comparison to the United State and other advanced economies in terms of building a smart, innovation based, knowledge-driven economy[98]'. The research indicates, that in a worldwide competition, the EU lags behind using big data to create innovative and smart technologies.

Facing the comparison among EU Member States, a division into 'innovative rich' and 'innovative poor' economies can be identified. While the northern and north-Western European countries perform strongly, the southern, central and eastern European countries are lagging behind[99]. There is a risk of leaving EU Member States behind while competing with strong international parties. The growing competition with international parties in pioneer positions may cause that only developed EU Member States utilize the capacity of a data economy and thus, a stronger social disparity emerges. However the aim of the Europe 2020 Strategy is a smart, sustainable and inclusive economy. The Europe 2020 Strategy is the EU's ten-year growths strategy focussing on the creation of jobs and reduction of poverty. The strategy has been created to counteract the development of Japan, the US, China and South Korea and to be able to catch up with these economically strong countries. The Europe 2020 Strategy endorses a (digital) single market to attract foreign businesses and companies. Through a single market the regulative frameworks of all EU Member States have the same conditions[100].

Coming back to the EC's communication on 'Building a European Data Economy'[101], unjustified data localization does not only inhibit the internal economy, but also operations with third countries[102]. Therefore, the EC wants to remove unjustified international data localizations to stronger engage into international operations.

---

[96] European Union (n.n.), '*The economy*', available at https://europa.eu/european-union/about-eu/figures/economy_en.

[97] European Commission (n.n.d.), '*Global Europe competing in the world - A contribution to the EU's Growth and Jobs Strategy*', available at http://trade.ec.europa.eu/doclib/docs/2006/october/tradoc_130376.pdf.

[98] World Economic Forum (2014), '*The Europe 2020 Competitiveness Report - Building a More Competitive Europe*', 2014 Edition.

[99] World Economic Forum (2014), *supra* 98.

[100] European Commission (2010), '*Turning Europe into a true Innovative Union*', MEMO 10/473, available at http://europa.eu/rapid/press-release_MEMO-10-473_en.htm.

[101] The communication has been presented in the *section 3.1.2*.

[102] European Commission (2017c), *supra* 76, page 3-4.

This section indicated that the interest in a data economy is not only caused through internal motivation, but also due to international competition. The EU as a strong trading partner and competitor in the world's economy does not want to lag behind and thus, encounters the global developments towards a data-driven society.

3.3 Conclusion on the relationship between the European Commission's strategy on big data and the data economy

In the previous sections, the EC's strategy on big data and a data economy and the EU's interest in a data economy have been elaborated. This section indicates the relationship between the EC's strategy on big data and the data economy and thus, answers the second subquestion of the study: How is the big data strategy of the European Commission related to the data economy?

Big data as a transnational process does influence the world's international competition and the creation of a new market. All economically strong countries are interested in maintaining their position and to not fall behind in a data-driven society, which raises a strong competition. Through the development of a new market, former economically weaker countries have chances to impact the global economy as the digital age offers new opportunities. For economically less developed countries, the access to the digital age and big data usage may be easier as there are less regulative frameworks and restrictions. Therefore, big data enables chances for players that have not dominated the economy before and creates the risk of lagging behind for current world-beaters. However, as the DESI presents, the diverging standing points may cause higher inequalities. The changing 'nature of a global trend[103]' claims the efficient use of resources and 'knowledge, innovation, intellectual property and services[104]' for the EU to compete with other countries. Moreover, the trading policies and competition law of the EU have to be adjusted to the new developments[105].

The localization of data arouses new challenges: Digital data is permanently created through the use of digital devices and used by businesses for daily operations, by governments as a decision bases or by researchers to indicate trends or developments. However, the localization of data, restricts the free flow of data across borders and thus, the transnationality of digital data. Data localization restrictions have been created to protect privacy and security and to maintain internal economic growth. Nevertheless, data localization restrictions are not only seen as protection measurements, but also as 'serious, harmful, and unintended consequences to economies and citizens[106]'. Examples include the strict localization measures in China where all servers used for online publishing have to be located within China and thus, the access to information which is not produced internally is limited. This measurement indicates the missing

---

[103] World Economic Forum (2014), *supra* 98.

[104] World Economic Forum (2014), *supra* 98.

[105] World Economic Forum (2014), *supra* 98.

[106] Information Technology Industry Council (ITI) (2017), '*Data Localization*', available at https://www.itic.org/policy/forced-localization/data-localization.

freedom of press and information[107] and stresses possible critiques on localization restrictions. Having introduced into the challenges of data localization the connection between the data economy and protection of privacy becomes highly visible. Thus, the fourth chapter discusses big data and the data economy through the lense of privacy protection.

Emerging from this chapter, the EC's current strategy on big data is strongly linked to the DSM and thus, the data economy. As stated in the communication papers of the EC, the EC supports the evolving opportunity of big data and a data-driven economy and focuses on a business-oriented approach regarding big data. The study shows, that big data is a consequence of the digital era and the technological age. However, big data is not only the output, but also a tool to conquer in the technological age. While big data as an output cannot be regulated, big data as a tool needs regulation, not only economical-wise as indicated by this chapter, but also privacy-wise. Therefore, the next chapter stresses the individual's perspective on big data and raises issues of privacy and data protection (*section 4.1*). Moreover, the fragmentation of data and the principle of purpose and the emerging unsolved privacy are analyzed (*section 4.2*). Thus, the fourth chapter links big data and the data economy to the right of privacy and data protection. The current results evolving from the EC's strategy on big data are combined with the fundamental rights of the EU and therefore, challenges occurring in the field of big data and the data economy in regard with privacy and EU standards are enlightened.

4. BIG DATA AND THE DATA ECONOMY THROUGH THE LENSE OF THE RIGHT OF PRIVACY

In the previous chapters, the Maximillian Schrems case, the evolving principles and the related frameworks have been discussed, as well as the strategy of the European Commission (EC) on big data and its interest in a data-driven economy. This section introduces into the individuals' privacy concerns and the relationship of big data, the data economy and the right of privacy and data protection. While the previous chapter has stressed the business-oriented approach towards big data, this section focuses on the citizen-oriented approach and indicates the applicable frameworks to ensure privacy and data protection. First of all, an introduction in the right of privacy is given (*section 4.1*). Afterwards, the challenges related to big data are addressed in relation to the specific problem of data fragmentation (*section 4.2*). Finally, a conclusion will be made on the relationship of big data, the data economy and the right of privacy and an answer to the third subquestion is given: To what extent are human rights torn in between big data and the data economy (*section 4.3*)?

4.1 The general framework of the right of privacy and data protection

While the business-oriented approach focuses on a free market economy, enabling the free access of data and a strong competition among countries, the consumer-oriented approach tends towards

[107] Article 8 (3) China's Online Publishing Services Management Rules, available at https://chinacopyrightandmedia.wordpress.com/2016/02/04/online-publishing-service-management-rules/.

privacy and data protection regulations to ensure the individuals private space. The European Union (EU) currently proposes different regulative frameworks focusing on the right of privacy and data protection. To receive a more precise image of the right of privacy and data protection, this section presents the general frameworks and thus, refers to the definition of the right of privacy and data protection (*section 1.2.3.2*). A universal definition of the right of privacy is given in article 12 Universal Declaration of Human Rights (UDHR)[108]. Moreover, article 8 of the European Convention of Human Rights (ECHR) and article 7 of the Charter of Fundamental Rights of the European Union (CFREU) present general provisions for the right of privacy. Article 16 Treaty on the Functioning of the European Union (TFEU) ensures the data protection through its provision. Thus, not only the United Nations (UN), but also the EU includes the right of privacy in its human rights standards.

As the study analyzes the impact of the right do privacy and data protection on big data and the European Commission's strategy, the two terms have to be distinguished[109]. The right of privacy is a general human right ensuring 'private life' for individuals, online and offline. Evolving from the right of privacy, data protection has developed. Data protection is more specific and focuses on the digital sphere, whereas the right of privacy is a more general provision. The right of privacy restricts the interference with the individual's privacy to a minimum. Contrarydictory, the right to data protection focuses on how person-related data has to be treated. Even though both rights are closely linked, they cannot be seen as identical: first there has been the right of privacy, evolving from it data protection was included and regulates data individually. In the Maximillian Schrems case both rights were seen as violated. It shows that the rights often apply in the same context. By the infringement of data protection, often the right of privacy is pointed out as well.

The previously presented frameworks do not explicitly refer to the right of privacy and data protection in regard with big data. The legislative instruments were concluded before the technological age, however, as the provisions are general human rights they still exist in the digital sphere. The judgment of the Court of Justice of the European Union (CJEU) in the Maximillian Schrems case was based on article 7, 8 and 47 of the CFREU and has validated the general provisions even though they do not explicitly refer to the digital sphere. Moreover, the European area of freedom, security and justice (AFSJ) raises the issue of data protection as it is linked to the individual's fundamental rights and guarantees a high level of security[110]. It can be stated that human rights are general provisions, that are from an individual perspective always accessible. However, it is questionable if sector specific human rights provisions are needed or if the general provisions are sufficient to regulate big data? Are there rules on big data which respectfully incorporate human rights provisions? And do we regulate big data as an economic

---

[108] Article 12 UDHR: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

[109] A conceptualization of the terms 'right of privacy' and 'data protection' is given in *section 1.2.3.2*.

[110] Article 67 Treaty of the Functioning of the European Union.

service or entrepreneurial issue and are the rules compatible with human rights? These leading questions shall be answered throughout the chapter to emphasize the link between privacy concerns and the data economy.

But, to ensure the right of privacy and data protection in the digital sphere these general frameworks have to be adjusted. Due to the fundamental principle of conferral in the European Union law (article 4 and 5 TEU), only EU Member States can amend the treaties for the EU. The EU Member States can only decide unanimously. Thus, an improvement of sector specific regulations can be introduced by the EU institutions, while an update on human rights law and EU primary law involves the unanimity of all EU Member States. This is the reason why the following section focuses on secondary EU law in the sphere of privacy and data protection in the field of big data: the General Data Protection Regulation (GDPR) (*section 4.1.1*) and the proposed Regulation on Privacy and Electronic Communications (RPEC) (*section 4.1.2*). Both, the GDPR and the RPEC are announced in the DSM strategy to provide privacy and protection for all users and market players. Additionally, the initiative Charter of Digital Fundamental Rights of the European Union (CDFREU) is introduced (*section 4.1.3*)[111].

4.1.1 The General Data Protection Regulation

'The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established[112].' Thus, the GDPR still follows the same key principles as the previous directive, but is adjusted to today's challenges. Its adjustments strengthen the fundamental rights of the consumer. It has been adapted in April 2016 and applies from the 25 May 2018. The GDPR replaces the data protection directive (DPD) from 1995 and is the general provision of EU secondary law ensuring privacy and data protection. As presented in chapter one, the Lisbon treaty has introduced article 16 TFEU. Article 16 TFEU gives a specific competence to the EU in the sphere of privacy and data protection. The GDPR is the first instrument adopted on this provision.

In the following, the focus is on several of the adjustments made in the GDPR and their effects[113]. The main difference occurs in the scope of the application of the GDPR. The GDPR applies to all companies utilizing personal data of EU citizens. It is no longer relevant where the company or the company's server who is processing the data is located. The DPD has regulated the processing of data inside the EU and thus, the GDPR causes an increased territorial scope (article 3 GDPR). This increased territorial scope ensures EU standards for all EU citizens no matter where and by whom their data is stored, processed and utilized. In the DPD, the processing and tracing of data has been regulated by article 25 DPD, which assessed the adequate level of protection. Next to article 3 GDPR on the territorial scope, the principle on the adequacy

---

[111] Initiative of the Charter of Digital Fundamental Rights of the European Union, available at https://digitalcharta.eu/wp-content/uploads/2016/12/Digital-Charta-EN.pdf.

[112] EU GDPR Portal, '*GDPR Key Changes*', available at http://www.eugdpr.org/key-changes.html.

[113] EU GDPR Portal, *supra* 112.

has been transferred to the GDPR and is laid down in article 45 GDPR. Additionally, the conditions for consent have changed. Article 7 GDPR defines that the consent has to be given in a written and easy accessible declaration. Moreover, one has the right to withdraw his or her consent at any time. This change is relevant as it empowers the user. Next to these rather general changes, the subjects on data rights have changed. The GDPR includes the right to access in article 15 which means that the individual has the right to obtain whether or not personal data concerning him or here is being processed. This is a progress in the development of data protection rights and the right of privacy from the consumer perspective. In addition to the right of access, the right to be forgotten has been included (article 17). The right to be forgotten has been claimed by privacy activists as it offers the opportunity to correct and erase data produced by oneself. Moreover, the right of data portability is introduced in article 20. The right of data portability ensures that the individual is able to receive all personal data concerning him or her and thus, the consumer can decide if she or he wants to make use of the right to be forgotten. The right to data portability is linked to the right of access, however it differs in many ways. The right of data portability is not only a mechanism ensuring that the individual is able to receive all the data concerning him or her, additionally, it can be used to directly transfer data from one controller to the other. Thus, it facilitates services in a data economy and strongly refers to services where for example the individual uses his or her Facebook account to log in to other services. The principle of purpose is extensively discussed later in the study (*section 4.2*). All in all, it becomes visible that the GDPR has been adjusted to the current challenges due to the emerging use of big data. Next to general changes, the regulation ensures more privacy to the individual.

An other adjustment is that the directive from 1995 has been transformed to a regulation. While a directive sets out aims that all EU Member States have to achieve, it is left open how the EU Member States realize it. A regulation has to be applied in its entirety among all EU Member States, as well as public and private entities and thus, does not require any choices of form or method from the EU Member States. It is the stronger instrument of EU secondary law[114].

4.1.2 The proposal on the Regulation on Privacy and Electronic Communications

The RPEC has been proposed the 10 January 2017 in context with the Digital Single Market (DSM) and the adoption of the GDPR. The European Data Protection Supervisor (EDPS) states that the RPEC has been proposed as the former version of the Directive 95/46/EC was incoherent due to its concepts in regard of personal data processing[115]. The RPEC provides ‘a high level of privacy protection for users of electronic communications services and a level playing field for all market players[116]’ and thus, complements the current needs due to the

---

[114] Article 288 Treaty on the Functioning of the European Union.

[115] European Data Protection Supervisor, ‘*Opinion 5/2016*’, available at https://edps.europa.eu/sites/edp/files/publication/16-07-22_opinion_eprivacy_en.pdf.

[116] Proposal for a Regulation 2017/0003 (COD) 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)

development towards a data-driven economy and the increasing use of big data. The respect for privacy and communication are fundamental rights stated in the CFREU (article 7). Through the technological age and the introduction of the DSM, the field has been enlarged to a new sphere, the digital sphere, and thus, regulative frameworks have to be adapted to ensure the fundamental rights of the citizens of the EU.

The RPEC is strongly connected with the GDPR and the DSM and ensures consistency with the GDPR and the realization of the DSM strategy[117]. The RPEC enables certainty for citizens and businesses. It does not only ensure the protection of fundamental rights in regard with the respect for privacy, but also realizes the free movement of (electronic) data (article 1(2) RPEC). While the GDPR focuses on general regulations, the RPEC focuses on personal data gathered through electronic communications and is thus, 'lex specialis' to the GDPR. The RPEC is in accordance with the GDPR and cannot violate the GDPR[118]. It is discussed, that the RPEC might even overshadow the GDPR as its wide territorial scope on privacy, internet of things and data protection related to devices covers the full range[119]. However, through the implementation of the GDPR and the RPEC the EU distinguishes clearly between the two fundamental rights and both are recognized as necessary. Through the implementation of article 7 of the CFREU into the RPEC it is included in EU secondary law[120]. While article 7 CFREU is rather abstract, the RPEC has several articles focusing on the realization of the right of privacy and extends the right of privacy to the digital sphere.

The RPEC is a regulation focusing on the digital sphere and data generated through the use of electronic devices. Therefore, it can be seen as a pioneer in the field of frameworks regulating the technological age. Complementary to the GDPR, the RPEC is a regulation whereas the former framework has been a directive, thus the coherence among EU Member States is ensured. However, critical voices comment that the RPEC is lacking in the field of metadata which should be treated more sensitive[121]. But not only privacy activist criticize the RPEC, due to its citizen-oriented approach, businesses fear the outcome as their market will be restricted by the RPEC.

4.1.3 The Charter of Digital Fundamental Rights of the European Union

Next to the legislative instruments analyzed above, a citizens' initiative has designed the CDFREU to boost the discourse about legal rights in the digital sphere. The EU has been criticized for its democratic deficit[122], thus article 11 of the Lisbon Treaty lays down an instrument for citizens to actively participate in the EU's policy process: a European citizen

---

[117] Proposal for a Regulation 2017/0003 (COD), *supra* 116, page 2.

[118] Proposal for a Regulation 2017/0003 (COD), *supra* 116, page 2.

[119] Gabriela Zanfir-Fortuna (2017), '*Will the ePrivacy Regulation overshadow the GDPR in the age of IoT?*', available at https://iapp.org/news/a/will-the-eprivacy-reg-overshadow-the-gdpr-in-the-age-of-iot/.

[120] Article 7 of the Charter of Fundamental Rights of the European Union focuses on the respect for private and family life.

[121] J. Backer (2016), '*EPrivacy leaked draft: The 'good', the 'bad' and the 'missing'*', available at https://iapp.org/news/a/eprivacy-leaked-draft-the-good-the-bad-and-the-missing/.

[122] The term 'democratic deficit' is defined in *supra* 74.

initiative (ECI). A ECI is 'the invitation to the EC to propose legislation on matters where the EU has competence to legislate[123]'. It has to come from at least 7 EU Member States and initiated by at least one million EU citizens. Once the ECI meet the requirements the EC meets the organizer within three months. The EC has to reason in a formal matter what action will be taken in response to the initiative and argue why or why not to do so. Additionally, the organizer receives the opportunity of a public hearing in the European Parliament (EP). Thus, a ECI is communicated to the EC, the initiative organ of the EU, and the only democratically assigned institution, the EP[124]. It offers citizens the opportunity to yield their claims and to receive a proper answer from the EU institutions. However, many citizens criticize that the ECI should become more user-friendly and practical. The strict timeframe, liability[125], big amount of information needed[126] and the high rate of initiative declared as inadmissible by the EC during the first phase[127] cause resistance by the EU citizens. In the following a ECI on fundamental rights in the digital sphere is analyzed.

As the initiative represents the emerging discussion about fundamental rights in the digital sphere it is included in the study. The CDFREU has been presented to the European Parliament in 2016 and EU citizens are invited to participate and discuss the proposal. The CDFREU presents fundamental rights in the digital sphere and shall provide a fundament for a civil discussion about fundamental rights in the technological age. The CDFREU relates to the fundamental rights of the EU including human dignity (article 1), freedom (article 2), equality (article 3), internal and external security (article 4), and freedom of opinion and openness (article 5). Facing these fundamental rights, it can be critically assessed that these fundamental rights are already ensured through the CFREU[128]. A repetition does not cause a better ensurance, therefore, it can be stated that these general provisions do not need sector specific regulations. However, next to the fundamental rights, the 23 articles discuss the most relevant issues raised by the technological age and do focus on algorithms (article 7), artificial intelligence (article 8), data protection and sovereignty (article 11) and net neutrality (article 16). Nevertheless, the citizens' initiative does not only focus on a citizen-oriented approach, but does also emphasize plurality and competition (article 17)[129]. It has to be pointed out, that the CDFREU proposes actions needed due to the

---

[123] European Commission (n.n.e.), '*The European citizens' initiative*', available at http://ec.europa.eu/citizens-initiative/public/welcome.

[124] European Commission (n.n.e.), *supra* 123.

[125] Article 13 Regulation (EU 2011/211) on the citizens' initiative makes the organizer liable for any damage they cause in the organization of a citizens' initiative in accordance with applicable national law.

[126] Annex II Regulation (EU2011/211) on the citizens' initiative involves all the required information for registering a proposed citizens' initiative.

[127] Around 40% of the initiatives are declared inadmissible, available at http://www.eesc.europa.eu/?i=portal.en.news.38442.

[128] Article 1 Charter of Fundamental Rights of the European Union does already ensure the human dignity, thus the Charter of Digital Fundamental Rights of the European Union is repetitive in some sections.

[129] Initiative of the Charter of Digital Fundamental Rights of the European Union, available at https://digitalcharta.eu/wp-content/uploads/2016/12/Digital-Charta-EN.pdf.

technological age and focuses on including stronger digital rights in the charter of fundamental rights, however, it duplicates a lot. All in all, the initiative raises awareness for the need of digital fundamental rights and proposes a regulative framework, but not all of the articles are necessary and the focus should rather be only on the regulation of big data and new technologies in the digital age as the general fundamental rights do apply to the technological age and are ensured in the UDHR, ECHR, CFREU and the TFEU (*section 1.2.3.2 and section 4.1*).

This section shows that the right of privacy and data protection is extensively discussed in times of an emerging use of big data. However, there are diverging interests by the data-driven economy and privacy-activists. Therefore, the next section deals with unsolved privacy issues in relation to big data and the data economy.

4.2 Unsolved privacy concerns and the data economy

Facing the challenges of privacy and data protection, a relationship to big data and the data-driven economy becomes clear. Without emerging interests in personal data processing, most of the privacy regulations would not be necessary. However, in a society where more and more data is used to compete in a growing market based on personal data, stronger privacy and data protection regulations are needed to ensure the humanitarian standards of the EU.

Currently, one of the main challenges is to link the right of privacy to big data and the digital sphere and thus, a data-driven economy. To ensure human rights standards in the technological age, regulative frameworks have to be enlarged to the digital sphere. Stronger digital privacy and data protection can be found in EU secondary law, however, as the EU institutions themselves cannot change EU primary law, the EU Member States are in need to incorporate the digital sphere into EU primary law. The previous section shows, that regulative frameworks concluded by the EU[130] currently develop to be applied to the online and offline sphere.

In the following a concise example of diverging interests between businesses and individuals is analyzed: Data fragmentation and emerging risks are presented to state the close connection between big data usage and the right of privacy. For individuals as well as businesses the storage and fragmentation of data is an important subject. Once data is produced, it has to be stored and thus, datasets are usually broken up into smaller fragments to facilitate the storage and distribution process among multiple machines. This process is called the fragmentation of data. A daily life example for the fragmentation of data are cloud services. Smaller fragments are easier distributable than large fragments, thus, the respond time of the server can be decreased. The fragmentation of data is used for storage and operations and is an automated procedure. Different providers offer different sharding policies and usually, the user has no influence on the data fragmentation process itself, although some businesses offer a choice in the geographical zone of the server[131].

---

[130] As only secondary EU law can be concluded by the institutions itself, the development refers only to EU secondary law.

[131] CCSK Guide (2013), '*Data fragmentation*', available at https://ccskguide.org/data-fragmentation/.

The fragmentation of data causes risks and chances. As this study is about person-related data, the risk in data fragmentation is examined in a perspective only focusing on personal data. It enables shorter respond times of the servers and one could think that the fragmentation of data causes less risk as the information is stored in different places, hence, cyber attacks or the break down of a server is less harmful. But, as long as the fragmented data unleashes enough information to identify the user, the idea of storing data in different habitats to avoid abuse is not given. Thus, fragmented data should not contain personal information which can be redirected. Due to the increasing use of big data, the amounts of data that are processed have been proliferated. Therefore, more eloquent solutions dealing with new amounts of data have to be invented. More and more businesses rely on data fragmentation to handle the amounts of big data. Digital devices produce big data that is stored and processed in servers as businesses rely on big data in a data-driven economy. This means, that the individual citizen is loosing track of its own data and cannot control what is stored, where it is stored and under which conditions. As presented in the Maximillian Schrems case, the fragmented data of Maximillian Schrems could be easily assigned to him and he received a 1,200 pages record.

Next to data fragmentation, another unsolved privacy concern revealing the diverging interests between a data economy and a strong emphasize on human rights standards in the EU is the principle of purpose protected by article 25 GDPR stating that personal data shall only be used for the signed purpose. The principle of purpose protects data protection by design and by default this includes that it shall be ensured 'that only personal data which are necessary for each specific purpose of the processing are processed. […] [And that] by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons[132]'.

However, to sign up for new services there are mostly two choices: either way the user receives access through his or her Facebook account or creates a new individual account for each service. For the sake of simplicity, most users make use of big data technologies and connect with their Facebook accounts. Once the data is used for multiple purposes it becomes difficult for the user to make use of the right of access and the right of data portability as most citizens do not keep track of the services they use. It is questionable if there is a way to combine a user- and data-friendly possibility that goes along with the human rights provision and flourishes the data economy. The insecurities and new technologies disclose uncertainties and unsolved privacy issues related to a data economy. To ensure human rights standards, the citizens have to claim their rights and be aware to not always confirm with the proposed options As this awareness cannot be included into the provisions and ensured by law, active and mature citizens are needed to minimize unsolved privacy concerns.

4.3 Conclusion on privacy and data protection in the context of big data

The study emphasizes in chapter three the EU's interests in a data-driven economy and the EC's strategy on big data. In this chapter we saw that the economic interests are extensively linked to

[132] Article 25 (2) General Data Protection Regulation.

privacy debates. The EC argues that 'the EU has the highest data protection standards in the world[133]', which is offering a coherent and privacy-oriented environment for individuals among the EU.

Through higher privacy standards, companies providing services in the EU have to offer their clients privacy-friendly services. Moreover, the Digital Single Market (DSM) ensures a coherent regulative framework among all EU Member States, which makes the EU an attractive market for innovative technology companies as they can offer the identical services all over the EU. As the rules do apply to EU and non-EU companies, having a server placed outside the EU becomes less attractive. The EC expects a growing economy as more businesses may settle down in the EU. In the past, the EU market has been rather unappealing due to its uncertainties and different regulative frameworks between the EU Member States. Through the coherence brought by the regulation, the EC anticipates a stronger and fair competition among the businesses as the EU offers henceforth, a large-scaled market for businesses[134]. This is also solving privacy concerns regarding the fragmentation of data. As the sharded data, contain sufficient information to identify the individual, the data has to be treated according to it and the process has to comply with the GDPR. Data fragmentation shows that through the GDPR, a new coherent regulative framework was conducted. As a result, the location does not release the businesses from the GDPR and to settle in other regions becomes less attractive.

The third subquestion demands to what extent human rights are torn in between big data and the data economy. To answer the subquestion to the full extend of this research, the Maximillian Schrems case has to be incorporated. The judgment of the Maximillian Schrems case has been decided in favor of the protection of human rights. Thus, even though the right of privacy is torn between big data and the data economy it is anything than less meaningful or powerful. This chapter identified that the regulative frameworks in EU secondary law are strongly adapted to the challenges and needs of a globalized data-driven economy and emphasizes the missing competence-competence of the EU institutions. On the one hand, the dependence on the EU Member States to recreate EU primary law limits the chances of sector specific human rights provisions. On the other hand, there are existing general human rights provisions that do apply also to the digital sphere as long as it is not explicitly foreclosed. Thus, sector specific secondary law has to be conducted on big data to ensure human rights standards and regulate big data. These provisions adopt slowly and have to be adjusted to market developments. As analyzed in this chapter, the sector specific provisions are all laid down in secondary law and therefore, have to be in accordance with EU primary law and thus, human rights standards.

To realize the EC's interests in a competitive data-driven economy and the AFSJ, coherent and strong privacy and data protection regulations are needed, as well as the opportunity to enter the emerging market of big data usage. As identified before, law making is often a reactive process

---

[133] European Commission (2016c), '*The EU Data Protection Reform and Big Data Factsheet*', available at http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf, page 1.

[134] European Commission (2016c), *supra* 133.

and thus, reacts once challenges have emerged[135]. This indicates for the future, that the current general provisions may need to be updated to new challenges and cannot be seen as an ultimatum. The Maximillian Schrems case has shown that EU institutions have to control each other. However, they strongly rely on the cooperation of the EU Member States as they possess power in the legislative process. The diverging interests between privacy and a data-driven economy do not only require active citizens, but also a clear separation of power between the EU institutions to safeguard humanitarian standards and at the same time enable a flourishing economy. Thus, this chapter strongly links the field of big data and privacy protection and shows that it is a continuous process that cannot be ignored and is constantly in need to be updated.

5. THE EUROPEAN UNION'S INTERNAL STANDARDS IN REGARD WITH TRADE AGREEMENTS CONCERNING DATA-TRANSFERS WITH THIRD COUNTRIES

The Maximillian Schrems case is linked to the external sphere, as big data and the data economy are by definition transnational. Big data is not limited to national borders, as data is fluid. The growing interconnectedness and transfers of personal data to third countries emphasizes the transnational character of big data[136]. Moreover, Facebook's business is based on data and is an example for a company living off the data-driven economy. Facebook has been founded in the United States of America (US), nevertheless, it is offering its services nearly all over the world which stresses the transatlantic character of the data economy[137]. Hence, the Maximillian Schrems case indicates the transnational challenges regarding big data and its regulation[138].

This chapter analyzes agreements signed by the European Union (EU) and third countries on trade and partnership that may contain provisions regulating big data, the data economy and data protection. Therefore, it links the topics that were discussed in the previous chapters and enhances the challenges to an external level. This chapter answers the fourth and last subquestion of the study: To what extend are big data, the data economy and human rights considerations, in the sense of data protection, placed in the relationship of the EU and its external relations? To answer this subquestion, the chapter analyzes the EU's internal standards and principles on trade relations with third countries with the emphasis on the impact of the Maximillian Schrems case and the evolving consequences for the EU (*sections 5.1*). Moreover, the impact of the Maximillian Schrems case on comprehensive trade agreements is analyzed with a focus on recently negotiated trade agreements with economic partners of the EU. Therefore, the data protection clauses as well as the relation to big data and the data economy in the trade and partnership agreements are analyzed (*section 5.2*). In the end, the internal standards of the EU on

---

[135] D. J. B. Svantesson, *supra* 13.

[136] The transnationality of big data has been emphasized in *section 2.1*, p.18f.

[137] The connection between Facebook and the data economy are introduced in *section 2.3*, page 21.

[138] The case is extensively analyzed in chapter 2, *section 2.2*.

trade relations, in respect to big data, the data economy and data protection, with third countries are examined and the consequences for further agreements are stressed (*section 5.3*).

5.1 The European Union's internal standards and principles on trade relations with third countries

The Maximillian Schrems case introduces the transnational character, as it enlightens the tracing and processing of personal data across borders by Facebook[139]. As presented in the fourth chapter, the EU has regulated data protection internally; however, the transnational nature of the data economy and the use and marketing of big data — bring new dilemma, namely the level of data protection and privacy. Hence, this chapter introduces into the EU's internal standards and principles on trade agreements with third countries.

First of all, the European Commission's (EC) general understanding of trade agreements is presented. The EC states that 'the EU negotiates trade agreements to strengthen our economy and create jobs[140]'. Trade agreements offer the opportunity for EU businesses to compete globally. They allow a connective economy with the expertise of transnational companies. Through the access to the latest technologies, the local economy as well as job offers profit. Moreover, the EU relies on raw material and other goods and services from around the world. In general there are three main types of trade agreements: Custom Union, Partnership and Cooperation Agreements and Association Agreements, including Stabilization Agreements, Free Trade Agreements and Economic Partnership Agreements[141]. The study focuses on bilateral trade and partnership agreements that may contain regulative provisions on big data, the data economy and data protection. After having analyzed the general understanding and range of trade agreements, the next section emphasizes the EU's internal standards on comprehensive trade agreements with third countries regarding data transfers.

Through the Lisbon Treaty in 2009, one of the general internal provisions regarding the EU's external action has been extended. The European Union's main external trade policy is the Common Commercial Policy (CCP). As the study focuses on the interaction of big data, the data economy and data protection and the play field is transnational, the CCP and its scope have to be taken into consideration. In article 1(3) Treaty of the European Union it is determined that 'the Union shall ensure consistency between the different areas of its external action […]'. The CCP, laid down in article 207 Treaty of the Functioning of the European Union (TFEU), aims at the conclusion of trade agreements with third countries on the basis of common principles established among the EU Member States. The scope of this policy has been extended by the Lisbon Treaty in 2009. Through the adjustments, the role of the European Parliament (EP) has been reinforced as it has to give its compliance to external trade agreements and the Commission

---

[139] The tracing and processing of person-related data by Facebook is stressed in *section 2.2*, p. 19f.

[140] European Commission (n.n.f.), '*Trade Agreements*', available at http://ec.europa.eu/trade/policy/countries-and-regions/agreements/.

[141] European Commission (n.n.f.), *supra* 140.

is in need to regularly report about negotiations to the EP[142]. Before the Lisbon Treaty, the EP's approval was not necessary to negotiate agreements with third countries. Thus, through the development the democratic deficit[143] is countered. In addition to the empowerment of the EP, the Lisbon Treaty extends the scope of the CCP and thus, clarifies and simplifies the conclusion of trade agreements with third countries[144]. The main development in the Lisbon Treaty regarding the CCP is that it includes foreign direct investment which means that the EU has the competence to conclude bilateral investment treaties in most sectors[145]. In the TFEU a plurality of necessities needed to conclude agreements with international organizations are given[146]. Agreements concluded by the EU are binding on all EU institutions and EU Member States[147]. The procedure on how to conclude an agreement with a third country is laid down in article 218 TFEU. Thus, the mechanisms as well as the purpose of trade agreement are regulated by EU primary law.

Also in regard with data transfers, the EU reposes on internal standards. In 2016 Jean-Claude Juncker stated that '[b]eing European means the right to have your personal data protected by strong, European laws. […] Because in Europe, privacy matters. This is a question of human dignity[148]'. Thus, since the General Data Protection Regulation (GDPR) came into force, data protection of EU citizens is not limited to the territorial scope of the EU anymore. Article 3 GDPR states that it applies to the processing of personal data, irrespective where the data is processed. The former article 25 Data Protection Directive (DPD), which held that data transfers with third countries must ensure an adequate level of protection, is laid down in article 45 GDPR, has been expanded to today's challenges and comprises mechanisms that have to be taken into consideration to determine the level of adequacy. As chapter two clarified, the Maximillian Schrems case shows that an adequate level of protection is difficult to assess because the national laws of third countries have to be taken into consideration[149]. Moreover, the assessment of the adequacy is rather subject as no general procedure can be applied[150]. Thus, article 3 GDPR is an improvement as it sets EU standards as a benchmark in the field of privacy and data protection. The point of origin of the data traced or processed is the ultimate benchmark and not the location of the business. Consequently, the Maximillian Schrems case has influenced the privacy and data protection. From a European perspective, the level of data protection is thus, taken out of the

---

[142] This is stated in article 207 (2) and article 218 (6) Treaty on the Functioning of the European Union.

[143] The term 'democratic deficit' is defined in *supra* 74.

[144] The scope is defined in article 207 (1) Treaty on the Functioning of the European Union.

[145] A. Pollet-Fort (2010), '*Implications of the Lisbon Treaty for the European Union External Trade Policy (Common Commercial Policy)*', EU Centre in Singapore, Background Brief No 2.

[146] The necessities are laid down in 'Title V International Agreements' Article 216-219 TFEU.

[147] Article 216 (2) Treaty of the Functioning of the European Union.

[148] European Commission (2017f), '*Exchanging and Protecting Personal Data in a Globalised World*', COM (2017) 7 final.

[149] The term 'adequacy' has been assessed in *section 2.1*, p.16.

[150] Article 45 (2) strikes the points that shall be taken into consideration by the Commission while assessing the level of adequacy, however, no mechanism is provided.

negotiating table. Hence, this chapter analyzes trade and partnership agreements with third countries (*section 5.2*).

Through the implementation of the GDPR an other agreement, similar to the Safe Harbor Decision (SHD), cannot be concluded, neither content-wise nor procedurally. Such an agreement cannot be concluded content-wise anymore, as article 3 GDPR states that internal data protection regulation have to be applied externally, thus data of EU citizens has to be treated according to EU law regardless of where the data os traced, stored or processed. Regarding the procedure the previous article 25 DPD has been transformed to article 45 GDPR. Thus, the adequate level of data protection is still assessed by the EC. However, article 45 (2) GDPR states more detailed which elements shall be taken into consideration while assessing the adequacy. Compared to the DPD this ensures that the level of adequacy is assessed after a — even though broad — mechanism.

Article 3 GDPR is a general provision and hence, applicable anywhere for the processing of data. As a general provision, the GDPR impacts agreements, companies and the EU citizens. Article 3 GDPR is setting the general guidelines, however, it does not restrict individual agreements from implementing higher standards. The EU's internal standards regarding privacy and data protection have risen, however, it is questionable how the application of article 3 GDPR influences further trade and partnership agreements, as third countries with a less regulated data-driven economy may profit less from trade agreements with the EU. However, third countries do profit from the internal coherence of the EU standards through the GDPR. Thus, a Digital Single Market (DSM) can have positive and negative effects. The future will show the impact of the GDPR on future trade relationships of the EU.

In the following, the impact between trade relations and data protection are further analyzed by looking at recently concluded trade agreements with third countries and long-term partners of the EU. During the legal force of the DPD, the Commission had the power to assess whether a third country protects personal data adequately[151]. In addition to that, the GDPR has strengthened coherent regulations among the EU Member States, which have to be taken into consideration by trading partners[152].

All in all, this section shows that the EU strongly relies on internal standards on the conclusion of trade and partnership agreements with third countries. As the provisions have changed over the past years a shift of power can be identified. Moreover, the data protection provisions became stricter and coherent among the EU Member States. In the following section the influence of big data, the data economy and data protection trade and partnership agreements with third countries are identified through the lense on the EU's internal standards.

5.2 Recent Trade and Partnership Agreements with Third Countries

In this section, recently negotiated trade and partnership agreements with the EU and third countries are analyzed to examine the influence the Maximillian Schrems case may have on those

[151] Article 25 Data Protection Directive.

[152] Article 3 and 45 General Data Protection Regulation.

agreements. The emphasis of this section is on how data protection is regulated in these trade agreements and if big data and the data economy are regulated. As big data can be seen as a good, it belongs to the field of trade and may be explicitly mentioned in trade agreements. The agreements are analyzed in chronological order: the EU-South Korea Free Trade Agreement (FTA), the Comprehensive Economic Trade Agreement between the European Union and Canada (CETA), the EU-Singapore FTA, the EU-Japan FTA and the Transatlantic Trade and Investment Partnership (TTIP) between the EU and the United States of America (US). An external provision for trade and partnership agreements is the World Trade Organizations' General Agreement on Trade Services (GATS). It is a general provision regulating trade on services. It applies to all of the following analyzed trade agreements as they are based on services and states that all trading partners have to be treated equal[153].

5.2.1 The EU-South Korea Free Trade Agreement

The FTA between the EU and the Republic of Korea was signed on 6 October 2010 and entered into force on 13 December 2015[154]. The EU-South Korea FTA is of the first generation of trade agreements after the Lisbon Treaty and is the EU's first trade deal with an Asian country. The FTA has been signed before the Maximillian Schrems case evoked and the GDPR was concluded.

In chapter seven on trade in services, establishment and electronic commerce of the FTA a link to the DPD and thus, the protection of data, and a data economy can be identified. First of all, it is laid down, that each party has to treat the services and suppliers of the other party as favorable as its own services and suppliers[155]. Moreover, article 7.43 (b) aims on adequate safeguards to ensure the protection of privacy and personal data. This article founds itself in a relation to the rights and freedoms indicated by the Universal Declaration of Human Rights[156], the Guidelines for the Regulation of Computerized Personal Data Files[157] and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data as both parties are members of these provisions. The OECD Privacy Frameworks includes the connection between big data and data protection challenges and therefore, indicates the transnationality[158].

Article 7.43 is based on the commitment to previously concluded regulative framework. Moreover, the term 'adequacy' connects the FTA between the EU and South Korea to the DPD.

---

[153] A. Bendiek & E. Schmieg (2016), '*European Union Data Protection and External Trade - Having the Best of Both Worlds?*', German Institute for International and Security Affairs.

[154] Free Trade Agreement between the EU and the Republic of Korea, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2011:127:FULL&from=EN.

[155] Article 7.6 National Treatment FTA between the EU and South Korea.

[156] The right of privacy is laid down in article 12 of the Universal Declaration of Human Rights, *section 1.2.3.2*, p.13.

[157] The Guidelines encourage the minimum guarantees for national legislation regarding computerized data files. Next to the internal character of the guidelines, article 9 emphasizes the external character and states that comparable safeguards in regard of privacy protection of two or more parties shall enable a free flow of information, available at http://www.refworld.org/pdfid/3ddcafaac.pdf.

[158] The OECD Privacy Framework (2013), p.42 and p.83.

Next to the previously presented provisions, 'section F' focuses on electronic commerce and indicates that international data protection standards shall ensure the confidence of the user[159]. Article 7.48 (1) emphasizes the economic growth and trade opportunities in the field of electronic commerce and thus, relates to a data-driven economy or even big data. Even though these terms are not mentioned and have probably not explicitly be taken into consideration while signing the FTA, a flourishing electronic economy shall be promoted. Therefore, it can be stated that the way towards a data economy is paved. However, as the agreement has been signed in 2010, the GDPR has not been taken into consideration, thus, the enlargement of the FTA will cause the recognition of the GDPR, including article 3.

However, to sum up, it can be stated that even the agreement that has been signed and entered into force the earliest, does already provide privacy and data protection provisions. Nevertheless, they are not directly linked to the EU law, they only refer to the DPD using the terminology 'adequate'. Apart from that, the focus is on international provisions that can be used as a fundament and reference as both parties have approved to them.

5.2.2 The Comprehensive Economic Trade Agreement between the European Union and Canada (CETA)

In this section, the focus is on a comprehensive trade agreement between the EU and Canada. CETA shall encourage the bilateral trade of goods and services between both parties. All EU Member States approved the negotiations concluded in August 2014. On 30 October 2016, Justin Trudeau, the Prime Minister of Canada, has signed the trade agreement on behalf of Canada in Brussels.

In 2001, the EU considered for the purpose of data protection, that Canada has an adequate level of protection in relation to the DPD[160]. The CETA has been concluded with the expectation that not only goods and services will be exchanged, but also an increasing volume of consumer and employee data was expected to flow into Canada from the EU. Therefore, the comprehensive trade agreement has been included with the idea of incorporating big data and the data economy to strengthen the economy and create jobs.

As the negotiation process took place after the Maximillian Schrems case, the case study had an influence on the comprehensive trade agreement. Motivated by the Maximillian Schrems case the EP's Committee on Civil Liberties, Justice and Home Affairs (LIBE) has risen concerns in 2013 and demanded a review of the Canadian privacy regime[161]. In the past, Canada was accused to share identifiable metadata of its citizens with countries of the Five Eyes Alliance[162]. This

---

[159] Article 7.48 (2) Electronic Commerce, Objective and Principles FTA between the EU and South Korea.

[160] The term 'adequate' and the Data Protection Directive are analyzed in *section 2.1*, p.16.

[161] Colin J. Bennet (n.n.), 'I*s Canada still 'adequate' under the new European General Data Protection Regulation*', available at http://www.colinbennett.ca/data-protection/is-canada-still-adequate-under-the-new-general-data-protection-regulation/.

[162] The Five Eyes Alliance incorporates the US, Canada, UK, Australia and New Zealand and is an intelligence alliances.

caused European concerns as personal data may not be adequately protected. However, through the implementation and the on-going negotiation process, the GDPR and Canadian privacy law were taken into consideration.

Comparable to the GDPR provision, Canada has a data privacy relating law: the Personal Information Protection and Electronic Documents Act (PIPEDA). The PIPEDA is a federal privacy law for private-sector organizations and regulates how businesses have to deal with personal information and person-related data. Even though, both parties ensure the right of privacy and data protection through their individual laws, they differ. While both legislative frameworks ensure the right of access, the GDPR includes, unlike the PIPEDA, the right to data portability in article 20 GDPR[163]. As a result, the EU's regulation offers the individual more information and stronger control over the individual data. Next to the right of data portability, the GDPR incorporates the right to erasure, also known as the right to be forgotten. Complementary to article 17 GDPR, PIPEDA comprises a basic right to be forgotten as it states that 'personal information shall be retained only as long as necessary for the fulfillment of those purposes[164]'. Thus, based on the PIPEDA, there is no explicit right of erasure, it is only stated that businesses shall not store and process unnecessary data. These are only several examples on how the legislative frameworks differ. Subsequently, it can be stated that the individuals privacy and data is more protected by the GDPR than by the PIPEDA.

However as CETA is an individual agreement, this section analyzes to which degree CETA includes the right of privacy and data protection. In article 13.15 CETA the focus is on the transfer and process of information.

> Article 13.15 (2) CETA
> Each Party shall maintain adequate safeguards to protect privacy, in particular with regard to the transfer of personal information. If the transfer of financial information involves personal information, such transfers should be in accordance with the legislation governing the protection of personal information of the territory of the Party where the transfer has originated.

Evolving from this article influences of the DPD and the GDPR can be identified. While the DPD has shaped the adequacy of safeguards, the GDPR has its influence regarding the fact that the person-related data shall be treated according to the legislation of the party where the transfer has originated. This section strongly relies to article 3 GDPR which states that the regulation applies regardless whether the processing takes place in the Union or not. Resulting from article 13.15 CETA, data originating from the EU has to be treated according to EU law even though it is processed in Canada and vise-versa.

---

[163] The terms 'right of access' and 'right to data portability' are distinguished in *section 4.1.1*, p. 33.

[164] Principle 4.5 of Schedule 1 Personal Information Protection and Electronic Documents Act.

Having analyzed the privacy and data protection of the CETA an impact of the Maximillian Schrems case can be identified. Before the Maximillian Schrems case, trade agreements with third countries have been concluded on the basis of the adequacy of safeguards and international standards, the Maximillian Schrems case caused that introduction of the GDPR and thus, EU law is applicable for EU citizens no matter of the territorial scope. This progress has been included in the CETA and therefore, all person-related data from EU citizens that is exchanged on the basis of this trade agreement has to be treated according to the GDPR.

5.2.3 The EU-Singapore Free Trade Agreement (EUSFTA)

Singapore is the second Asian economy after South Korea[165] that has concluded a FTA with the EU. Moreover, Singapore is the first country of the Association of Southeast Asian Nations with a FTA with the EU. The negotiations were launched in 2010 and the agreement between the EU and Singapore has been concluded in October 2014[166].

The EUSFTA was built as an EU-only agreement, however on 2015 the Court of Justice of the EU (CJEU) was asked for an opinion to state which competences of the agreement fall within the EU's exclusive or shared competences and which remain exclusive competences of the EU Member States. In May 2017, the CJEU stated that agreement between the EU and Singapore also covers areas of shared competences and thus, has to be concluded as a mixed agreement with the approval of each individual EU Member State. Due to the long negotiation process the FTA is not ratified yet[167].

To analyze the impact big data, the data economy and data protection had on the trade and partnership agreement, the emphasis is on chapter nine EUSFTA dealing with investment and investment protection. In article 9.3 the reference is made to the national treatment, which has been incorporated in the previously presented FTA between the EU and South Korea. In the National treatment it is stated that the other party should not be treated less favorable than the own party. In article 9.3 (3) (d) (ii) EUSFTA, the protection of individuals in relation to the processing of personal data is laid down. Hence, even if the section focuses on investment, a provision focusing on the privacy and data protection of the individual is included in the FTA.

Next to the previously presented chapter nine, chapter eight of the EUSFTA focuses on services, establishment and electronic commerce. Article 8.54 EUSFTA encounters data processing and states that appropriate safeguards on privacy and confidentiality shall be taken in regard of data processing. Moreover, privacy and personal data shall be protected.

To sum up, it can be said that the FTA agreement between the EU and Singapore includes a provision incorporating the transnational phenomena of big data and the data economy on the agreement. Nevertheless, the protection of the individuals data and privacy is only given in the area of investment. Data protection is incorporated in the dimension that appropriate safeguards

---

[165] The free trade agreement between the EU and South Korea is analyzed in *section 5.2.1*.

[166] European Parliament (2017), '*EU-US Singapore Free Trade Agreement - Stimulus for negotiations in the region*', available at http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/607255/EPRS_BRI(2017)607255_EN.pdf.

[167] European Parliament (2017), *supra* 166, p.3.

need to be taken in the field of investment. Hence, in some aspects privacy and data protection are covered, but there is no general provision applicable for the entire FTA agreement between the EU and Singapore. The agreement has been finalized before the GDPR was discussed. Therefore it is based on the DPD, which can be seen in article 8.54 EUSFTA. It will be interesting to see, if the GDPR impacts the free trade agreement between the EU and Singapore once the framework comes into force in May 2018.

5.2.4 The EU-Japan Free Trade Agreement

In 2013 the negotiations of the EU-Japan FTA were launched. However, there have been multiple rounds of negotiations since then. The 18th round took place from the 3 until the 5 April 2017 in Tokyo between Jean-Claude Juncker, Donald Tusk and the Prime Minister Abe. After China, Japan is the EU's second biggest trading partner in Asia, Moreover, Japan is one of the major investors in EU. Thus, a trade and partnership agreement offers an increasing market and new opportunities for both parties. In the world's comparison, Japan is the fourth largest national economy. As the negotiation process is in progress, this section is based on the report of the 18th EU-Japan FTA negotiating round[168]. The EU aims on finalizing the negotiation process until July 2017, before the G-20 takes place[169].

The report covers six different topics regarding the trade agreement between the EU and Japan: trade in goods, non-tariff measures, rules of origin, services, procurement and intellectual property rights. In the fourth section on services, an emphasis is on cross-border trade and the free flow of data. Japan is interested in enabling the free flow of data and the prohibition of data localization requirements. The EU stated that this section is to be discussed internally[170].

To sum up, it can be stated that the details of the FTA between Japan and the EU are not published yet. However, from the report it can be analyzed that big data and the data economy has an impact on the agreement. Moreover, the report shows that Japan wants a rather open deal, whereas the EU tends to solve this diverging interest internally. Due to the internal standards and provisions of the EU an open deal with Japan means that Japan has to acknowledge all data protection and privacy standards laid down in the GDPR. In addition to that, the adequacy of Japan has not been assessed yet, thus, Japan still has to present an adequate level of data protection to incorporate the trade of data between the EU and Japan in the free trade agreement. All in all, this agreement founds itself still at an early time, therefore, the following negotiation rounds have to show how data protection and privacy are incorporated and hence, the data economy between Japan and the EU is enabled.

---

[168] European Commission (2017g), '*Report of the 18th EU-Japan FTA/EPA negotiating round*', available at http://trade.ec.europa.eu/doclib/docs/2017/april/tradoc_155506.pdf.

[169] D. Brössler & A. Mühlauer (22.06.2017), '*EU strebt Handelsabkommen mit Japan an*', Süddeutsche Zeitung.

[170] European Commission (2017g), *supra* 168, p.3.

5.2.5 The Transatlantic Trade and Investment Partnership between the European Union and the United States of America (TTIP)

The Transatlantic Trade and Investment Partnership is a proposed trade and partnership agreement between the EU and the US. Originally, the agreement should have been negotiated until 2014. However, the process is on-going and the documents are not public. Nevertheless, some leaks came to the public and enable to discuss the present state of the trade and partnership agreement in this study.

In the leaks, a chapter dealing with electronic communications can be identified. The TTIP strongly focuses on a data economy as the access and use for enterprises of the other party is highlighted[171]. The interconnectedness of electronic services is highly emphasized and shall enable a greater competition on the market and empower the economy. In article 48 TTIP it is stated that each party shall ensure confidentiality of electronic communications and the processed data. However, no mechanism is identified. The data protection in the bilateral negotiated trade and partnership discussion is strongly debated. The previously discussed parts of TTIP, seek for a liberalization of the service sector and focus on a data-driven economy. Data protection activists fear that TTIP undermines the EU privacy and data protection standards. From the US perspective, it is strongly discussed to what extent a fundamental right such as the right of privacy can be incorporated into a trade agreement as both parties take an opposing view on privacy and data protection: the US has a strong interest in a free international exchange of data, whereas the EU wants to empower the economy whilst ensuring human rights standards[172].

An US-lobby association led by Google, Facebook and IBM strongly claims the inclusion of the free flow of data into the agreement and thus, seek to incorporate an interoperability clause. However, as the jurisdiction of the CJEU on Maximillian Schrems has shown, that previously concluded agreements between the EU and the US have lacked data protection provisions. Thus, it will be interesting to see, to which degree the EU tries to incorporate their standards on privacy and data protection in the trade and partnership agreement. In 2015, the European Parliament required that the EX shall include European fundamental rights, such as EU data protection law, in the TTIP. In 2015, the GDPR was not concluded and therefore, the argumentation of the EP is based on article XIV GATS and that a provision stating that the full application of EU data protection rules is guaranteed and respected. The LIBE committee claims that the Commission shall an adequate and high data protection standard[173]. Anyhow, the report of the latest round of negotiations shows, that privacy and data protection have not been discussed[174].

---

171 The article is not numbered, but is expected to be in the 40s.

172 A. Bendiek & E. Schmieg (2016), *supra* 153.

173 European Parliament (2015), 'TTIP: Trade agreements must not undermine EU data protection laws, say Civil Liberties MEP's', available at http://www.europarl.europa.eu/news/en/press-room/20150330IPR39308/ttip-trade-agreements-must-not-undermine-eu-data-protection-laws-say-meps.

174 European Commission (2017h), '*Report of the 14th Round of Negotiations for the Transatlantic Trade and Investment Partnership*', available at http://trade.ec.europa.eu/doclib/docs/2016/august/tradoc_154837.pdf.

It has to be taken into consideration, that the EU's reform on data protection influences the agreement as it has not been concluded yet and is not expected to be negotiated before the GDPR comes into force.

5.3 Conclusion on the European Union's internal standards in regard with trade agreements concerning data-transfers with third countries

As analyzed in the previous sections, the Maximillian Schrems case has an influence on the conclusion of trade agreements with third countries. While data protection clauses have not been discussed extensively before the Maximillian Schrems case and the GDPR, the later concluded trade agreements have been criticized by privacy activists, as well as by the European Parliament once they do not incorporate data protection and privacy provisions. Trade agreements concluded before the jurisdiction on the Maximillian Schrems case rely on the GATS and other international provisions or individually concluded frameworks between the EU and a third country. Moreover, the adequate level of data protection has been assessed according to article 25 Data Protection Directive and later article 45 General Data Protection Regulation.

It can be identified that all analyzed trade and partnership agreements between the EU and third countries somehow incorporate the exchange of data or data-related services. Though, the degree to which big data usage and the transfer of person-related data is incorporated varies. This once more identifies the strong connection between human rights standards and a data-driven economy in the field of big data usage.

Most of the agreements contain, next to the general frameworks, sector specific provisions such as the EU-US Privacy Shield discussed in chapter two and the trade and partnership agreements analyzed in this chapter. While general provisions are applicable in all situations and for all fields, sector specific regulations do only regulate a specific field of action. Hence, general provisions do ensure a general stability and coherence, whereas specific provisions can further regulate sectors which are not sufficient controlled yet. Big data as an emerging technology cannot be regulated through sector specific provisions as they will have to be enlarged constantly over the next time. The study emphasizes that general provisions are needed to regulate human rights protection. Moreover, the general provisions serve as a benchmark for sector specific regulations which can be added on top if the general guidelines are insufficient. However, one has to keep in mind that the general provisions always serve as a fundament and hence, cannot be overridden by sector specific frameworks. Moreover, as the EU's internal standards present, general and coherent guidelines help to ensure a certain level of data protection. It should be taken into consideration, that the current status quo of the TTIP does not incorporate the GDPR and therefore, is not a sufficient basis for data transfers between the EU and the US.

Through the introduction of a DSM the idea of coherent regulative frameworks among EU Member States is realized, which has influenced the conclusion of trade and partnership agreements as the national legislation of the EU Member States does not inhibit trade agreements with third countries through diverging legislation. Next to the DSM, the enlargement of the CCP through the Lisbon Treaty enhanced the influence of the policy and broadened its scope. The

coherent principles among the EU Member States help to conclude important trade agreements with third countries in a world that becomes more and more interconnected and globalized.

Regarding future trade agreements that the EU concludes with third countries, the GDPR can be seen as a fundament that has to be taken into consideration once the agreement includes person-related data of EU citizens. Therefore, Maximillian Schrems has not only influenced how the EU treats person-related data internally (*chapter 4*), but also externally. All in all, it can be stated that through the GDPR the EU's internal standards on how to conclude trade and partnership agreements with third countries has been complemented. The GDPR offers certainty, while before the term 'adequacy' had a leading role and could not ensure a particular level of protection. Thus, from a regulatory perspective the GDPR can bee seen as an improvement. However, the time will show if the GDPR sufficiently regulates data protection.

The fourth subquestion demanded: To what extend are big data, the data economy and human rights considerations, in the sense of data protection, placed in the relationship of the EU and its external relations? As analyzed in this chapter, the EU's internal standards are used to shape the external relations with third countries. The EU's behavior is based on its internal standards, as internal standards determine the EU's external actions[175]. As identified in the second, third and fourth chapter, the EU's internal regulation on big data is on its way, however, it has to be seen how it can be implemented externally while ensuring the internal standards. Thus, the Maximillian Schrems case was able to answer internal questions on data protection and privacy in the EU, but does not provide insurance of data protection when acting abroad, as the pooling of data due to security purposes is not ensured. However, as the degree of the study focuses on big data, the data economy and data protection of commercial data, it can be stated that the EU aims on defending its internal standards in external relations and that the introduction of the GDPR is a regulatory improvement as it causes coherence among the EU Member States which facilitates to protect internal standards externally. Moreover, the Maximillian Schrems case as a precedential case in the field of big data has shown how the transnational character of big data influences the internal and external standards of the European Union and identifies risks and chances emerging through the emerging use of big data.

6. Conclusion on the European Commission's Strategy on Big Data and Human Rights and the Data Economy

Through the technological age, big data becomes an increasingly more relevant topic in the world and for the European Union. New technologies require new regulations and reactions and offer chances and risks. The purpose of the study was to investigate to what extent the strategy of the European Commission on big data promotes a data-driven economy whilst respecting human rights standards. The research was inspired by the Maximillian Schrems case. It is a precedential case in the field of big data, presenting the interconnectedness of the European Commission's strategy on big data, a data-driven economy and European Union human rights standards. To tackle the main research question, four subquestions were identified.

[175] Part Five The Union's External Action Treaty on the Functioning of the European Union.

The first subquestion asked for the principles emerging from the Maximillian Schrems case on the relationship between human rights protection and a data-driven economy and has been answered in the second chapter. Chapter two identified the relationship between the Maximillian Schrems case and a data-driven economy. Next to the data-driven economy, the transnational character became visible as the relation between the EU and US does influence the case. The Safe Harbor Decision, an agreement between the EU and US, was declared as invalid due to the Maximillian Schrems case. Thus, the case caused the development of a new agreement: the EU-US Privacy Shield. Moreover, the developing regulative frameworks have been identified. While the Data Protection Directive was into force before the jurisdiction of the Maximillian Schrems case, the jurisdiction caused the implementation of the General Data Protection Regulation. All in all, the Maximillian Schrems case caused major changes in cross-border flow from a European perspective[176].

The second subquestion focused on the relation of the Commission's big data strategy and the data economy and has been solved in the third chapter. The study analyzed that the data economy causes a strong competition among countries and that economically strong countries are interested in maintaining their pioneer position and to not fall behind while former less economically strong countries seek their chance on a new developing market of big data services. Thus, a data-driven economy causes a high competition among countries. However, the EU Member States have diverging economic positions. Therefore, it has to be taken into consideration that due to a coherent strategy towards big data and the data economy inequalities are likely to increase. While some countries are lagging behind and cannot compete in the technological age as they still struggle with the access and utility of digital devices, and have not adopted to a data-driven economy yet other EU Member States are in direct competition with the world-wide forerunners[177].

The third subquestion investigated in the third chapter to what extent human rights are torn in between big data and the data economy. The third chapter pointed out that the economic interest of the European Union in a data-driven economy is extensively linked to privacy debates. The impact of the European Union's higher privacy standards and coherent regulative framework have been discussed. The General Data Protection Regulation ensures that person-related data from EU citizens' is treated according to EU standards regardless where the business or servers are placed. Thus, the aim is to defend internal standards externally. Through the coherent regulative framework among all European Union Member States, the EU market shall become more attractive as businesses can offer the same services and rely on the same regulations in all EU Member States. The third chapter identified that the Maximillian Schrems case showed that data protection and the right of privacy have highly influenced the field of big data and that human rights standards define the degree to which a data economy can be realized[178].

---

[176] Read chapter two for further information.

[177] Read chapter three for further information.

[178] Read chapter four for further information.

The fourth subquestion has been answered in the fifth chapter and demanded: To what extend are big data, the data economy and human rights considerations, in the sense of data protection, placed in the relationship of the EU and its external relations? In chapter four the internal standards of the European Union have been applied to the external action of the Union. It has been investigated how the conclusion of trade and partnership agreements is shaped by big data, the data economy and human rights standards. Generally, most recently discussed trade and partnership agreements somehow include the exchange of data, once more it can be seen that big data is a good belonging to trade and services. Having analyzed the European Union's approach, internal standards do determine the external actions of the Union. It can be stated that the Maximillian Schrems case has not only influenced the internal standards of the Union, but due to the transnational character of big data and the data economy also influenced the external action of the European Union. Through the conclusion of the General Data Protection Regulation trade and partnership agreements are strongly influenced[179]. Moreover, previous decisions between the EU and the US have been withdrawn due to the jurisdiction of the Maximillian Schrems case[180].

Taking into account the findings of the different chapters, it is now possible to provide an answer to the main research question of this study. The study analyzed to what extent the strategy of the European Commission on big data promotes a data-driven economy whilst respecting human rights standards. It can be stated that the strategy of the European Commission on big data strongly emphasizes the chances of a data-driven economy and sees it as a necessary step to compete in the global market[181]. However, next to the data economy, the European Union highlights its human rights standards. As the study identified, compared to other countries, the EU's standards are rather high which makes it difficult to conclude trade and partnership agreements with third countries according to the EU's internal standards. The EU is enlarging the rights on privacy and data protection to ensure its standards not only offline, but also online. Through the quick implementation of big data services, the regulative frameworks of the EU had to be adjusted to the new challenges and now serve a high level of protection for its citizens[182].

The study has shown that there are unresolved questions in regard to big data, the data economy, privacy regulations and external relations. Hence, it can be stated that the current regulative frameworks are insufficient. To flourish the data-economy, the EU has to be an attractive location for data-driven businesses. Therefore, the EU has to prepare all EU Member States and encourage the growth in less developed countries. Moreover, the EU has to find a better balance in enhancing the data economy and the human rights standards. The General Data Protection Regulative is a first step towards coherent regulations on data protection among all EU Member States which facilitates the process. Other than that, general provisions, like the Charter of Fundamental Human Rights, have to be taken into consideration as well as primary and secondary EU law while concluding trade and partnership agreements with third countries to ensure the EU's internal standards externally. From a regulatory perspective, more coherent

[179] Read chapter five for further information.

[180] This is extensively discussed in *section 2.1*.

[181] For further information read *section 3.3*.

[182] For further information read *section 4.3*.

measurements and policies among the EU Member States will encourage the data economy. From a privacy perspective, one has to see, how the General Data Protection Regulation is implemented and if future (technological) developments will cause the need for further adjustments.

Future research should investigate how the General Data Protection Regulation is implemented and how it influences trade and partnership agreements between the EU and third countries. Once the General Data Protection Regulation has been into force for a while, it will be interesting to see if the internal standards are obeyed by countries which have concluded a trade and partnership agreement with the European Union. Moreover, this study only stressed the processing of person-related data due to commercial purposes, thus, further research could take into consideration how the security purpose of data influences the storage, tracing and processing of data. As big data technologies are continuously developing, the future will show if more sector specific and stronger regulations are needed to ensure the right of privacy and data protection in a data-driven economy. Thus, another interesting research would be to analyze the same situation a decade later.

BIBLIOGRAPHY

Literature

Books

Mohanty, H., Bhuyan, P. & Chenthati, D. (2015). *Big Data - A Primer*. Studies in Big Data, Volume 11. Springer India.

Journals

Fosso Wamba, S., Akter, S., Edwards, A., Chopin, G., & Gnanzou D. (2015). *How big data can make big impact: Findings from a systematic review and a longitudinal case study*. International Journal Production Economic, 2015(165), 234-246.

Warren, S. D. & Brandeis L. D. (1890). *The Right to Privacy*. Harvard Law Review. December 5, 1890. Vol. IV. No. 5.

Policy documents

Backer, J. (2016). *EPrivacy leaked draft: The 'good', the 'bad' and the 'missing'*. Retrievd from: https://iapp.org/news/a/eprivacy-leaked-draft-the-good-the-bad-and-the-missing/.

Bennett, C. J. (n.n.). *Is Canada still 'adequate' under the new European General Data Protection Regulation*? Retrieved from: http://www.colinbennett.ca/data-protection/is-canada-still-adequate-under-the-new-general-data-protection-regulation/.

Bendiek, A. & Schmieg, E. (2016). *European Union Data Protection and External Trade - Having the Best of Both Worlds?* German Institute for International and Security Affairs.

Boardmann, R., Mole, A. & Voisin G. (06.10.2015). *CJEU invalidates Safe Harbor*. Retrieved from: https://www.twobirds.com/en/news/articles/2015/global/cjeu-invalidates-safe-harbor.

Brössler, D., Mühlauer, A. (22.06.2017). *EU strebt Handelsabkommen mit Japan an*. Süddeutsche Zeitung.

Bradatan, C. E. (n.n.). *Transnationality as a fluid social identity*. Retrieved from: http://www.academia.edu/230389/Transnationality_as_a_fluid_social_identity.

Buttarelli, G. (2016). *EDPS Opinion on coherent enforcement of fundamental rights in the age of big data*. European Data Protection Supervisor, Opinion 8/2016.

CCSK Guide (2013). *Data Fragmentation*. Retrieved from: https://ccskguide.org/data-fragmentation/.

Coudert, F. (15.10.2015). *Schrems vs. Data Protection Commissionr: A Slap on the Wrist for the Commission and New Powers for Data Protection Authorities*. Retrieved from: https://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/.

Hastings, P. (04.07.2016). *Five Ways that Privacy Shield is Different from Safe Harbor and Five Simple Steps Companies Can Take to Prepare for Certification.* Retrieved from: https://www.paulhastings.com/publications-items/details?id=eaffe969-2334-6428-811c-ff00004cbded.

Information Technology Industry Council (ITI) (2016). *The EU-US Privacy Shield*. Retrieved from: http://www.itic.org/safeharbor.

Information Technology Industry Council (ITI) (2017). *Data Localization*. Retrieved from: https://www.itic.org/policy/forced-localization/data-localization.

Lodderhose, D. (21.11.2016). *Europe's Digital Single Market: What You Need To Know & How It Could Kill The Indie Biz*. Retrieved from: http://deadline.com/2016/11/europe-digital-single-market-what-you-need-to-know-how-it-could-kill-the-indiebusiness-1201857973/.

Matera, C. (2016). *Writing a bachelor thesis in law in the European Public Administration program at the University of Twente*. University of Twente (internally provided course material).

Pollet-Fort, A. (2010). Implications of the Lisbon Treaty for the European Union External Trade Policy (Common Commercial Policy). EU Centre in Singapore, Background Bried No 2.

Stretton T., & Gest, L. (22.04.2016). *How will the new EU-US privacy shield fit with the upcoming General Data Protection Regulation*. SC Magazine UK. Retrieved from: https://www.scmagazineuk.com/how-will-the-new-eu-us-privacy-shield-fit-with-the-upcoming-general-data-protection-regulation/article/531527/.

Svantesson, D. J. B. (2010). *A Legal Method for Solving Issues of Internet Regulation; Applied to the Regulation of Cross-border Privacy Issues*. EUI Working Papers, Law 2010(18).

Wessing, T. (13.07.2016). *EU-US Privacy Shield - What's new in comparison with Safe Harbor*. Retrieved from: http://www.lexology.com/library/detail.aspxg=e02eccc0-9c26-4eb6-9293-00fb41272693.

Wessing, T. (n.n.). *The Digital Single Market*. Retrieved from: https://united-kingdom.taylorwessing.com/en/digital-single-market.

World Economic Forum (2014). *The Europe 2020 Competitiveness Report - Building a More Competitive Europe*. 2014 Edition.

Zanfir-Fortuna, G. (2017). *Will the ePrivacy Regulation overshadow the GDPR in the age of IoT?* Retrieved from: https://iapp.org/news/a/will-the-eprivacy-reg-overshadow-the-gdpr-in-the-age-of-iot/.

Official Papers

European Commission (2010). *Turning Europe into a true Innovative Union*. MEMO 10/47. Retrieved from: http://europa.eu/rapid/press-release_MEMO-10-473_en.htm.

European Commission (02.07.2014). *Towards a thriving data-driven economy*. Retrieved from: https://ec.europa.eu/digital-single-market/en/news/communication-data-driven-economy.

European Commission (2015a). *Digital Single Market: driving economic growth*. Retrieved from: https://ec.europa.eu/digital-single-market/en/economy-society-digital-single market#Article.

European Commission (2015b). *Why we need a Digital Single Market?*. Retrieved from: https://ec.europa.eu/commission/publications/why-we-need-digital-single-market_en.

European Commission (2016a). *A Digital Single Market for Europe*. Retrieved from: https://ec.europa.eu/commission/publications/digital-single-market-two-years_en.

European Commission (2016b). *Protection of personal data*. Retrieved from: http://ec.europa.eu/justice/data-protection/.

European Commission (2016c). *The EU Data Protection Reform and Big Data Factsheet*. Retrieved from: http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf.

European Commission (2017a). *Commission outlines next steps towards a European data economy.* Retrieved from: http://europa.eu/rapid/press-release_IP-17-5_en.htm.

European Commission (2017b). *Hearing: Respect for private life and protection of personal data in electronic communication*. Retrieved from: http://www.europarl.europa.eu/news/en/news-room/20170411IPR71014/respect-for-private-life-personal-data-protection-in-electronic-communication.

European Commission (2017c). *Building a European Data Economy*. Retrieved from: https://ec.europa.eu/digital-single-market/en/building-european-data-economy.

European Commission (2017d). *Right environment for digital networks and services*. Retrieved from: https://ec.europa.eu/digital-single-market/node/78516.

European Commission (2017e). *The Digital Economy and Society Index (DESI)*. Retrieved from: https://ec.europa.eu/digital-single-market/en/desi.

European Commission (2017f). *Exchanging and Protecting Personal Data in a Globalised World*. COM (2017) 7 final.

European Commission (2017g). *Report of the 18th EU-Japa FTA/EPA negotiating round*. Retrieved from: http://trade.ec.europa.eu/doclib/docs/2017/april/tradoc_155506.pdf.

European Commission (2017h). *Report of the 14th Round of Negotiations for the Transatlantic Trade and Investment Partnership*. Retrieved from: http://trade.ec.europa.eu/doclib/docs/2016/august/tradoc_154837.pdf

European Commission (n.n.a). *Data transfers outside the EU*. Retrieved from: http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm.

European Commission (n.n.b). *Digital Single Market - Commission strenghtens trust and gives a boost to the data economy*. Retrieved from: https://ec.europa.eu/digital-single-market/en/news/commission-strengthens-trust-and-gives-boost-data-economy.

European Commission (n.n.c). *The European Single Market*. Retrieved from: https://ec.europa.eu/growth/single-market_en.

European Commission (n.n.d.). *Global Europe competing in the world - A contribution to the EU's Growth and Jobs Strategy*. Retrieved from: http://trade.ec.europa.eu/doclib/docs/2006/october/tradoc_130376.pdf.

European Commission (n.n.e.). *The European citizens' initiative*. Retrieved from: http://ec.europa.eu/citizens-initiative/public/welcome.

European Commission (n.n.f.). *Trade Agreements*. Retrieved from: http://ec.europa.eu/trade/policy/countries-and-regions/agreements/.

European Data Protection Supervisor (14.07.2014). *The transfer of personal data to third countries and international organizations by EU insitutions and bodies*. Position paper. Retrieved from: https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf.

European Data Protection Supervisor (30.05.2016). *Opinion on the EU-US Privacy Shield draft adequacy decision*. Opinion 4/2016. Retrieved from: https://edps.europa.eu/sites/edp/files/publication/16-05-30_privacy_shield_en.pdf.

European Data Protection Supervisor (2016). *Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC)*. Opinion 5/2016. Retrieved from: https://edps.europa.eu/sites/edp/files/publication/16-07-22_opinion_eprivacy_en.pdf.

European Parliament (2015). *TTIP: Trade agreements must not undermine EU data protection laws, say Civil Liberties MEP's*. Retrieved from: http://www.europarl.europa.eu/news/en/press-room/20150330IPR39308/ttip-trade-agreements-must-not-undermine-eu-data-protection-laws-say-meps

European Parliament (2017). *EU-Singapore Free Trade Agreement - Stimulus for negotiations in the region*. Retrieved from: http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/607255/EPRS_BRI(2017)607255_EN.pdf.

European Union (n.n.). *The economy*. Retrieved from: https://europa.eu/european-union/about-eu/figures/economy_en

Gomes, A. (2017). *Report on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law enforcement*. Document LIBE/8/07753.

Office of the High Commissioner (n.n.). *What are human rights?* United Nations Human Rights. Retrieved from: http://www.ohchr.org/EN/Issues/Pages/WhatareHumanRights.aspx.

Legislation

Legislation

Charter of Fundamental Rights of the European Union 2000/C364/01. Official Journal of the European Communities.

China Copyright and Media Online Publishing Management Rules (20.02.2016)

Commission decision 2000/520/EC of July 2000.

Commission Implementing Decision 2016/1250/EU on the adequacy of the protection provided by the EU-US Privacy Shield.

Comprehensive Economic and Trade Agreement between Canada and the European Union.

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Directive 2016/680/EU on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalies, and on the free movement of such data.

European Convention of Human Rights.

EU-Singapore Free Trade Agreement.

Free Trade Agreement betwen the European Union and the Republic of Korea. Guidelines for the Regulation of Computerized Personal Data Files. Resolution 45/95 adopted by the General Assembly. Retrieved from: http://www.refworld.org/pdfid/3ddcafaac.pdf.

Proposal for a Regulation 2017/0003 (COD) 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).

Regulation EU 2011/211 on the citizens' initiative.

Regulation EU 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Safe Harbor Decision 2000/520/EG.

The OECD Privacy Framework (2013).

Transatlantic Trade and Investment Partnership between the European Union and the United States of America (leaked version).

Treaty on European Union, Official Journal C326, 26/10/2012.

Treaty on the Functioning of the European Union, Official Journal C326, 26/10/2012.

Universal Declaration of Human Rights.

Case law

C-362/14, Judgement of the Court of 6 October 2015, Maximillian Schrems vs. Data Protection Commissioner.

Irish Data Protection Commissioner vs. Facebook Ireland Ltd and Maximillian Schrems. Retrieved from: http://europe-v-facebook.org/EN/en.html.