Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

European Union Law Working Papers

No. 62

GDPR and Data Transfer: Focusing on Data Flow Between the EU and USA Before and After the Schrems II Decision

Dani Manfreda

2022

European Union Law Working Papers

Editors: Siegfried Fina and Roland Vogl

About the European Union Law Working Papers

The European Union Law Working Paper Series presents research on the law and policy of the European Union. The objective of the European Union Law Working Paper Series is to share "works in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The working papers can be found at http://ttlf.stanford.edu.

The European Union Law Working Paper Series is a joint initiative of Stanford Law School and the University of Vienna School of Law's LLM Program in European and International Business Law.

If you should have any questions regarding the European Union Law Working Paper Series, please contact Professor Dr. Siegfried Fina, Jean Monnet Professor of European Union Law, or Dr. Roland Vogl, Executive Director of the Stanford Program in Law, Science and Technology, at:

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Dani Manfreda earned his LL.M. degree in European and International Business Law with the highest distinction from the University of Vienna School of Law in 2022. Prior to that, he received his bachelor's and master's degrees with the highest distinction from the University of Ljubljana, Faculty of Law, in Slovenia. In August 2021, Dani successfully completed the professional certificate summer program Understanding U.S. Intellectual Property Law at Stanford Law School. Currently, he works as Deputy Head of Legal & Compliance at an international company in Vienna, Austria.

General Note about the Content

The opinions expressed in this student paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum, or any of TTLF's partner institutions, or the other sponsors of this research project.

Suggested Citation

This European Union Law Working Paper should be cited as:
Dani Manfreda, GDPR and Data Transfer: Focusing on Data Flow Between the EU and USA Before and After the Schrems II Decision, Stanford-Vienna European Union Law Working Paper No. 62, http://ttlf.stanford.edu.

Copyright

Abstract

Data protection and transfer of personal data from the EEA to the USA is a heavily discussed topic, especially in the business world. Probably there is not a single company in the EEA not processing personal data of its employees, customers, or vendors and many of these companies are considering transferring personal data also outside of the EEA, for example to their subsidiaries or vendors, to successfully perform on the market. However, not all the countries outside of the EEA can guarantee a level of protection of personal data equivalent to the level of protection guaranteed and expected in the EEA by the GDPR. Especially in the USA, the historical development of the perception of data protection is completely different in comparison to the development of the same in the European Union. On one hand, privacy of personal data is treated as a human right in the EU, and in the US, they still look at it as a property right, protection of which can be sacrificed for other benefits, such as national security or economic benefits.

Nevertheless, the EU legislation does not forbid every transfer of personal data to a third country. There are different data transfer mechanisms that companies can rely on, from adequacy decisions granted by the EU to the third country in question, to appropriate safeguards and to other data transfer mechanisms as set out in the GDPR. Specifically, between the EU and the USA there were a couple of trans-Atlantic frameworks in place in the last decades. The idea of these frameworks was to reduce bureaucracy and enable companies on both sides of the Atlantic to securely share personal data. However, the above-mentioned frameworks were successfully challenged in front of the CJEU, which invalidated them. This initially led to legal uncertainty as there was no clear instructions provided by the European Courts on how and if the companies may continue to transfer personal data from the EEA to the USA. The uncertainty was mitigated to some extent with the guide published by the European Data Protection Board, however the transfers of personal data form the EEA to a country that cannot guarantee a level of protection of personal data equivalent to the one in the EEA remains complex and very difficult to achieve.

Companies on both sides of Atlantic are craving for a new, updated trans-Atlantic framework which would ease such data transfers, however it is already clear that any such new framework agreement will be thoroughly reviewed and challenged by those who opposed the initial frameworks, unless the USA first changes its legislation in a way that would give protection of personal data in the same way or at least similar recognition and treatment as it has in the EEA.

TABLE OF CONTENTS

TABLE OF ABBREVIATIONS

CFREU	Charter of fundamental rights of the European Union
CJEU	Court of Justice of the European Union
DPA	Data Protection Authority
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
ECSP	Electronic Communication Service Providers
EDPB	European Data Protection Board
EEA	European Economic Area
EU	European Union
DPD	Directive 95/46/EC
FTC	Federal Trade Commission
NAACP	National Association for the Advancement of Colored People
NOYB	none of your business
NSA	National Security Agency
TFEU	The Treaty on the Functioning of the European Union
PS	Privacy Shield
SH	Safe Harbor
U.S.	Unted States of America

1. INTRODUCTION

I decided to write about data protection and transfer of personal data between Europe and the United States, because this is a topic that I need to take into account working as an in-house legal counsel on daily basis. The definition of personal data is so wide, that basically every European company falls under the scope of GDPR. Moreover, according to the statement of the White House, data transfers between the EU and the USA are the most used in the world, bringing the economic value of such collaboration to $7.1 trillion[1], this is why it is logically in the interest of most companies doing business on both sides of the Atlantic to be able to keep transferring personal data and they should be able to do this in a safe and GDPR-compliant manner. There were attempts to justify data transfers on the bases of a trans-Atlantic legal framework, such as Safe Harbor and Privacy Shield, however, the data protection landscape has gone through some turbulent times in the recent years, which challenged the existing legal frameworks which allowed for personal data to be transferred out of the EU to the USA. All this has led to a high level of uncertainty, where companies were not sure if they are allowed to transfer personal data to the USA and if yes, under which conditions. Thus, the purpose of this master thesis is to analyze the development of regulation of international transfers of personal data between the European Union and the United States, focusing on the situation before the landmark decision *Schrems II*, as well as on the implications of this judgment and the life in the business world after it, when it comes to transfers of personal data.

As the master thesis will show, there are still major differences when it comes to perception and regulation of data privacy and protection of personal data on both sides of the Atlantic. In order to understand why this is so, I focus in the early chapters of this master thesis on providing

[1] The White House, 'FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework' (*The White House*, 25 March 2022) <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/> accessed 8 May 2022.

an overview of the development of the right of protection of personal data throughout history in the EU and in the USA, as well as shed light on why the right to protect personal data is considered to be a fundamental human right in the EU, but in the USA they look at it as a property right which does not deserve to have the same level of protection as it has in the EU. Next, I will describe what the relevant provisions of GDPR dealing with transfer of personal data outside of the EEA are and what are the different options companies can use when it comes to data transfer mechanisms. I then write about the trans-Atlantic legal frameworks which companies relied on in the past, such as Safe Harbor and Privacy Shield, as well as about the CJEU's decision in *Schrems I* case, which followed after Edward Snowden discoveries, and which invalidates Safe Harbor. However, the real landmark case is CJEU's decision in *Schrems II* case, which invalidated the then used Privacy Shield framework and brought uncertainty to the future of data transfers to the USA in general. As this is a landmark decision, I dedicate a separate chapter to it. The final chapters of my master thesis focus on the options and requirements that companies need to consider if they wish to continue transferring personal data to the USA in a safe and GDPR compliant manner. I conclude with what the future of data transfer could look like, based on the recent statements from the EU Commission and the White House where they announced a potential new political solution which should take care of this uncertainty. Despite a new political solution is on the horizon, there are already predictions that any such new solution will be thoroughly analyzed and again challenged in front of the CJEU if the aspects highlighted in *Schrems II* will not be addressed.

2. DATA PROTECTION IN THE EUROPEAN UNION

2.1. EUROPEAN CONVENTION FOR THE PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS

In the EU, the right to the protection of personal data has evolved from the right to the protection of an individual's private life. The latter was first recognized in international law in Article 12 of the 1948 Universal Declaration of Human Rights[2], which was drafted under the auspices of the United Nations.

The European Convention for the Protection of Human Rights and Fundamental Freedoms[3] ("ECHR") was approved two years later by the Council of Europe. The ECHR does not specifically mention the protection of personal data, but the right to personal data protection derives from Article 8 of the ECHR, which deals with the protection of private 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 wellbeing 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."[4]

The protection of private life has eventually evolved to also include protection of privacy and the protection of privacy has become an intrinsic component of Article 8 also through the

[2] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR).
[3] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).
[4] Article 8 ECHR.

European Court of Human Rights' ("ECtHR") case law (case *Niemietz*[5], case *Bensaid*[6], case *Leander*[7]), which clearly presented ECtHR's view that Article 8 indeed does also includes protection of personal data.[8]

2.2. CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

The European Union's Charter of Fundamental Rights ("CFREU") has the status of primary legislation inside the EU, and as such, it may be used to assess the legality of secondary EU legislation and national laws. The necessity to establish an independent right in the protection of personal data was widely held inside the EU towards the end of the 1990s, when the CFREU was being drafted.[9] CFREU was agreed in 2001 as part of the Treaty of Nice[10], but it was not legally effective until the Lisbon Treaty[11] took effect on December 1, 2009. When Lisbon Treaty was adopted, protection of personal data has been defined as a fundamental right under Article 8 of CFREU. Provisions on the protection of personal data are contained in the second chapter of the Charter, entitled "Freedoms".

Article 8 of CFREU:

"*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

[5] Niemietz v Germany App no 13710/88 (ECtHR, 16 December 1992).
[6] Bensaid v the United Kingdom App no 44599/98 (ECtHR, 6 February 2001).
[7] Leander v Sweden App no 9248/81 (ECtHR, 26 March 1987).
[8] EU Network of Independent Experts on Fundamental Rights, 'Commentary of the Charter of Fundamental Rights of the European Union' (EU Network of Independent Experts on Fundamental Rights, June 2006) <https://sites.uclouvain.be/cridho/documents/Download.Rep/NetworkCommentaryFinal.pdf> accessed 28 April 2022, p. 90.
[9] Ibid 90-92.
[10] Treaty of Nice amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts [2001] OJ 1 80/01.
[11] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007 [2007] OJ 1 306/01.

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."

Protection of personal data is not an absolute right, it must always be weighed against its function in society according to the principle of proportionality. In accordance with Article 52 of CFREU[12]: "*Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."*

2.3. THE TREATY ON THE FUNCTION OF THE EUROPEAN UNION

The right to protection of personal data is mentioned also in The Treaty on the Functioning of the European Union ("TFEU"). TFEU is also primary EU law, and it guarantees that everyone *"has the right to the protection of personal data concerning them."*[13]

Furthermore Article 16 TFEU mentions also that: *"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. Compliance with these rules shall be subject to the control of independent authorities."*[14]

[12] Charter of Fundamental Rights of the European Union (CFREU) [2012] OJ C 326/391, Art.52
[13] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union [2016] OJ C202/1 (TFEU), Articlr 16 para 1.
[14] Article 16 para 2 TFEU.

2.4. DIRECTIVE 95/46/EC

The Directive 95/46/EC[15] ("DPD") was adopted in 1995 by the European Parliament and the Council, with a view to regulating the protection of personal data in the processing of personal data and the free movement of such data. There were several reasons for the adoption but one of the key ones is certainly the increasing processing of personal data in various economic and social activities and advances in information technology.[16] The objective of the Directive 95/46/EC was to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data and preventing prohibition of free flow of personal data between Member States.[17]

Among the most important things regulated by the Directive 95/46/EC were principles under which the data must be processed, it establishes criteria for legitimate data processing, cross-border data flow and legal basis for transfers of personal data out of the EU. The introductory provisions of the GDPR state that the objectives in the principles of Directive 95/46/EC still apply, so I will not go into details here, especially since the GDPR largely summarizes and builds on the regulation of Directive 95/46/EC. As of 25 May 2018, Directive 95/46/EC is no longer valid, as it was repealed and replaced by the General Data Protection Regulation in accordance with Article 94[18].

2.5. GENERAL DATA PROTECTION REGULATION (EU) 2016/679

[15] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ 2 281/31.
[16] Preamble para 4 Directive 95/46/EC.
[17] Article 1 Directive 95/46/EC.
[18] Article 94 GDPR.

One of the reasons for the adoption of the General Data Protection Regulation[19] ("GDPR"), is the rapid technological development, which has brought new challenges for the protection of personal data.[20] This development required a solid and more coherent framework for the protection of personal data, supported by consistent enforcement.[21]

Businesses and other organizations handle data as part of their workflow or maintain data on their employees, customers, and affiliates, among other things. GDPR has a broad reach, and it is reasonable to anticipate that it will apply to all parts of enterprises and other organizations that handle personal information.[22] The GDPR stipulates that to ensure a consistent and high level of protection of individuals' rights and to remove obstacles to the transfer of personal data, the level of protection of rights and freedoms in the processing of personal data should be the same in all Member States. In connection with general and horizontal law on the protection of personal data, Member States have adopted several sectoral laws where more detailed provisions are needed. [23] This is probably the reason why this time they decided to regulate the area with a regulation, as the latter is an EU legal act that is directly applicable in all Member States of the European Union.

As can be seen from Article 1[24] of the Regulation, the GDPR lays down rules on the protection of individuals about the processing of personal data and rules on the free movement of personal data. Article 2[25] stipulates that the GDPR is used for the processing of personal data in whole

[19] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 2 119/1.
[20] Preamble para 6 GDPR.
[21] Preamble para 7 GDPR.
[22] Sanjay Sharma, Data Privacy and GDPR Handbook (Newark: John Wiley & Sons, Incorporated 2019) 45
[23] Preamble para 10 GDPR.
[24] Article 1 GDPR.
[25] Article 2 GDPR.

or in part by automated means and for other processing for personal data that are part of the collection or are intended to form part of the collection. The GDPR applies only to activities within the EU and does not apply to natural persons during personal or domestic activities.

Article 3[26] defines extended territorial validity, stating that the GDPR applies to the processing of personal data in the context of the activities of the controller's or processor's registered office in the European Union. It also applies to the processing of personal data by a controller or processor not established in the European Union where the processing activities involve the provision of goods or services to such individuals in the European Union or the monitoring of their behavior insofar as this is the case in the European Union.

What follows is a definition of terms where it is necessary to mention the expanded definition of personal data and processing, the new definition of consent and quite a few new terms that have been included in the GDPR. In the definition of personal data, they have added, for example, the online identifiers, including web identifiers such as cookie IDs, IP addresses, RFID tags, etc.[27]

A new concept that is emerging is also “profiling”, which means any form of automated processing of personal data that involves the use of personal data to assess certain personal aspects of an individual. The definition of individual consent was changed by adding that it must be an explicit and unambiguous statement of will, which excludes the most frequently used, opt-out or automatic consent. New concepts are also genetic and biometric data, which became personal data protected by the GDPR on 25 May 2018.[28]

[26] Article 3 GDPR.
[27] Article 4 GDPR.
[28] Article 4 GDPR.

The principles pursued by the GDPR are very similar to those already laid down in Directive 95/46/EC, with one exception. These principles are listed in Article 5 and determine legality, fairness and transparency, restrictions on the purpose of the data together with the minimum amount of data, the principle of accuracy, storage limitations and the principle of responsibility of the controller. A new principle not contained in Directive 95/46/EC is the principle of integrity and confidentiality, which imposes on controllers the duty to ensure the security of personal data, including protection against unauthorized and illegal processing and against loss or destruction of data.[29]

The legal bases for the processing of personal data set out in Article 6[30] of the GDPR remain the same as those already laid down in Directive 95/46/EC. The novelty set out in the GDPR is the possibility of processing data for a purpose other than that for which they were selected, under certain conditions and insofar as the processing is not based on the consent of the individual.

Article 7[31] of the GDPR sets out the conditions required for the consent of an individual to the processing of personal data not covered by Directive 95/46/EC:

1. Consent must be given in such a way that the controller is able to demonstrate that the individual has consented to the processing.

2. If consent is given in a written statement relating to other matters, the consent form shall be separate from the rest of the text, in an intelligible and accessible form and in a clear and simple manner language.

[29] Article 5 GDPR.
[30] Article 5 GDPR.
[31] Article 7 GDPR.

3. The individual must always be able to withdraw his statement in the same or similarly simple way as he gave it.
4. In the case of performance of a contract, including the provision of services, the conclusion of a contract may not be conditional on consent to the processing of personal data which are not necessary for the performance of the contract in question.

The third chapter[32] of the GDPR regulates the rights of the data subject. In addition to those rights already provided for in Directive 95/46/EC, such as the right of access, objection, and rectification, they also added the right of the individual to information on how long his personal data is kept. In Article 17[33] of the GDPR, they added the right to erasure or right to be forgotten, based on which an individual can achieve the erasure of his personal data, under certain conditions, and the right to data portability, which is regulated by Article 20[34] of the GDPR, which allows individuals' data to be transferred directly from one operator to another.

The most relevant GDPR chapter for this master thesis is chapter five[35], which deals with transfers of personal data to third countries or international organizations. I will write about this chapter in connection to transfers of personal data to the US into details below.

[32] Chapter 3 GDPR.
[33] Article 17 GDPR.
[34] Article 20 GDPR.
[35] Chapter 5 GDPR.

3. DATA PROTECTION IN THE UNITED STATES OF AMERICA

The United States of America and the European Union perceive data privacy and data protection topics from completely different angles. USA is unique among the world's leading countries in that it lacks an umbrella privacy legislation and a governmental authority, who would be responsible for protecting privacy of personal information.[36] Instead, data privacy is governed by several various federal and state laws, which derive from case law and legislation.[37] These address specific topics or sectors, instead of having one single piece of national legislation that would cover both public and private sectors.[38]

For example, the US Constitution (Bill of Rights) addresses the protection of privacy of individuals in a variety of ways, even though the term "privacy" cannot be found in the Constitution.[39] Some of the Amendments (as described below) include components related to it, however, the problem is that constitutional privacy rights are always directed against the federal or state government. As a result, these rights do not obligate the government to safeguard them against third parties, but they only forbid the government from violating them. I will shortly describe where in the Constitution we can find the right to privacy.

3.1. THE US CONSTITUTION AND THE BILL OF RIGHTS

3.1.1. FIRST AMENDMENT

[36] Law Reform Commission of New Zealand, Invasion of Privacy: Penalties and Remedies – Review of the Law of Privacy (NZLRC 2009) 80.
[37] Dan Jerker B Svantesson, 'The regulation of cross-border data flows' [2011] 1(3) International data privacy law 185.
[38] Law Reform Commission of New Zealand, Invasion of Privacy: Penalties and Remedies – Review of the Law of Privacy (NZLRC 2009) 81.
[39] Daniel J Solove, The Digital Person : Technology and Privacy in the Information Age (New York, NY : : New York University Press 2004) 62.

The *First Amendment*[40] does not only safeguard free speech, but it also protects the right of people to associate with each other. This right prevents government from being allowed to ask different organizations to reveal who their members are and where they live or to force citizens to reveal the names of organizations which they are a member of. The Supreme Court decided that privacy is needed for the individuals to be able to exercise the freedom of association. Only if individuals have the right to privacy. This will allow them to be members of organizations of their choice and they do not need to be afraid to lose jobs, or suffer other form of retaliation if someone else finds out about their membership.[41]

To be more specific, the Supreme Court held in *NAACP v Alabama*[42], that it is not allowed to reveal membership information, for example first name, last name, home address, because this could have consequently a highly negative impact on the lives of the individuals concerned. The State of Alabama wanted to stop the National Association for the Advancement of Colored People (NAACP) from doing business in the State. The State issued a demand for different information, including the NAACP membership lists, after the circuit Court imposed a restraining order.[43] The Court safeguarded supporters of the Civil Rights Movement who may have faced persecution if their names were public, and thereby helped the movement in drawing new members, by preserving the anonymity of the then-current members.[44]

[40] U.S. Constitution amend. I.
[41] Daniel J Solove, The Digital Person : Technology and Privacy in the Information Age (New York, NY : : New York University Press 2004) 62-63.
[42] NAACP v Alabama, 357 US 449, 462 [1958].
[43] Oyez, 'National Association for the Advancement of Colored People v Patterson' (Oyez) <https://www.oyez.org/cases/1957/91> accessed 30 April 2022.
[44] Law Library - American Law and Legal Information, 'National Association for the Advancement of Colored People v Patterson' (Law Library - American Law and Legal Information) <https://law.jrank.org/pages/22818/National-Association-Advancement-Colored-People-v-Alabama-Significance.html> accessed 30 April 2022.

To sum up, there is some protection of privacy of individuals through the *First Amendment*, however, the problem with the First Amendment is that it is only applicable if the government is involved in the compulsion of information. If the same is collected by private entities, then the protection by the First Amendment is not applicable to them.[45]

3.1.2. FOURTH AMENDMENT

According to the *Fourth Amendment*[46] of the US Constitution, the State is prohibited to perform "unreasonable searches and seizures". Before performing a search, government officers are usually required to acquire judicial authorization.[47] For example, government officers must carry out a standard search warrant and if they do not discover what they were searching for, for example at a house specified in the warrant, they must leave that place immediately and seek a second order if they desire to return to search.[48] So the search can only be performed if it there is no reasonable expectation of privacy.

The *Fourth Amendment* is applied under the "reasonable expectation of privacy" approach. This approach establishes where and when a person has a right to privacy. A person's reasonable expectation of privacy, sometimes known as the "right to be left alone," means that someone who unjustly and significantly jeopardizes another's interest in keeping her affairs private can be held accountable for that exposure or intrusion.[49]

---

[45] Daniel J Solove, The Digital Person : Technology and Privacy in the Information Age (New York, NY : : New York University Press 2004) 63.
[46] U.S. Constitution amend. IV.
[47] Daniel J Solove, The Digital Person : Technology and Privacy in the Information Age (New York, NY : : New York University Press 2004) 63.
[48] James X Dempsey, 'Communications privacy in the digital age: revitalizing the federal wiretap laws to enhance privacy' [1997] 8(1) Albany Law Journal of Science & Technology 70.
[49] Findlaw's team of legal writers and editors, 'What Is the "Reasonable Expectation of Privacy"?' (FindLaw, 2017) <https://www.findlaw.com/injury/torts-and-personal-injuries/what-is-the--reasonable-expectation-of-privacy--.html> accessed 4 May 2022.

However, there are a couple of issues with this approach to the *Fourth Amendment*. First, the Supreme Court determined that reasonable expectations of privacy do not apply to public acts or objects managed by a third party. Therefore, the *Fourth Amendment* provides no protection for the person if the State can "see" the act, whether through the naked eye of its officials or with the use of technology or can locate proof of it elsewhere.[50] Second, the *Fourth Amendment* applies only in situations where individuals would fairly expect it to be applied. As a result, Fourth Amendment privacy information protection does not exist when a demand for privacy is out of step with the prevailing society view of adequate privacy.[51] In *United States v White*, the Supreme Court mentions that "we all know, after all, that anyone we talk with might wear such a device; thus, there can be no reasonable expectation of privacy in such conversations".[52] For example, it can be very easily argued by the government that sharing some personal information while accessing websites does not satisfy the condition of "reasonable expectation of privacy", as one should expect that such behavior means that there is no such reasonable expectation of privacy.

3.1.3. NINTH AMENDMENT

Protection of individual privacy can be found also in the *Ninth Amendment*[53] of the US Constitution. In *Griswold v Connecticut,*[54] the Supreme Court stated that a legislation adopted in Connecticut that did not allow the use of contraceptives (even if a couple was married) was unconstitutional. The argumentation of the Court was that the legislation was interfering with *"a zone of privacy created by several fundamental constitutional guarantees"*.[55] The right to privacy

[50] Paul M Schwartz, 'Privacy and participation: personal information and public sector regulation in the United States' [1995] 80(3) Iowa law review 572.
[51] Ibid 573.
[52] United States v White, 401 US 745, 752 [1971].
[53] U.S. Constitution amend. IX.
[54] Griswold v Connecticut, 381 US 479 [1965].
[55] Priscilla M Regan, Legislating Privacy : Technology, Social Values, and Public Policy (Chapel Hill : : The University of North Carolina Press 1995) 39.

prohibits States from making the use of contraception by married couples unlawful.[56] The Supreme Court ruled in *Roe v. Wade* that a woman's right to privacy *"is broad enough to encompass her decision whether or not to terminate her pregnancy."*[57]

To sum up, looking at the right to privacy in the US Constitution, it can be concluded that the protection of privacy is only taken into account for the scenarios when a protection goes against violations by the government, but there is no impact on how private players acquire and utilize information.[58] For protection against private institutions, the only option is to look outside of the constitutional sphere and to rely on state and federal laws.

3.2. DATA PRIVACY IN THE US LEGISLATION

There were quite of few different industry-specific legislations passed by the US Congress that were dealing in some way with data privacy from different angles. Over 20 privacy laws have been approved by the Congress in the last 40 years, like for example The Fair Credit Reporting Act (FCRA),[59] the Privacy Act[60], The Family Educational Rights and Privacy Act (FERPA)[61], the Cable Communications Policy Act (CCPA)[62], the Electronic Communications Privacy Act (ECPA)[63], the Telephone Consumer Protection Act (TCPA)[64], the Driver's Privacy Protection Act (DPPA)[65], Health Insurance Portability and Accountability Act (HIPAA)[66], the Children's Online Privacy Protection Act (COPPA)[67], The Gramm-Leach-Bliley (GLB) Act[68], etc.

[56] Oyez, Griswold v. Connecticut' (Oyez) < https://www.oyez.org/cases/1964/496> accessed 30 April 2022.
[57] Daniel J Solove, The Digital Person : Technology and Privacy in the Information Age (New York, NY : : New York University Press 2004) 65.
[58] Ibid 64.
[59] 15 U.S.C. § 1681.
[60] 5 U.S.C. § 552a.
[61] 20 U.S.C. § 1232g.
[62] 47 U.S.C. § 551.
[63] 18 U.S.C. § 2510.
[64] 47 U.S.C. § 227.
[65] 18 U.S.C. § 2721.
[66] Pub. L. No. 104-191, 110 Stat. 1936 (1996).
[67] 15 U.S.C. § 6501.
[68] 15 U.S.C. § 6801.

However, unlike the EU, which passed a general regulation ensuring complete privacy protection (GDPR), the US has not established such legislation. Instead, Congress has enacted a series of laws that are specifically targeted only at certain privacy issues.[69] Federal laws provide people just a limited level of control over only a portion of their information, and they frequently impose no system of default control on other data holders. It is true that the federal laws aid in the control of information dissemination, however they usually contain vast exceptions and loopholes that restrict their efficacy. Also, many of the privacy laws enacted by Congress are difficult to enforce, because an individual does not even get the information that personal information has been leaked; and even if such individuals becomes aware of the leak, it would be very difficult for him or her to find out who is the culprit.[70] There is currently still independent data protection authority in the United States, that would oversee the enforcement of data subjects rights when it comes to protection of personal data.

USA sees privacy protection as a property right rather than a human right, and this view comes from the US being driven by economic interests, as compared to EU's rights-based approach.[71] This US government's belief is that the if the information flow is to be good for the economy, than this should not be obstructed by any data privacy legislation.[72]

3.3. DIFFERENT VIEWS ON DATA PRIVACY IN EU AND USA

The American legal system differs from the legal system based on the European continental tradition. There is no comprehensive review in the American common law system that covers

[69] Daniel J Solove, The Digital Person : Technology and Privacy in the Information Age (New York, NY : : New York University Press 2004) 67.
[70] Ibid 71.
[71] Chuan Sun, 'The European Union Privacy Directive and Its Impact on the US Privacy Protection Policy: A Year 2003 Perspective' [2003] 2(1) Northwestern Journal of Technology and Intellectual Property 106.
[72] William J Long and Marc Pang Quek, 'Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise' [2002] 9(3) Journal of European public policy 332.

all laws and regulations. The courts or judges, who decide on precedents in individual cases, have an extremely important role in formulating legal guidelines. This differs from civil law in the countries of continental Europe, where laws and regulations are precisely codified or enacted and where the role of judges is to enforce the relevant measures set out in the Code, depending on the facts of the case.

Therefore, the approach to privacy in the US is different than in Europe. There is no general privacy law in the United States that covers many different areas, as the European Union's GDPR does. The US acquis treats privacy through a filter of freedom and free market principles[73], and at the same time sectoral, which means that privacy issues depend on individual areas with their own laws and regulations, such as health, education, and finance. Above all laws and regulations is the US Constitution, which as the supreme law with its amendments also addresses some aspects of privacy, although it is not explicitly mentioned in it.[74] The drafters of the US Constitution probably did not even imagine that in the future this will have an impact, so they did not consider it necessary to define privacy as an explicit right.[75] In the private sector, there is no comprehensive federal data privacy legislation, and the sectoral rules that do exist are restricted in scope and depending on the type of data covered or the people who are protected.[76] So the USA does have some regulation of data protection, however of the US issue-by-issue approach, there are various gaps and places where data protection is not provided in the US.[77]

[73] Ibid 17.
[74] Lauren B Movius and Nathalie Krup, 'US and EU Privacy Policy: Comparison of Regulatory Approaches' [2009] 3 International journal of communication 174.
[75] Bruce Schneier, 'The Eternal Value of Privacy' (Wired, 18 May 2006) <https://www.wired.com/2006/05/the-eternal-value-of-privacy/> accessed 30 April 2022.
[76] Gregory W. Voss and Kimberly A. Houser, 'Personal Data and the GDPR: Providing a Competitive Advantage for US Companies' [2019] 56(2) American business law journal 312.
[77] Paul B. Lambert, Essential Introduction to Understanding European Data Protection Rules Lambert, Paul B (1st edn, CRC Press 2018) 12.

The American concept of the right to privacy is commonly defined as the control of information concerning a subject.[78] If the American system of legislation can be described as a bottom-up approach, we can say that the European system works from the top to the bottom.[79] Proponents of a strong privacy law are considered a European model. Many countries have the right to privacy enshrined in their constitution. The reasons why the European system is so different from the American one can be found in a different tradition, entrepreneurial culture and history. Unlike the United States, Europe has a lot of experience with totalitarian regimes, which have also benefited from the acquisition of personal data to control and repress its own and foreign populations. These methods were used not only by the secret police and intelligence services, but also by the Nazis during the Second World War, who also used the data to help separate Jews from non-Jews and run concentration camps. The need for strong protection of the privacy of the individual and the recognition of privacy as an inalienable right to be protected is therefore deeply rooted in European consciousness.

[78] Terence Craig and Mary E Ludloff, Privacy and Big Data: The Players, Regulators, and Stakeholders (O'Reilly Media, Inc 2011) 16.
[79] Ibid 29 and 32.

4. TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES UNDER THE GDPR

4.1. GENERAL PRINCIPLES FOR TRANSFER OF PERSONAL DATA

The GDPR's rules strike a compromise between the requirement for data transfers as a foundation for international commerce and trade and the need for affected persons' privacy to be protected as one of their basic human rights. The Regulation ensures the free movement of personal data between EU Member States as an aspect of the European Single Market, with all Member States abiding by the GDPR's data protection standard. Transfers to third countries is regulated in Articles 44–50 GDPR.[80]

Article 44 of the GDPR defines that: *"Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."* [81]

As set out above, it is not allowed for companies (no matter if a company is a data controller or a data processor) to transfer personal data if the criteria set in GDPR is not fulfilled. Goal of this GDPR chapter is to guarantee that the GDPR's degree of protection is not jeopardized when personal data is transferred to a third country. As per GDPR there are 3 possible basis for

[80] Julian Wagner, 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' [2018] 8(4) International data privacy law 320.
[81] Article 44 GDPR.

exporting personal data outside of the EU: adequacy decisions, appropriate safeguards, and derogations for specific situations. The latter come into play only if the criteria set in Article 45, Article 46 and Article 47 are not satisfied.[82]

4.2. TRANSFERS OF PERSONAL DATA ON THE BASIS OF AN ADEQUACY DECISION

Personal data may only be transferred if the third country guarantees an adequate level of data protection, as per Article 45 (1) of the GDPR. The European Commission (EC) has the authority to decide which nations outside the EU meet the adequacy criteria.[83]

Since the introduction of the Data Protection Directive in 1995, adequacy has been the cornerstone of EU data protection reasons for transfer to third countries. Although an adequate determination is preferable and often the most comforting foundation for transfer, it has three major flaws. To begin with, not every country has been accepted as a country that offers an adequate protection. Second, even when functioning in a nation with an approved mechanism, the approved mechanisms only protect the entities that are subject to those rules. Third, because the GDPR requires periodic reviews of such determinations, those who rely on adequacy may no longer assume that once authorized, their adequacy decision will last permanently. When an adequacy decision is available, it is the preferable method of meeting transfer responsibilities. Because the decisions often involve legal frameworks with broad application, operationalizing adequacy as rationale in many situations requires no extra effort. Because adequacy has lately become a status that may be given as well as cancelled, and with little or no warning, a contingency plan may be prudent.[84]

[82] Article 49 GDPR.
[83] Article 45 (1) GDPR.
[84] Mark Phillips, 'International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)' [2018] 137(8) Human genetics 579.

GDPR does not provide a definition of the term adequacy. Recital 103 of the GDPR, on the other hand, states that an acceptable degree of protection basically similar to that provided within the European Union is required. As such, the word refers to a third country's suitability for receiving personal data from controllers or processors in the European Economic Area. This interpretation is compatible with Article 45 GDPR goal of bringing consistency and legal clarity to the EEA.[85] Article 45 GDPR has the effect of allowing personal data to be transmitted to foreign nations without the need for extra protections.[86] According to Article 45(2) GDPR, when assessing the adequacy of the level of protection, the European Commission shall take into accounts, in particular elements such as: respect for human rights, data protection legislation, the presence of an independent supervisory authority, and international agreements to protect personal data.[87] Because the European Commission must conduct an overall evaluation of the circumstances, not all of the requirements must be met equally.

European Commission may find that a third country provides an adequate level of protection due to its national law or international obligations. The finding is published in the Official Journal of the EU and thus becomes legally binding on all EU and EEA Member States and their authorities. As a result, personal data may be transferred to the relevant third country without the involvement of national data protection authorities or other additional safeguards.[88]

[85] Recital 103 GDPR.
[86] Recital 103 GDPR.
[87] Article 45 (2) letter a-c GDPR.
[88] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law: 2018 edition (Luxembourg: Publications Office 2018) 253-255.

The European Commission has released a list of third-country nations, regions, and certain sectors within a third country that have been recognized by the European Commission as having appropriate data protection.[89]

4.3. TRANSFERS OF PERSONAL DATA TO THIRD COUNTRY ON THE BASIS OF APPROPRIATE SAFEGUARDS

Although the GDPR forbids the transfer of personal data to a third country that does not provide a sufficient level of protection, this does not completely preclude data transfers to third countries. Alternative transfer mechanism under GDPR exist to ensure that personal data is protected to the necessary degree when transferred.

If the adequacy decision does not exist, then controllers or processors may transmit personal data to third countries if appropriate safeguards are implemented, according to Article 46 (1) of the GDPR.[90] When personal data is transferred, the data subject must have enforceable rights and effective remedies and the appropriate safeguards are intended to ensure this.[91] The term appropriate safeguards is not defined in the regulation, but recital 108 GDPR[92] states that the safeguards must ensure compliance with data protection requirements and principles and ensure compliance with data subject's rights per the regulation. As per Article 46 (2) GDPR[93], the appropriate safeguards may be ensured by: a legally binding and enforceable instrument between public authorities or bodies; binding corporate rules; standard data protection clauses; approved code of conduct pursuant to Article 40 GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate

[89] European Commission, 'Adequacy decisions' (European Commission) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 15 May 2022.
[90] Article 46 (1) GDPR.
[91] Article 46 (1) GDPR.
[92] Recital 108 GDPR.
[93] Article 46 (2) GDPR.

safeguards; an approved certification mechanism pursuant to Article 42 GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards.

4.3.1. STANDARD CONTRACTUAL CLAUSES ("SCCs")

Standard Contractual Clauses are a contractual solution. These are standard contracts prepared by the European Commission. They are concluded by a data exporter from the European Union and a data importer from a third country, thus ensuring an adequate level of protection of personal data in the third country.[94] Contractual provisions must adequately compensate for the lack of a general level of acceptable protection by incorporating crucial aspects of protection that are missing in a particular case.[95]

Contracting parties normally agree on shared obligations and responsibilities in the areas of personal data protection. In 2021, the European Commission issued 4 new sets of Standard Contractual Clause: Module 1 (transfer from data controller to data controller), Module 2 (transfer from data controller to data processor), Module 3 (transfer from data processor to data processor) and Module 4 (transfer from data processor to data controller abroad).[96]

[94] Informacijski Pooblaščenec, 'Smernice glede prenosa osebnih podatkov v tretje države in mednarodne organizacije' (Informacijski Pooblaščenec Republike Slovenije, 2021) <https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_glede_prenosa_OP_v_tretje_drzave_in_mednarodne_organizacije_po_Splosni_uredbi.pdf> accessed 13 May 2022, p. 14-15.
[95] European Commission, 'Working Party on the Protection of Individuals with regard to the Processing of Personal Data' (European Commission, 24 July) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf> accessed 9 May 2022, p. 16.
[96] European Commission, 'Standard Contractual Clauses (SCCs)' (European Commission, 2021) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en> accessed 15 May 2022.

Following the *Schrems II* decision the European Data Protection Board published recommendations, where they further requirements when the SCCs are valid and can be used. The recommendations have their own section in this master thesis.

4.3.2. BINDING CORPORATE RULES ("BCRs")

Binding corporate rules mechanism is defined in Article 4 (20) GDPR as: *"binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity"*.[97]

Binding corporate rules allow for transfer within a group of companies. These are therefore internal acts adopted in the framework of several interconnected companies that transfer personal data from EU companies to their branches located in non-EU countries. These internal acts aim at the free movement of personal data by specifying the company's policy regarding transfers to third countries. Their validity requires approval from the national supervisory authority.[98]

Also binding corporate rules are enforceable in the EU, which means that eligible third parties individuals can lodge a complaint with the national supervisory authority or bring an action before the courts of the Member States.[99] However, one main disadvantage is the lengthy

[97] Article 4 (20) GDPR.
[98] Informacijski Pooblaščenec, 'Smernice glede prenosa osebnih podatkov v tretje države in mednarodne organizacije' (Informacijski Pooblaščenec Republike Slovenije, 2021) <https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_glede_prenosa_OP_v_tretje_drzave_in_mednarodne_organizacije_po_Splosni_uredbi.pdf> accessed 13 May 2022, p. 15-16.
[99] European Commission, Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)' (European Commission, 6 November)

approval procedures by national supervisory authorities, which are usually quite expensive, so such solutions are mostly used only by multinational corporations that can afford them.[100]

Articles 47 (1) and (2) GDPR establish minimum content criteria for BCRs. After the assessment by the European Data Protection Board, the appropriate national supervisory authority must approve the instrument as the appropriate transfer tool.[101]

4.3.3. CODE OF CONDUCTS

The GDPR states that an organization's adherence to a code of conduct aimed at a specific sector that has been approved by the European Commission using the GDPR's processes, when combined with binding and enforceable commitments to apply appropriate safeguards, constitutes an independent justification for allowing personal data to be transferred to that organization.[102] Drawback of the method is that while following an authorized Code of Conduct gives evidence of GDPR compliance in general, it does not provide proof of compliance. In other words, even if flawless adherence to an established Code of Conduct is maintained, it is theoretically conceivable to be found in violation of the GDPR. The purpose of such a Code of Conduct is not to replace the GDPR's requirements, but to explain and aid in their interpretation in certain situations. The GDPR requires engagement with key parties while a document is developed, the development and certification of an enforcement organization with adequate independence, and, finally, European Commission approval.[103]

<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0566&rid=3> accessed 11 May 2022, p. 8.

[100] Xavier Tracol, '"Invalidator" strikes back: The harbour has never been safe' [2016] 32(2) The computer law and security report 359.

[101] Article 47 (1) letter a GDPR.

[102] Mark Phillips, 'International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)' [2018] 137(8) Human genetics 580.

[103] Ibid 580.

4.4. TRANSFER OF PERSONAL DATA IN SPECIAL CASES

Further options for transfers of personal to third countries are available under Article 49 of the GDPR, which establishes exceptions to the general prohibition on transferring personal data to a third country that does not provide an acceptable degree of protection. The transfer is possible if:[104]

a) *the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;*
b) *the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;*
c) *the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;*
d) *the transfer is necessary for important reasons of public interest;*
e) *the transfer is necessary for the establishment, exercise or defence of legal claims;*
f) *the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;*
g) *the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.*

[104] Article 49 GDPR.

The conditions are set alternatively. It is clear that these are exceptions based on the interests of the individual and the legitimate interests of others, such as the public interest. However, the interests of the individual cannot provide an appropriate basis for mass, repetitive data transfers.[105] Due to the unusual character of certain instances, the Working Party recommends using a narrower interpretation here.[106] They also advise that multiple, bulk, or structural data transfers be done with protections in place and, if possible, under standard contractual provisions or binding corporate rules.[107]

[105] Jelena Burnik, 'Bodo podatki iz EU res našli varnejši pristan v ZDA? : trenutek streznitve' [2015] 34(41) Pravna praksa : PP : časopis za pravna vprašanja 3.
[106] European Commission, 'Article 29 Working Party: Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995' (European Commission, 25 November) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf> accessed 14 May 2022, p. 9-10.
[107] Ibid 9.

5. TRANSFERS OF PERSONAL DATA BETWEEN THE EU AND THE USA BEFORE *SCHREMS II* DECISION

5.1. SAFE HARBOR

As previously stated, a transfer of personal data from the EU to a third country is permitted if such country has an acceptable degree of data protection. The USA was found to not provide an adequate degree of protection. One reason for this is that the United States lacks a well-organized data protection framework that encompasses both the public and commercial sectors, as well as an independent data protection authority.[108] As a result, the US Department of Commerce and the European Commission began discussing the construction of a framework for US corporations to be governed by the Data Protection Directive's provisions in 1998. After two years of discussions, an agreement was reached, and the Safe Harbor ("SH") under Decision 2000/520/EC was established.[109] Decision 2000/520/EC was binding on all Member States and their bodies. The Safe Harbor Agreement was designed to encourage trade and commercial connections by ensuring seamless movement and appropriate protection of EU personal data in US-based enterprises. It established minimal data protection requirements and allowed for the continuous movement of personal data from the EU to the US. Since 2000, the US and EU have had an agreement that promises to protect personal data of EU individuals when it is transferred to the US. Safe Harbor has permitted large corporations such as Facebook, Apple, and Microsoft to certify for themselves that they would preserve EU people' basic right to privacy while transferring data to and storing it in US data centers.[110]

[108] Kenneth A Bamberger and Deirdre K Mulligan, 'Privacy in Europe: Initial data on governance choices and corporate practices' [2013] 81(5) The George Washington law review 1542.
[109] Daniel R Leathers, 'Giving bite to the EU-US data privacy safe harbor: model solutions for effective enforcement' [2009] 41(1) Cleveland: Case Western Reserve University School of Law 200.
[110] Samuel Gibbs, 'What is 'safe harbour' and why did the EUCJ just declare it invalid?' (The Guardian, 6 October 2015) <https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection> accessed 15 May 2022.

The Safe Harbor privacy standards for the protection of data transmitted from a Member State to the United States, as well as the most often asked question, are split into two parts. The US Department of Commerce issued both documents on July 21st, 2000.[111] Safe Harbor went live later that year, and American corporations were initially wary of it. Nevertheless, businesses progressively subscribed to the system to prevent penalties and data flow blockage by Data Protection Authorities.[112]

The Safe Harbor Framework allowed businesses on both sides of the Atlantic to exchange personal data without having to do a detailed data protection analysis or check compliance with EU data protection laws. This initiative was created to alleviate administrative burdens and ensure the continued flow of personal data throughout the EU. The system relied on firms' voluntary involvement.[113]

If a business wished to join the framework, it had to first develop a privacy policy that adhered to the following principles: notice, choice, onward transfer, data security, data integrity, access, and enforcement.[114] The main purpose of notice requirement was to empower the individuals by mandating that they are informed about why their personal is processed, and enabling them

[111] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance) [2000] OJ 2 215/1, Article 1.
[112] European Commission, 'Commission Staff Working Document: The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce' (European Commission, 20 October) <https://ec.europa.eu/transparency/documents-register/detail?ref=SEC(2004)1323&lang=en> accessed 16 May 2022.
[113] Sergio Carrera and Elspeth Guild, 'The End of Safe Harbor: What Future for EU-US Data Transfers?' [2015] 22(5) Maastricht journal of European and comparative law 651.
[114] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance) [2000] OJ 2 215/1.

to select if they wish that their data is processed for another reason than those that were initially obtained.[115]

Commitment to the Safe Harbor could also be restricted in some situations: (a) if necessary to meet the requirements of national security, public interest or detection and prosecution; (b) by law, governmental act or case-law which creates incompatibilities of obligations or express powers, provided that the organization can demonstrate in the exercise of such powers that its failure to comply with the principles is limited to what is necessary to pursue legitimate interests. on the basis of such powers; or (c) where a directive or the law of a Member State allows exceptions and derogations, provided that such exceptions and derogations apply in comparable circumstances. [116]

An entity intending to transmit personal data from the EU via the Safe Harbor framework was required to self-certify its compliance to the principles and frequently asked questions with the US Department of Commerce.[117] Only businesses that clearly and publicly announced their commitment to the Safe Harbor while also being controlled by the Federal Trade Commission ("FTC") were able to join the framework.[118]

Individual data subjects had access to complaint channels in the case of infringement by organizations. In accordance with the implementation principle, effective privacy protection had to include mechanisms to ensure compliance with the principles, complaint mechanisms for data subjects affected by non-compliance with the principles, and consequences for organizations

[115] Annex I Decision 2000/520/EC.
[116] Annex I Decision 2000/520/EC.
[117] Article 1 para 3 Decision 2000/520/EC..
[118] Article 1 para 2 Decision 2000/520/EC.

that do not respect the principles.[119] Complaints had to be directed first to the proper organization, and subsequently to independent grievance channels. The Federal Trade Commission oversaw addressing infringements.[120]

Companies registered with the Safe Harbor could be held legally accountable for breaches of privacy, and civil causes of action for damages for invasion of individuals' privacy were available under US common law, as well as several federal and state privacy legislation.[121] However, the FTC's real enforcement power was restricted to misleading business practices, and it had no regulatory control over the banking, telecommunications, or employment sectors.[122]

This framework has been chastised for its dependence on voluntary adherence, certified corporations' self-certification, and public authority enforcement obligations.[123] It was judged to be deficient in terms of enforcing those principles by the European Commission itself.[124] Until the CJEU canceled it in 2015, it continued to function as the most frequently used legal bases for EU-US data transfers of personal data and was depended on by hundreds of firms.

5.2. SNOWDEN DISCOVERIES

The revelations of Edward Snowden, which were published by three powerful newspapers: The Guardian, The Washington Post, and Der Spiegel, stunned the globe in June 2013. These are

[119] Annex I Decision 2000/520/EC.
[120] Annex II Decision 2000/520/EC.
[121] Annex IV Decision 2000/520/EC.
[122] Joel R Reidenberg and Elspeth Guild, 'E-commerce and trans-Atlantic privacy' [2001] 38(3) Houston law review 743.
[123] European Commission, 'Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU' (European Commission, 27 November) <https://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com(2013)0847_en.pdf> accessed 15 May 2022, p. 4
[124] Ibid 5.

discoveries about the actions of American intelligence agencies, specifically the National Security Agency ("NSA"), and the existence of large-scale surveillance programs.

The first document to be made public was a secret court order revealing that the National Security Agency was collecting phone conversation recordings taken from one of America's top telecommunications companies. The NSA was given access to text, phone, and video messages held on the servers of firms involved in the internet and technology, including Facebook, Google, Apple, and Yahoo. Both Americans and foreigners' data were affected. Some records even suggest that the NSA had direct access to the firms' systems, something the companies deny.[125] The Snowden disclosures also showed that communication data from fiber-optic connections connecting North America and Europe was intercepted in bulk (program TEMPORA).

In response to the charges, the NSA and the US government stated that the program's usage was lawful and that it has proven to be an invaluable tool in the fight against terrorism thus far. However, the discoveries had a significant influence on public opinion in the United States.[126] After all, the consequences of Snowden's revelations were reflected in revisions in American legislation. In January 2014, Obama issued a presidential directive urging intelligence services to focus data collection, limiting the use of large databases to six national security purposes (counter-spying, terrorism, weapons of mass destruction, cyber security threats to the armed forces, and international threats of crime). The Freedom Act, which restricts the collecting of vast volumes of data and permits corporations to provide transparency reports on how many times US authorities have sought access to data, has been in effect since 2015.[127]

[125] Ewen Macaskill and Gabriel Dance, 'NSA Files: Decoded' (The Guardian, 1 November 2013) <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1> accessed 16 May 2022.
[126] Ibid.
[127] European Commission, 'EU-US Privacy Shield: Frequently Asked Questions' (European Commission, 12 July 2016) < https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_2462> accessed 16 May 2022.

However, the Snowden discoveries triggered additional complaints, and one of them resulted in *Schrems I* judgment, which had a direct effect on validity of Safe Harbor Framework.

5.3. *SCHREMS I* DECISION

Maximillian Schrems is an Austrian citizen who has been a user of Facebook since 2008. Schrems, like every other EU person, had to sign a contract with Facebook Ireland, a subsidiary of Facebook Inc. in the United States to be able to use Facebook platform. The reality back then was that personal data of EU persons on Facebook is thus transmitted in part or in full from Facebook Ireland to Facebook Inc. servers in the United States and is processed there.[128]

Following the Snowden leaks, which exposed widespread surveillance programs in the US, Maximillian Schrems began looking into whether Facebook users in the European Economic Area (EEA) were being monitored. Maximillian Schrems filed a complaint with the Irish Data Protection Commissioner on June 25th, 2013, requesting that the Data Protection Commissioner uses his powers to prevent Facebook Ireland from sending users' personal data to the USA. Maximillian Schrems cited Edward Snowden's allegations about the actions of US intelligence agencies, arguing that present US law and practice did not provide enough security for personal data stored there from national authorities' control. In light of the Snowden revelations, he stated that there were reasonable grounds to believe that his personal information was shared with the NSA. The Data Protection Commissioner dismissed the complaint as unfounded, stating that there was no evidence that US intelligence services had access to Maximillian Schrems' personal data and that all questions about the adequacy of personal data protection in the US should be resolved in accordance with the European Commission's decision, where the European Commission determined that the US offers an appropriate degree of personal data protection within the Safe Harbor Framework.[129]

[128] Case C-362/14, Maximillian Schrems v Data Protection Commissioner joined party Digital Rights Ireland Ltd (October 6, 2015), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=en, para 26 and 27.
[129] Ibid para 28 and 29.

Later, Maximillian Schrems filed a case in the Irish High Court, challenging the Data Protection Commissioner's decision and reviewing his appeals. According to the Irish High Court, it is illegal to transmit users' personal data to a third country unless the third country offers an equivalent degree of privacy and basic rights and freedoms protection. A Safe Harbor agreement is believed to provide an acceptable level of protection from the United States. However, because the Irish court believed the issue involved the application of European law, it asked the Court of Justice of the European Union ("CJEU") for a preliminary ruling on whether a national data protection authority could or should conduct an investigation into the adequacy of data protection in a third country bound by a European Commission's decision.[130]

Advocate General Yves Bot presented his opinion on the matter on September 23, 2015. According to the Advocate General's judgment, the Safe Harbor agreement, which facilitates the transfer of personal data from the EU to the US, must be terminated since it does not offer the legal protection required under EU law. A European Commission's finding of sufficiency, according to Advocate General Yves Bot, cannot preclude a national DPA from examining a complaint. The Safe Harbor agreement, he believes, should be ruled unlawful.[131]

The CJEU has ruled that the existence of a European Commission's decision finding that a third country provides an adequate level of protection for transferred personal data of individuals does not limit or nullify national authorities' powers under the EU Charter of Fundamental Rights and Directive 95/46/EC. The national supervisory authority to whom the request is directed must also be able to independently assess whether the transfer of a specific individual's

[130] Case C-362/14, Maximillian Schrems v Data Protection Commissioner joined party Digital Rights Ireland Ltd (October 6, 2015), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=en, para 30-34.
[131] Court of Justice of the European Union, ' Opinion of Advocate General Bot' (Court of Justice, 23 September) < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CC0362&from=EN > accessed 16 May 2022.

data to a third country complies with the Directive 95/46/EC criteria. The CJEU will consider whether the Commission provision is legitimate or not. Furthermore, the national security and public interest requirements in the United States take precedence over the Safe Harbor Framework, and American corporations must refuse to implement the Safe Harbor regulations without limitation where they contradict with such requirements. The CJEU went on to say that allowing public authorities access to the content of electronic communications infringes on the fundamental right to privacy, and that a regime that does allow for redress by data subjects, infringes on the fundamental right to effective judicial protection. CJEU stressed the need of comprehensive and effective protection and determined that the European Commission's decision of July 26, 2000, is unlawful and should be invalidated.[132]

The CJEU made clear that data transfers to the United States based on the Safe Harbor principles are no longer compliant with EU legislation by finding the Commission's adequacy determination unlawful. As a result, organizations who previously relied on the Safe Harbor for transatlantic data transfers encountered a slew of problems.[133]

5.4. PRIVACY SHIELD

If there is no determination on adequacy based on an overall evaluation of a third country, data transmission could be based on contractual solutions, according to Article 26 of the DPD. However, the contractual solution must contain critical security features. In this way, the data controller provides necessary measures for the protection of people' privacy and basic rights. These protections might be provided by contractual provisions.[134] The European Commission adopted

[132] Court of Justice of the European Union, 'The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid ' (CJEU, 6 October) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf> accessed 16 May 2022.
[133] Shara Monteleone and Laura Puccio, From safe harbour to privacy shield: advances and shortcomings of the new EU-US data transfer rules : in-depth analysis (Brussels: European Parliament 2017) 12.
[134] Article 26 (2) Directive 95/46/EC.

four sets of Standard Contractual Clauses to make data transmission easier, as well as Binding Corporate Rules for data transmission within a corporate group. Each one specifies data exporter and importer requirements.[135]

Following the *Schrems I* decision, the European Commission stated that it was in talks with the US government to create a new transatlantic data transfer agreement.[136] The discussion over enhancing the Safe Harbor Framework began already in 2014, but after the *Schrems I* decision, it became more intense and centered on the adoption of a new adequacy decision.[137] A new agreement, the Privacy Shield ("PS"), was formed to replace the Safe Harbor after discussions between the EU and the US. The PS aimed to offer a sufficient degree of protection to EU citizens whose data was transmitted to the US under the PS framework.[138] The Privacy Shield was designed to provide EU individuals with real enforcement procedures if US corporations break their personal data protection and privacy rights. EU citizens had access to a free alternative dispute resolution system through which they were able to contact their national data protection authorities, who would work with the US Federal Trade Commission to resolve disputes, as well as file a complaint with the EU's Data Protection Supervisor.[139]

The Privacy Shield scheme was similar to the Safe Harbor in that it was based on self-certification by enterprises who choose to participate and have a privacy policy that adheres to the

[135] European Commission, Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)' (European Commission, 6 November) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0566&rid=3> accessed 11 May 2022, p. 14.
[136] Ibid 3.
[137] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance) [2016] OJ 2 201/1, Article 1 (12).
[138] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance) [2016] OJ 2 201/1.
[139] Maja Brkan, 'The Unstoppable Expansion of EU Fundamental Right to Data Protection Little Shop of Horrors?' [2016] 23(5) Maastricht journal of European and comparative law 839.

privacy standards outlined in the adequacy judgment. A self-certification system could be trusted, but it must meet the requirements for effective noncompliance detection, monitoring, and discipline processes. To that purpose, any noncompliance should be detected, and any rule violations should be sanctioned.[140] The US Department of Commerce overseed monitoring and executing the Privacy Shield, as well as ensuring that organizations who self-certify are adhering to their obligations. Every year, "membership" in the Privacy Shield had to be renewed. Organizations that consistently violated the PS-principles would be withdrawn from the PS and would be required to return or erase personal data obtained under the PS. The Department of Commerce kept track of organizations that have been removed from the PS list (either by voluntary withdrawal or failure to re-certify) to see if they have returned, erased, or kept personal data previously obtained.

The Privacy Shield set more stringent duties on US corporations to protect EU individuals' personal data and to guarantee that US agencies are more closely monitored and enforced, as well as providing explicit protections. The US established a role of an ombudsman to address data protection authorities' complaints and inquiries. It was envisioned also to have shared yearly review of the PS agreement and an alternate dispute resolution method for settling grievances.[141]

The Privacy Shield principles contained the same seven principles of personal data protection as the Safe Harbor principles, but their implementation changes significantly. Changes to legal protection in general, and specifically in the case of access by US governmental agencies, as

[140] Case C-362/14, Maximillian Schrems v Data Protection Commissioner joined party Digital Rights Ireland Ltd (October 6, 2015), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=en, para 81.
[141] Julia Fioretti, 'New European, US data transfer pact agreed' (Reuters, 2 February 2016) <https://www.reuters.com/article/us-eu-dataprotection-usa-accord/new-european-u-s-data-transfer-pact-agreed-idUSKCN0VB1RN> accessed 17 May 2022.

well as data protection in the event of later transfers, were particularly important. The affected individual had various more accessible and cost-effective procedures for resolving disputes and removing recognized infractions available in the case of a breach of the Privacy Shield regulations. Personal data processing had to be based on accessible and explicit regulations, be proportionate, and have an effective, independent, and impartial control system, according to the requirements.

Some analyses claimed that the US system has a long history and that the Privacy Shield fits the EU Court's requirements, which required the US to carefully explore how to provide EU individuals with the option to safeguard their rights in the US. Some, on the other hand, underline the Privacy Shield's ambiguity. Some key assurances that security and intelligence services no longer covered personal data *en masse* were only given in the form of a written promise from the director of the US Intelligence Service, which is debatable in terms of how legally binding such a written promise is.[142]

The scope of EU legislation gradually extended with implications for foreign acquis. Enlargement through the Privacy Shield can be described as "extraterritorial enlargement" rather than "territorial enlargement" from a theoretical standpoint because the connection with the EU is established by transmitting data of EU citizens to the US rather than through a direct connection to EU territory.[143]

While US intelligence services could still access personal data in organizations under the Privacy Shield, the US assured the EU that access to public authorities for law enforcement and

[142] Jelena Burnik, 'Kako varno bo za Ščitom zasebnosti?' [2016] 35(14) Pravna Praksa: PP : Časopis za pravna vprašanja 3.
[143] Maja Brkan, 'The Unstoppable Expansion of EU Fundamental Right to Data Protection Little Shop of Horrors?' [2016] 23(5) Maastricht journal of European and comparative law 839.

national security purposes is subject to clear restrictions, safeguards, and controls, and that non-selective mass control of personal data will no longer be used in the future. Thus, mass data gathering would be employed only if specified circumstances are satisfied, and even then, it will be as targeted and concentrated as feasible. This was only intended to happen to the degree that it is required to achieve public interest purposes, such as national security or the prevention, detection, and investigation of criminal acts.[144]

Some principles in the Privacy Shield have been criticized, like for example that data subjects' rights as defined by GDPR are being weakened in the PS. This is true of the access principles, which state that an individual does not have the right to modify or erase data under the PS unless the data has been used in a way that is in violation of the PS principles.[145] Furthermore, the PS was criticized because of US government's ambiguity on personal data limitation and access, which does not specify to what degree US authorities have access to personal information or how access to such information is restricted to US authorities through the PS.[146]

Also Privacy Shield framework was challenged in front of the CJEU, the outcome of which was the landmark decision *Schrems II*.

[144] Jelena Burnik, 'Kako varno bo za Ščitom zasebnosti?' [2016] 35(14) Pravna Praksa: PP : Časopis za pravna vprašanja 3.
[145] European Commission, 'Article 29 Data Protection Working Party - Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision' (European Commission, 13 April) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf> accessed 6 May 2022, p. 25.
[146] Ibid 17.

6. *SCHREMS II* DECISION

The *Schrems II* judgment has shaken the data privacy landscape. This case affects the main current options for cross-border data transfers from the EU to the United States, while also complicating data transfers from the EU to the rest of the world. The practical impact is that it put pressure on businesses to maintain data within the European Union.[147] It invalidated the Privacy Shield framework and made transfers of personal data from EEA to USA more complicated and compliance with EU data protection legislation became more difficult to achieve. The decision provided no grace period and it brought big amount of legal uncertainty for the companies doing business on both sides of the Atlantic.[148] Given its market-disruptive potential, this is arguably one of the most important judgments in recent years. The European Court of Justice established conditions that made relying on international data transfer agreements like the Model Clauses and the Privacy Shield more problematic.[149]

In July 2020, the judgment *Schrems II* was published by the European Court of Justice (*Case C-3 1/18 Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*). This is a case that builds on the previous judgment of the CJEU – case *Schrems I* (*Case C-362/l4 Maximillian Schrems v. Data Protection Commissioner*). In *Schrems I* the Safe Harbor Framework, as already mentioned in this master thesis above, was invalidated.[150]

[147] Anupam Chander, 'Is data localization a solution for 'Schrems II'?' [2020] 23(3) Journal of international economic law 772.
[148] Barbara Sandfuchs, 'The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II' [2021] 70(3) GRUR International 245.
[149] JanXavier Dhont, 'Schrems II The EU adequacy regime in existential crisis?' [2019] 26(5) Maastricht journal of European and comparative law 597.
[150] Virgílio Emanuel Lobato Cervantes, 'The Schrems II judgment of the court of justice invalidates the EU – US privacy shield and requires 'case by case' assessment on the application of standard contractual clauses (SCCS)' [2020] 6(4) European data protection law review 602.

This case is another chapter of legal proceedings initiated by Maximillian Schrems whose complaint was pointed against Facebook Ireland and their transfer of EU individuals' personal data to Facebook Inc., which is based in the USA. The Irish Data Protection authority was responsible for leading the investigation. This proceeding got the final chapter at CJEU and, as already mentioned in this master thesis above, the outcome of the *Schrems I* judgement was invalidation of the Safe Harbor Framework, which allowed for data transfers between the EU and the US prior to its invalidation. As it was in the interest of EU and US for the companies to be able to continue transferring personal data, a political solution was introduced which resulted in the roll out of the Privacy Shield Framework.[151] Now this framework was again being challenged by Maximillian Schrems and in this chapter, I will explain more about the case and its consequences. What is important to highlight here is that the *Schrems I* judgement was based on Directive 95/46/EC, and the *Schrems II* judgement was issued based on the assessment of compliance with the General Data Protection Regulation - GDPR.[152]

The GDPR includes rigorous safeguards to guarantee that everyone's right to privacy is protected. Art. 44 GDPR requires that the right to privacy is safeguarded when personal data is transferred from EEA to a third country. Articles 45 and following of the GDPR outline the various data transfer mechanisms for ensuring that a data export meets the appropriate level of protection. Before this second judgment in the Schrems legal battle, the companies on both sides of Atlantic relied on the Privacy Shield framework and on the Standard Contractual Claues. With *Schrems II decision*, this has changed completely.[153]

[151] Barbara Sandfuchs, 'The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II' [2021] 70(3) GRUR International 245.
[152] Barbara Sandfuchs, 'The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II' [2021] 70(3) GRUR International 245.
[153] Ibid 245.

6.1. JUDGMENT BACKGROUND

The High Court of Ireland reversed the Irish Data Protection Authority's rejection of Maximillian Schrems' complaint after the *Schrems I* decision and returned the matter to this body for review. The Irish DPA launched an inquiry when the Grand Chamber invalidated the Safe Harbor judgement, and ordered Maximillian Schrems to reformulate his complaint.[154]

Maximillian Schrems asked that Facebook Ireland provide the legal basis for Facebook users' personal data being transferred from the EU to the US. The Standard Contractual Clauses were utilized by Facebook Ireland to underpin a data transfer processing agreement with Facebook Inc.[155] The Irish Data Protection Authority investigated whether the US offered appropriate protection for EU individuals' personal data and, if not, whether the use of Standard Contractual Clauses provided adequate protection for those people' freedoms and basic rights. Because the Maximillian Schrems' complaint hinged on the legal validity of the Standard Contractual Clauses decision[156], the Irish Data Protection Authority forwarded the questions to the High Court of Ireland, requesting that it refer questions to the Court of Justice for a preliminary ruling.[157]

The High Court of Ireland requested the preliminary finding sought by the DPA in a 152-page judgment dated 3 October 2017. The referring court asked the Court of Justice 11 questions.[158] They included queries about whether the GDPR applies to transfers of personal data made under

[154] Xavier Tracol, "“Schrems II”: The return of the Privacy Shield' [2020] 39(11) The computer law and security report 2.
[155] Ibid 2-3.
[156] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) (Text with EEA relevance) [2010] OJ 2 39/1.
[157] Xavier Tracol, "“Schrems II”: The return of the Privacy Shield' [2020] 39(11) The computer law and security report 3.
[158] Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (July 20, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CJ0311&qid=1653197642544&from=EN, para 57 and para 68.

the SCC decision's standard data protection clauses, what degree of protection the GDPR demands in such transfers, and what duties DPAs have in those situations. The legal validity of both the SCC and the Privacy Shield judgements was also questioned by the High Court.[159]

6.2. ADVOCATE GENERAL OPINION

Advocate General Saugmandsgaard Øe recommended in his opinion that the Grand Chamber respond that the investigation of the issues revealed nothing that would invalidate the SCC decision and that the decision was legally legitimate.[160]

The Advocate General also differentiated between the processing of personal data for the purpose of transfer and further processing by national security authorities in third country: *"In that regard, it must be emphasised that the transfer of personal data from a Member State to a third country constitutes, as such, 'processing' within the meaning of Article 4(2) of the GDPR, carried out on the territory of a Member State. The first question is specifically intended to determine whether EU law applies to the processing consisting in the transfer itself. That question does not concern the applicability of EU law to any subsequent processing by the United States authorities for national security purposes of the data transferred to the United States, which is excluded from the scope ratione territoriae of the GDPR."*[161]

The Advocate General was also of the opinion that the Standard Contractual Clauses are a valid data transfer mechanism, no matter if there is an adequacy decision granted to third country or not. His reasoning is that the data transfer mechanisms as defined in GDPR provide high level

[159] Xavier Tracol, '"Schrems II": The return of the Privacy Shield' [2020] 39(11) The computer law and security report 3.
[160] Ibid 3.
[161] Court of justice, 'Opinion of Advocate General Saugmandsgaard Øe ' (Court of Justice, 19 December) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CC0311&from=en> accessed 4 May 2022, para 104.

of protection of personal data, no matter if they are based on an adequacy decision or not. The Standard Contractual Clauses as published by the EU Commission, therefore establish a base-line procedure for all transfers in this respect, independent of the third-party destination or the level of data security provided there.[162]

Another thing that the Advocate General mentions in his opinion is that the Irish Court impliedly questioned the validity of the Privacy Shield. According to the Advocate General, the CJEU should not focus on assessing this question, because the proceeding in front of the referring court only deals with the validity of the Standard Contractual Clauses decision, and not about the validity of the Privacy Shield Framework.[163]

6.3. THE JUDGMENT

6.3.1. DECISION ON APPLICABLE LAW

To begin with, the CJEU believed that EU law, specifically the GDPR, applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, even if that data may be processed by the authorities of the third country in question for the purposes of public security, defense, and State security at the time of the transfer or thereafter. Furthermore, this form of data processing by third-country authorities cannot exclude a transfer from the GDPR's reach.[164]

"Therefore, the answer to the first question is that Article 2(1) and (2) of the GDPR must be interpreted as meaning that that regulation applies to the transfer of personal data for

[162] Xavier Tracol, '"Schrems II": The return of the Privacy Shield' [2020] 39(11) The computer law and security report 3.
[163] Ibid 4.
[164] Virgílio Emanuel Lobato Cervantes, 'The Schrems II judgment of the court of justice invalidates the EU – US privacy shield and requires 'case by case' assessment on the application of standard contractual clauses (SCCS)' [2020] 6(4) European data protection law review 604.

commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security."[165]

The CJEU determined that the potential that a public authority of such third country will be also processing personal data is not relevant, unlike Advocate General Saugmandsgaard, the CJEU did not make a difference between the processing connected to the transfer itself and to further processing.[166]

6.3.2. LEVEL OF PROTECTION REQUIRED FOR TRANSFERS OF PERSONAL DATA FROM THE EU TO THIRD COUNTRIES

The CJEU ruled in *Schrems II* that the personal data transferred to a third country has to be given a level of data protection that is equivalent to the one ensured in the EU by GDPR:[167]

"Therefore, the answer to the second, third and sixth questions is that Article 46(1) and Article 46(2)(c) of the GDPR must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter. To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or

[165] Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (July 20, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CJ0311&qid=1653197642544&from=EN, para 89.
[166] Xavier Tracol, '"Schrems II": The return of the Privacy Shield' [2020] 39(11) The computer law and security report 4.
[167] Ibid 5.

processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation."[168]

6.3.3. DECISION ON PRIVACY SHIELD

It is in the interest of companies in the EEA and the USA to be able to rely on legal bases that they can use for transferring personal data from EEA over the Atlantic Unfortunately, as presented above in this master thesis, there are major differences between level of protection of personal data in the USA and in the EEA, therefore a general adequacy decision granted to the USA was by the EU Commission was never on the table and was never really considered.[169]

This is why the Privacy Shield was introduced – it tried to de-bureaucratize data transfer mechanisms between the EEA and the USA on one hand, and take into account the necessity for protection of personal data of EU individuals by data exporters on the other. In *Schrems II*, the main problem that the CJEU found with Privacy Shield is that there were issues with the need and proportionality of US national surveillance bodies to access personal data of EU individuals, and the non-existence of judicial redress for EU individuals.[170]

The CJEU decided to assess also the validity of the Privacy Shield Decision. The assessment was made in the light of the rights in the Charter (Article 7 – right to respect for private life;

[168] Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (July 20, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CJ0311&qid=1653197642544&from=EN, para 105.
[169] Barbara Sandfuchs, 'The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II' [2021] 70(3) GRUR International 246.
[170] Ibid 246.

Article 8 – right to personal data protection; Article 47 – right to effective judicial protection), as well as the obligations and requirements of the GDPR. The CJEU found out that the legislation in the USA that deals with national security takes precedence over the safeguards that are included in the Privacy Shield Framework. This means that the problematic US legislation can interfere with the rights of EU data subjects, whose personal data is being transferred to the US. US surveillance laws - Section 702 of the FISA and EO 12,333.49 which both address the situation of servers in the EU that are run by US "electronic communication service providers" subject to Section 702 of the FISA or where some services are outsourced to a US service provider, were scrutinized by the CJEU.[171]

In terms of judicial protection, the Court considers that the Privacy Shield's ombudsperson system does not provide data subjects with any recourse before a body that provides assurances substantially equal to those needed by EU legislation. For example, assuring the ombudsperson's independence as well as the presence of procedures permitting ombudsperson to make enforceable decisions for US surveillance agencies. For all these reasons, the Court found the Privacy Shield to not be lawful and has invalidated it.[172]

6.3.4. DECISION ON STANDARD CONTRACTUAL CLAUSES

The CJEU found also that the Standard Contractual Clauses that were issued in 2010 (and amended in 2016) by the European Commission are a valid data transfer mechanism.[173] However, they should not be a general solution for all kinds of data transfers – each case should be

[171] Xavier Tracol, '"Schrems II": The return of the Privacy Shield' [2020] 39(11) The computer law and security report 6.
[172] Court of justice, 'The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield ' (Court of Justice, 16 July) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf> accessed 3 May 2022.
[173] Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (July 20, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CJ0311&qid=1653197642544&from=EN, para 148.

assessed and analyzed separately. The main purpose of this exercise is that the EU data subjects are granted efficient level of data protection – equivalent to the one guaranteed in the EU by the GDPR.[174]

The CJEU assessed whether the Standard Contractual Clauses decision is even a valid one, as this data transfer mechanism, because of their contractual characteristics, does not legally bind the public authorities in a third country. The Grand Chamber did add, however, that the Standard Contractual Clauses decision's validity hinged on whether it included effective mechanisms to ensure compliance with the level of protection required by EU law in practice, and that transfers of personal data pursuant to such clauses are either suspended or prohibited in the event of a breach of such clauses or the inability to honor them. The Standard Contractual Clauses decision, according to the Grand Chamber, indeed does include such effective mechanisms.[175]

As mentioned above, even though the Court did not invalidate Standard Contractual Clauses, it still provided that the involved parties should assess all circumstances of the specific data transfer in question and add additional supplementary measures[176] as an add-on to the Standard Contractual Clauses, in order to ensure the sufficient level of data protection: *"It is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to*

[174] Barbara Sandfuchs, 'The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II' [2021] 70(3) GRUR International 246.
[175] Xavier Tracol, '"Schrems II": The return of the Privacy Shield' [2020] 39(11) The computer law and security report 5.
[176] Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (July 20, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CJ0311&qid=1653197642544&from=EN, para 133.

those offered by those clauses".[177] However, the Court does not provide any example of what the additional safeguards could be or what could be the format of these. [178] This was later introduced by the European Data Protection Board in their recommendations, which I will describe into details later in this master thesis.

While the *Schrems II* judgement dealt with controller-processor SCCs, the same considerations apply to controller-controller SCCs. The CJEU's decisions apply not only to data exports to the United States, but also to any third country (not subject to an adequacy decision).[179]

6.3.5. OBLIGATIONS OF DPAS FOR TRANSFERS OF PERSONAL DATA FROM THE EU TO THIRD COUNTRIES: INADEQUATE PROTECTIONS COMPEL DPAS TO EITHER SUSPEND OR PROHIBIT SUCH TRANSFERS

CJEU also decided regarding the obligations of the competent supervisory authorities. In the ruling it states that in case there is no existing adequacy decision in place with a third country, then the competent supervisory authority is required to suspend or prohibit transfer of personal data where Standard Contractual Clauses are taken as legal basis, if the Standard Contractual Clauses alone do not ensure an efficient level of data protection in the third country, because they cannot be complied with in the third country:[180]

"(...) the competent supervisory authority is required, under Article 58(2)(f) and (j) of the GDPR, to suspend or prohibit such a transfer, if, in its view and in the light of all the

[177] Ibid para 134.
[178] Xavier Tracol, '"Schrems II": The return of the Privacy Shield' [2020] 39(11) The computer law and security report 5.
[179] Barbara Sandfuchs, 'The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II' [2021] 70(3) GRUR International 246.
[180] Virgílio Emanuel Lobato Cervantes, 'The Schrems II judgment of the court of justice invalidates the EU – US privacy shield and requires 'case by case' assessment on the application of standard contractual clauses (SCCS)' [2020] 6(4) European data protection law review 604.

circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer."[181]

[181] Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (July 20, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CJ0311&qid=1653197642544&from=EN, para 146.

7. THE FUTURE OF TRANSFERS OF PERSONAL DATA FROM THE EU TO THE USA

What does the *Schrems II* judgment mean for the companies doing business in the EEA and in the USA? Well, some support and guidance was presented by the European Data Protection Board, who issued the first draft of the EDPB recommendations in November 2020, and an updated version of recommendations in June 2021. This will be described more in details below.

Additionally, the European Commission issued revised Standard Contractual Clauses in June 2021. The implementation of a new set of Standard Contractual Clauses had been long overdue, given that the previous ones were still based on the Directive 95/46 and had additional flaws, such as transfers from EU processors to subprocessors and transfers from EU processors back to their controllers. These new sets of Standard Contractual Clauses take the above mentioned scenarios into account and until end of September 2021, all companies who are relying on the old set of Standard Contractual Clauses need to replace them with the updated ones. However, the EDPB mentioned that the updated Standard Contractual Clauses are not a "one-stop-shop" and need to be analyzed separately for each situation and in combination with additional supplementary measures.[182]

7.1. THE EUROPEAN DATA PROTECTION BOARD RECOMMENDATIONS

On 18th June 2021 the European Data Protection Board ("EDPB") published the *"Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU*

[182] Barbara Sandfuchs, 'The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II' [2021] 70(3) GRUR International 245.

level of protection of personal data".[183] The purpose of these recommendations is to help the data exporters with assessing a third country from a data protection point of view and to recognize and put in place the correct supplementary measures where necessary in order to comply with the GDPR and the *Schrems II* judgment.[184] The idea of the EDPB is to provide advice to data controllers and data processors operating as data exporters on how to detect and implement supplemental security measures. These guidelines are intended to provide a technique for exporters to use in determining if and which extra safeguards are required for their transfers of personal data.[185]

The right to data protection requires from data controllers and/or data processors to not just acknowledge that it exists, but also to comply with it. They should actively adhere to it by ensuring that contractual, technical, and organizational measures are included, so that compliance with the applicable data protection legislation can be assured. This concept is also known as accountability principle.[186] EDPB provides guidance on how to ensure the effectiveness of accountability principles in data transfers in 6 steps, which I will describe more in details below. These steps not only give recommendations to all data exporters that are transferring personal data outside of the EEA, but they also require from the data exporter to record the steps taken when making an assessment and provide them to the data protection authority if this is needed.[187]

[183] European data protection board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (*European Data Protection Board*, 18 June 2021) <https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf> accessed 5 May 2022.
[184] Ibid 3.
[185] Ibid 8.
[186] Ibid 9.
[187] Ibid 10.

7.1.1. FIRST STEP: DATA EXPORTER SHOULD FAMILIRIZE THEMSELVES WITH THEIR TRANSFER OF PERSONAL DATA

The EDPB recommendations require from data exporters to first of all analyze the transfer flow of personal data and to keep recordings of such data mapping.[188] This assessment should take place before first transfer of personal data for each separate purpose of data transfer.[189] It is important to check not only the processing location of the direct data importer, but also the onwards transfers of personal data (i.e. in case the direct data importer is using sub-processors, these data flows should be taken into consideration as well when performing the assessment). EDPB suggests that a potential solution on how to map the personal data transfer flow is to keep an up-to-date records of processing activities as required by GDPR.[190]

Data exporters should consider in this first step also the minimization principle – personal data shared to a third country should be limited to the data needed for the purpose of processing and nothing more than that.[191] Data exporter should also not forget that in case of usage of cloud infrastructure, we talk about an international transfer also if the data is only stored ("hosted") outside of the EEA. Moreover, the assessment should take place even if personal data is stored ("hosted") on servers in the EEA, but the support services are provided from a third country by the service provider. This would also count as a transfer of personal data to a third country, because the third country service provider is accessing personal data stored in the EEA.[192]

7.1.2. SECOND STEP: THE DATA EXPORTER SHOULD IDENTIFY THE DATA TRANSFER MECHANISM THEY RELY ON

[188] Ibid 10.
[189] Ibid 11.
[190] Ibid 11.
[191] Ibid 11.
[192] Ibid 11.

The next step that data exporters should take is to identify the valid transfer mechanism for international transfer of personal data they can rely on in accordance with Chapter V. of the GDPR[193] (see also section 6. of this master thesis).

As described in the section 6. above, the least complex to rely on is the case where the European Commission has granted an adequacy decision to a third country, and with this the third country was recognized as a country where data protection legislation and practices offers an adequate level of protection, like the level of data protection assured in the EEA. If the data exporter transfers data solely to such third country, then this transfer is considered a compliant with the GDPR and no additional steps of the EDPB recommendations need to be followed.[194] As already mentioned in this paper, there are currently 13 third countries with an adequacy decision granted by the European Commission. Data exporters should also keep in mind that the adequacy decisions are not permanent, and that they may be invoked, so this should be monitored on a regular basis.

In case there is no adequacy decision (as this is the case for the United States of America), then the data exporter must find another data transfer mechanism that they can rely on and that would ensure the satisfactory level of protection of personal data. According to the Article 46 GDPR[195], the possible options are - standard data protection clauses; binding corporate rules; codes of conduct; certification mechanisms and ad hoc contractual clauses. Nevertheless, relying solely on one of these data transfer mechanisms when transferring personal data to a third

[193] Chapter 5 GDPR.
[194] European data protection board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (*European Data Protection Board*, 18 June 2021) <https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf> accessed 5 May 2022, page 12.
[195] Article 46 GDPR.

country may not be enough and additional supplementary (technical, organizational, contractual) may need to be included to ensure a sufficient level of protection of personal data for the specific transfer.[196]

As per Article 49 GDPR[197], the possible data transfer mechanism can be also derogations, however these are exceptional, and the data exporter should ensure that the strict requirements for each of the options there are met first.[198] As these are rather exceptional in the commercial world, I will not go into details about these options in this paper.

7.1.3. THIRD STEP: IF DATA TRANSFER MECHANISM FROM ARTCILE 46 GDPR IS USED, THEN DATA EXPORT SHOULD ASSESS AL CIRCUMSTANCES OF THE DATA TRANSFER

This step should be followed if the data transfer mechanism is based on one of the options as set out in Article 46 GDPR. This step is important to be followed because these data transfer mechanism options do not ensure the adequate level of protection of personal data *per se*. Therefore, an additional assessment is needed – data exporter needs to check together with the data importer whether the legislation or practices in third country might impair the efficiency of the data transfer mechanism from Article 46 GDPR that is used.[199]

[196] European data protection board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (*European Data Protection Board*, 18 June 2021) <https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf> accessed 5 May 2022, page 13.
[197] Article 49 GDPR.
[198] European data protection board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (*European Data Protection Board*, 18 June 2021) <https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf> accessed 5 May 2022, page 13.
[199] Ibid 14.

In this step of the assessment the focus should be on whether the legislation and/or practices in a third country allow public authorities to access personal data that is transferred with or without informing the data importer about it. For example, the assessment of third party's legislation and practices should consider the following:[200]

- circumstances of the data transfer (purpose, types of entities involved, relevant industry sector, personal data categories, location of processing / storage, whether remote access will take place, format of transferred data, onward transfers)
- all involved parties processing personal data in third country should be assessed (controllers, processors, sub-processors)
- existence of legislation authorizing public authorities to access personal data processed by data importer
- assessment of rules and practices of general nature, because these affect the protections as set out in the selected data transfer mechanism as per Article 46 GDPR[201]
- the criteria that the EU Commission uses when they assess the adequacy of the level of protection as per 45 (2) GDPR[202]
- verification of effectiveness of data subjects' rights to access, correct, delete data and the right to judicial redress in third country (e.g. it should be ensured that third country legislation does not prevent exercising of these rights despite data importer's commitment to ensure then)
- assess whether the legislation in third country which allows public authorities to access personal data processed by data importer can count as justifiable interference (assessment criteria is provided in the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020)

[200] Ibid 14-17.
[201] Article 46 GDPR.
[202] Article 45 (2) GDPR.

The assessment should consider the specific use case of data transfer and it should take into the consideration the publicly available legislation and sources, which must be relevant, objective, reliable and verifiable.[203]

Finally, the result of the assessment might reveal that either:[204]

- The transfer of personal data to third country is safe and the level of protection of personal data in third country is equivalent to the level of protection of personal data in the EEA. In this case, no additional supplementary measures need to be implemented and the additional steps of the EDPB recommendations do not have to be followed. Nevertheless, the data exporter should still assess the status of data transfer to third country on regular basis and take actions if anything changes in that regard.
- The transfer of personal data to third country is problematic and does not offer equivalent level of protection as the one ensured within the EEA. In this case the data exporter should ensure to follow step four (see below) of the recommendations provided by the EDPB or not to transfer personal data at all.

The USA legal framework at this point does not efficiently ensure an essentially equivalent level of protection of protection of personal data, therefore the transfer of personal data to the USA is either forbidden or additional appropriate supplementary measures need to be put in place or, alternatively, if data exporter can prove and demonstrate with a detailed report that the problematic legislation / practices will not be applied to their transfer of personal data (e.g. also

[203] European data protection board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (*European Data Protection Board*, 18 June 2021) <https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf> accessed 5 May 2022, page 14 and 18.
[204] Ibid 20.

taking into account also experience of other companies in similar sector) and that the data importer will therefore be able to comply with their obligations, then the data exporter may also decide to proceed with the data transfer.

7.1.4. FOURTH STEP: ADDITIONAL APPROPRIATE SUPPLEMENTARY MEASURES

When the assessment as described in the step three above shows that the level of protection of personal data is not sufficient, then the data exporter and data importer should consider implementing appropriate supplementary measures to achieve the level of protection equivalent to the one ensured in the EEA. This should be done on case-by-case basis. There could also be cases where no supplementary measure would make the transfer of personal data to a third country legal – in this case the data exporter is not allowed to transfer data to a third country.[205]

Supplementary measures can be grouped into:[206]

- Contractual supplementary measures
- Technical supplementary measures
- Organizational supplementary measures

These can be combined to ensure that the satisfactory level of protection of personal data is achieved. However, it is important to highlight that only contractual and organizational supplementary measures are not sufficient to ensure that public authorities in third country will not access personal data processed by the data importer, and that only appropriate technical supplementary measures can ensure the efficient protection of personal data. Contractual and

[205] Ibid 21.
[206] Ibid 22.

organizational supplementary measures can only add an additional level of protection on top of the technical supplementary measures but will not be sufficient if not implemented together with technical ones.[207]

It is important that the appropriate supplementary measures are implemented based on, for example: format of personal data, nature of personal data, length and complexity of data processing workflow, number of processors, onward transfers, etc.[208]

EDPB recommendations also provide some examples of cases in which effective measures are satisfactory:

- Use case 1: "*Data storage for backup and other purposes that do not require access to data in the clear"*[209] - EDPB provides examples of what technical supplementary measures are effective in a case when the data exporter is transferring personal data to a service provider for hosting on their servers. These are the situations where the service provider does not access data in the clear, and therefore technical supplementary measures can be effective in preventing national authorities in third country from accessing them. Focus here is on efficient encryption and managing of encryption, as the encryption key has to be in the hands of the data exporter that is based in the EEA or in a jurisdiction that offers an equivalent level of protection of personal data.

- Use case 2: *"Transfer of pseudonymized data*"[210] - EDPB provides examples of what technical supplementary measures are effective when the data exporter first pseudonymizes personal data and only then shares it to a third country for processing. What is

[207] Ibid 22.
[208] Ibid 22.
[209] Ibid 30.
[210] Ibid 31-32.

important is that the data exporter keeps the "key" that can un-pseudonymize personal data and does not share this key with the data importer in a third country, so that the authorities in third country cannot decrypt such pseudonymized data.

- Use case 3: *"Encryption of data to protect it from access by the public authorities of the third country of the importer when it transits between the exporter and its importer"*[211] - EDPB provides examples of what technical supplementary measures are effective when the data exporter transfers personal data to a third country where the laws of such country allow that the public authorities access personal data while it is transiting from the EEA to the third country. The focus here is on the transfer encryption, potentially in a combination with the end-to-end content encryption.

- Use case 4: "*Protected recipient"*[212] - EDPB provides examples of what technical supplementary measures are effective when the data exporter transfers personal data to a third country where the laws of the third country safeguard the data importer from sharing the data (for example, provision of legal advice to customers – duty of professional secrecy applies to the service provider in third country). This is an example where transport encryption can be seen as a satisfactory supplementary measure.

- Use case 5: *"Split or multi-party processing"*[213] - EDPB provides examples of what technical supplementary measures are effective when the data exporter transfers personal data to more than one data importer. In this case data exporter splits the data in such a way that only the data exporter can connect all the pieces to be able to make

[211] Ibid 32-33.
[212] Ibid 33.
[213] Ibid 33-34.

personal data identifiable. This means that the data importers cannot identify personal data on their own, because they don't have all the pieces of the puzzle. The data importers in this situation each process their part of data as their part of providing the services and when they transfer the processed data back to the data exporter, data exporter is then able to merge it all together again. EDPB considers such a split to be an efficient supplementary measure and in line with GDPR requirements.

EDPB recommendations also provide a couple of examples of scenarios where effective measures are not identified:

- Use case 6: *"Transfer to cloud services providers or other processors which require access to data in the clear"*[214] - EDPB mentions a very common example, where the data exporter engages a cloud service provider in a third country and this cloud service provider is accessing data in the clear for the purpose of providing the services (e.g. technical support or any other processing of personal data in the cloud). This is different than just using a service provider for hosting purposes. Cloud service providers are accessing data in the clear so that they can perform the services, which also means that the public authorities are able to access it when such data is in the clear. EDPB recommendations state that if the data importer is in possession of the cryptographic keys then even encryption in transit and encryption at rest are not sufficient supplementary measures.

- Use case 7: "*Transfer of personal data for business purposes including by way of remote access"*[215] - also this is an example where the data importer that is based in a third

[214] Ibid 34-35.
[215] Ibid 35-36.

country is accessing personal data in the clear, so that personal data cannot be encrypted or pseudonymized in a way that would prevent public authorities from accessing it. Also in this case the data is unencrypted in order for the data exporter to provide the services, therefore encryption cannot be a sufficient supplementary measure.

In my opinion, especially use case 6 is very problematic for EEA based data exporters as there are many US based service providers who offer services and are therefore accessing data in the clear. As it stands at the moment, there is no technical solution that could count as an efficient supplementary measure in these situations.

In addition to the technical supplementary measures, the EDPB recommendations provide also examples of contractual and organizational supplementary measures:

- Contractual supplementary measures are contractual clauses that can be included in the contract between data exporter and data importer to ensure a greater level of protection of personal data. As mentioned above, if the technical supplementary measures are not efficient, then the contractual supplementary on their own will not be deemed as efficient as well. The focus of EDPB contractual supplementary measures examples is on obligation to use specific technical measures, transparency obligations and obligations to take specific actions.[216]
- Same as with contractual supplementary measures, also organizational measures are not enough if also technical supplementary measures are in place. They can only complement the efficient technical supplementary measures. The focus here is on internal policies, organizational methods and other standards that data exporter and data importer can implement. Examples provided by the EDPB mention the following groups of

[216] Ibid 36-43.

organizational supplementary measures: internal policies for governance of transfers especially with groups of enterprises, transparency and accountability measures, organization methods and data minimization measures and adoption of standards and best practices.[217]

7.1.5. FIFTH STEP: NEXT STEPS AFTER THE DATA EXPORTER HAS IDENTIFIED EFFECTIVE SUPPLEMENTARY MEASUERS

If the data exporter identifies effective supplementary measures, then the next step is to apply the selected data transfer mechanism[218] as per Article 46 GDPR:

- Standard Contractual Clauses
- Binding Corporate Rules
- Ad-hoc contractual clauses

Standard Contractual Clauses do not need an additional approval from the data protection authorities. As long as the supplementary measures do not contradict (directly or indirectly) the content of the Standard Contractual Clauses and the protection as ensured under GDPR is ensured, then the data exporter may proceed with this data transfer mechanism. However, as soon as the parties modify the supplementary measures or clauses in a way that these contradict the Standard Contractual Clauses, then the parties can no longer use this data transfer mechanism, but they must find another legal basis.[219]

7.1.6. SIXTH STEP: RE-ASSESSMENT OF THE SAFEGUARDS THAT ARE IN PLACE

[217] Ibid 43-46.
[218] Ibid 23-25.
[219] Ibid 23-24.

Data exporters should monitor and re-assess whether the initial assessment that allowed for the transfer of personal data to third country is still valid. The monitoring should include monitoring of development of legislation in third country as well as monitoring whether the supplementary measures put in place are still relevant. If the circumstances change and data transfers are no longer permitted, then the data exporter should suspend such transfers.[220]

7.2. NEED FOR A NEW POLITICAL SOLUTION

As seen above, the EU data exporters may face difficult and expensive challenges in ensuring that extra protections are in place to be allowed to transfer personal data based on Standard Contractual Clauses or Binding Corporate Rules in accordance with the GDPR and *Schrems II* judgment. Given the financial importance of data transfers from the EEA to third countries, particularly the United States of America, there is a pressing need for a new data privacy framework that would come into place instead of the invalidated Privacy Shield. What the new framework should consider is for sure the regulation of public authorities' and surveillance authorities' access to personal data as well as ensuring that data subjects have an option of an efficient judicial remedy.[221]

7.3. NEW TRANS-ANTLANTIC DATA PRIVACY FRAMEWORK AROUND THE CORNER?

The European Commission and the White House surprised with a joint statement in March 2022, where they informed the public that after more than 1 year of negotiations, the EU and the USA have agreed in principle about the new Trans-Atlantic Data Privacy Framework that

[220] Ibid 25.
[221] Barbara Sandfuchs, 'The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II' [2021] 70(3) GRUR International 248-249.

will deal with the transfers of personal data between the EU and the USA and address the concerns that were raised with the *Schrems II* judgement.[222]

This new agreement envisions obligations of the USA to make changes to their legislation and put stronger focus on data protection against their surveillance activities: *"Under the Trans-Atlantic Data Privacy Framework, the United States is to put in place new safeguards to ensure that signals surveillance activities are necessary and proportionate in the pursuit of defined national security objectives, establish a two-level independent redress mechanism with binding authority to direct remedial measures, and enhance rigorous and layered oversight of signals intelligence activities to ensure compliance with limitations on surveillance activities."*[223]

This new framework comes as good news for companies that do business in the EU and US or have partners or suppliers on both continents, as such arrangement could potentially bring more clarity, ease the way the companies work together as well as open space for further collaborations: *"By advancing cross-border data flows, the new framework will promote an inclusive digital economy in which all people can participate and in which companies of all sizes from all of our countries can thrive."*[224] According to the statement by the US government, data transfers between the EU and the USA are the most used in the world, bringing the economic value of such collaboration to $7.1 trillion.[225]

---

[222] European commission, 'European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework' (*European Commission*, 25 March 2022) <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087> accessed 8 May 2022.
[223] European commission, 'European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework' (*European Commission*, 25 March 2022) <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087> accessed 8 May 2022.
[224] European commission, 'European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework' (*European Commission*, 25 March. 2022) <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087> accessed 8 May 2022
[225] The White House, 'FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework' (*The White House*, 25 March 2022) <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/> accessed 8 May 2022.

This framework includes the following key aspects[226]:

- Data will be allowed to flow freely and without risk;
- Obligatory protections limiting US intelligence agencies' access to data to what is necessary and proportional to preserve national security;
- A new two-tier redress system;
- Strong obligations for companies processing data transferred from the EU;
- Specific monitoring and review mechanisms.

As the next step, the teams from the US administration and the European Commission will work on translating the agreed framework into binding legal documents.[227]

7.4. REACTION FROM EDPB

The announcement of the EU Commission and the US government of course triggered some reactions from different players in the data protection world. The European Data Protection Board published a statement[228] where they welcomed the announcement of the Trans-Atlantic Data Privacy Framework and highlighted that this comes as a very positive step in the right direction in times where the data transfers between the EU and the US are being challenged.

[226] European Commission, 'Trans-Atlantic Data Privacy Framework' (*European Commission*, 25 March 2022) <https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100> accessed 8 May 2022.
[227] The White House, 'FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework' (*The White House*, 25 March 2022) <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/> accessed 8 May 2022.
[228] Andrea Jelinek, 'Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework' (*European Data Protection Board*, 6 April 2022) <https://edpb.europa.eu/system/files/2022-04/edpb_statement_202201_new_trans-atlantic_data_privacy_framework_en.pdf> accessed 10 May 2022.

The EDPB also highlighted that the EU Commission must seek EDPB's opinion before issuing any adequacy decision to the USA, and that the EDPB will carefully assess the potential new legal framework that will be the basis for that, based on the relevant EU legislation and case law. The focus of this assessment will be especially in how the collection of personal data for national security purposes is limited and the redress mechanisms available to the EU data subjects.[229]

7.5. REACTION FROM NOYB

On the other hand, the noyb (NOYB – European Center for Digital Rights) whose chairman is Maximillian Schrems the lead litigant in the *"Schrems I"* and *"Schrems II"* cases before the CJEU, also published on their website[230] their view on to the announcement about the new Trans-Atlantic Data Privacy Framework.

Maximillian Schrems' statement: *"We already had a purely political deal in 2015 that had no legal basis. From what you hear we could play the same game a third time now. The deal was apparently a symbol that von der Leyen wanted, but does not have support among experts in Brussels, as the US did not move. It is especially appalling that the US has allegedly used the war on Ukraine to push the EU on this economic matter.*

The final text will need more time, once this arrives we will analyze it in depth, together with our US legal experts. If it is not in line with EU law, we or another group will likely challenge it. In the end, the Court of Justice will decide a third time. We expect this to be back at the Court

[229] Andrea Jelinek, 'Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework' (*European Data Protection Board*, 6 April 2022) <https://edpb.europa.eu/system/files/2022-04/edpb_statement_202201_new_trans-atlantic_data_privacy_framework_en.pdf> accessed 10 May 2022.
[230] Noyb, '"Privacy Shield 20"? - First Reaction by Max Schrems' (*Noyb*, 25 March 2022) <https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems> accessed 10 May 2022.

within months from a final decision. It is regrettable that the EU and US have not used this situation to come to a 'no spy' agreement, with baseline guarantees among like-minded democracies. Customers and businesses face more years of legal uncertainty."[231]

Additionally, they mention that it will take some more time (more than a few months) to move from this political announcement to the actual legal document that can be reviewed and assessed. The general impression of the noyb at this point about the Trans-Atlantic Data Privacy Framework: *"Overall a political announcement without a solid text, seems to generate even more legal uncertainty for the time being."*[232]

[231] Noyb, '"Privacy Shield 20"? - First Reaction by Max Schrems' (*Noyb*, 25 March 2022) <https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems> accessed 10 May 2022.
[232] Noyb, '"Privacy Shield 20"? - First Reaction by Max Schrems' (*Noyb*, 25 March 2022) <https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems> accessed 10 May 2022.

8. CONCLUSION

It is clear that the legal regime for the transfer of personal data from the EU to the US has undergone radical changes in recent years, and all indications are that this process is far from over. Despite the political attempts in the EU and the USA to come up with an agreement that will allow free flow of personal data from one side of the Atlantic to the other, there are simply still too many differences in the basic perception of how the right to privacy and the right to data protection should be perceived. This is a result of big cultural and political differences, which are in the US heavily influenced on their fear of terrorism. They therefore open the door to mass surveillance by US intelligence services in the name of national security, which is something that is not acceptable in the EU and the reason why the existing trans-Atlantic frameworks were all invalidated in the end. In the EU, protection of personal data is a human right and a transfer of personal data to a third country, where the national surveillance authorities might access such data, should not be permitted. Nevertheless, USA is such an important economic partner for the EU based companies that there is a big need for a solution that would allow transfers of personal data to this country on one hand, and guarantee the confidentiality and safety of them on the other.

The recommendations provided by the EDPB that give guidance on the transfer of personal data to third countries are useful and they help companies with navigating on when to transfer personal data to the USA and when not. However, these recommendations are a golden standard, which is for many companies difficult and expensive to achieve and therefore prevents them from doing business or working with US companies. Due to the growing importance of transatlantic economic contacts and the growing digitalization, it will be necessary to find an pragmatic solution and most importantly, get rid of the current uncertainty in the business world, which is still very much present after the *Schrems II* landmark decision. However, in my

opinion, any new trans-Atlantic framework agreement regulating transfer of personal data between the EU and the USA will only be successful if the US government takes care of changing their legislation on a federal level first and gives the protection of personal data the treatment it deserves, i.e. similar to the one in the EU. Unfortunately, it seems that there was no real political support in the US for that so far, and it will be interesting to see if the newly announced trans-Atlantic framework will change this status quo in a way that will result in a level of protection of personal data in the US that will be equivalent to the one guaranteed in the EU.

9. BIBLIOGRAPHY

9.1. BOOKS AND ARTICLES

Anupam Chander, 'Is data localization a solution for 'Schrems II'?' [2020] 23(3) Journal of international economic law 771-784.

Barbara Sandfuchs, 'The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II' [2021] 70(3) GRUR International 245-249.

Chuan Sun, 'The European Union Privacy Directive and Its Impact on the US Privacy Protection Policy: A Year 2003 Perspective' [2003] 2(1) Northwestern Journal of Technology and Intellectual Property 99-116.

Dan Jerker B Svantesson, 'The regulation of cross-border data flows' [2011] 1(3) International data privacy law 180-198.

Daniel J Solove, The Digital Person : Technology and Privacy in the Information Age (New York, NY : : New York University Press 2004).

Daniel R Leathers, 'Giving bite to the EU-US data privacy safe harbor: model solutions for effective enforcement' [2009] 41(1) Cleveland: Case Western Reserve University School of Law 193-242.

European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law: 2018 edition (Luxembourg: Publications Office 2018).

Gregory W. Voss and Kimberly A. Houser, 'Personal Data and the GDPR: Providing a Competitive Advantage for US Companies' [2019] 56(2) American business law journal 287-344.

James X Dempsey, 'Communications privacy in the digital age: revitalizing the federal wiretap laws to enhance privacy' [1997] 8(1) Albany Law Journal of Science & Technology 65-120.

Jan Xavier Dhont, 'Schrems II The EU adequacy regime in existential crisis?' [2019] 26(5) Maastricht journal of European and comparative law 597-601.

Jelena Burnik, 'Bodo podatki iz EU res našli varnejši pristan v ZDA? : trenutek streznitve' [2015] 34(41) Pravna praksa : PP : časopis za pravna vprašanja 3.

Jelena Burnik, 'Kako varno bo za Ščitom zasebnosti?' [2016] 35(14) Pravna Praksa: PP : Časopis za pravna vprašanja 3.

Joel R Reidenberg and Elspeth Guild, 'E-commerce and trans-Atlantic privacy' [2001] 38(3) Houston law review 717-750.

Julian Wagner, 'The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?' [2018] 8(4) International data privacy law 318-337.

Kenneth A Bamberger and Deirdre K Mulligan, 'Privacy in Europe: Initial data on governance choices and corporate practices' [2013] 81(5) The George Washington law review 1529-1664.

Lauren B Movius and Nathalie Krup, 'US and EU Privacy Policy: Comparison of Regulatory Approaches' [2009] 3(1) International journal of communication 169-187.

Law Reform Commission of New Zealand, Invasion of Privacy: Penalties and Remedies – Review of the Law of Privacy (NZLRC 2009).

Maja Brkan, 'The Unstoppable Expansion of EU Fundamental Right to Data Protection Little Shop of Horrors?' [2016] 23(5) Maastricht journal of European and comparative law 812-841.

Mark Phillips, 'International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)' [2018] 137(8) Human genetics 575-582.

Paul B. Lambert, Essential Introduction to Understanding European Data Protection Rules Lambert, Paul B (1st edn, CRC Press 2018).

Paul M Schwartz, 'Privacy and participation: personal information and public sector regulation in the United States' [1995] 80(3) Iowa law review 553-618.

Priscilla M Regan, Legislating Privacy : Technology, Social Values, and Public Policy (Chapel Hill : : The University of North Carolina Press 1995).

Sanjay Sharma, Data Privacy and GDPR Handbook (Newark: John Wiley & Sons, Incorporated 2019).

Sergio Carrera and Elspeth Guild, 'The End of Safe Harbor: What Future for EU-US Data Transfers?' [2015] 22(5) Maastricht journal of European and comparative law 651-655.

Shara Monteleone and Laura Puccio, From safe harbour to privacy shield: advances and shortcomings of the new EU-US data transfer rules : in-depth analysis (Brussels: European Parliament 2017).

Terence Craig and MaryE Ludloff, Privacy and Big Data: The Players, Regulators, and Stakeholders (O'Reilly Media, Inc 2011).

Xavier Tracol, '"Invalidator" strikes back: The harbour has never been safe' [2016] 32(2) The computer law and security report 345-362.

Virgílio Emanuel Lobato Cervantes, 'The Schrems II judgment of the Court of Justice invalidates the EU – US privacy shield and requires 'case by case' assessment on the application of Standard Contractual Clauses (SCCS)' [2020] 6(4) European data protection law review 602-606.

William J Long and Marc Pang Quek, 'Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise' [2002] 9(3) Journal of European public policy 325-344.

Xavier Tracol, '"Schrems II": The return of the Privacy Shield' [2020] 39(11) The computer law and security report 1-11.

9.2. WEBSITES

Andrea Jelinek, 'Statement 01/2022 on the announcement of an agreement in principle on a new Trans-Atlantic Data Privacy Framework' (*European Data Protection Board*, 6 April 2022) <https://edpb.europa.eu/system/files/2022-04/edpb_statement_202201_new_trans-atlantic_data_privacy_framework_en.pdf> accessed 10 May 2022.

Bruce Schneier, 'The Eternal Value of Privacy' (Wired, 18 May 2006) <https://www.wired.com/2006/05/the-eternal-value-of-privacy/> accessed 30 April 2022.

Court of Justice of the European Union, 'Opinion of Advocate General Saugmandsgaard Øe ' (Court of Justice, 19 December) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CC0311&from=en> accessed 4 May 2022.

Court of Justice of the European Union, 'The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid ' (CJEU, 6 October) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf> accessed 16 May 2022.

Court of Justice of the European Union, 'The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield ' (Court of Justice, 16 July) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf> accessed 3 May 2022.

EU Network of Independent Experts on Fundamental Rights, 'Commentary of the Charter of Funcamental Rights of the European Union' (EU Network of Independent Experts on Fundamental Rights, June) <https://sites.uclouvain.be/cridho/documents/Download.Rep/NetworkCommentaryFinal.pdf> accessed 28 April 2022.

European Commission, 'Adequacy decisions' (European Commission) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> accessed 15 May 2022.

European Commission, 'Article 29 Data Protection Working Party - Opinion 01/2016 on the EU – US Privacy Shield draft adequacy decision' (European Commission, 13 April) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf> accessed 6 May 2022.

European Commission, 'Commission Staff Working Document: The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce' (European Commission, 20 October) <https://ec.europa.eu/transparency/documents-register/detail?ref=SEC(2004)1323&lang=en> accessed 16 May 2022.

European Commission, 'Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU' (European Commission, 27 November)

<https://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com(2013)0847_en.pdf> accessed 15 May 2022.

European Commission, 'Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)' (Europe-an Commission, 6 November) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0566&rid=3> accessed 11 May 2022.

European Commission, 'EU-US Privacy Shield: Frequently Asked Questions' (European Commission, 12 July 2016) < https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_2462> accessed 16 May 2022.

European Commission, 'European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework' (*European Commission*, 25 March 2022) <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087> accessed 8 May 2022.

European Commission, 'Standard Contractual Clauses (SCCs)' (European Commission, 2021) <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en> accessed 15 May 2022.

European Commission, 'Trans-Atlantic Data Privacy Framework' (*European Commission*, 25 March 2022) <https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100> accessed 8 May 2022.

European Commission, 'Working Party on the Protection of Individuals with regard to the Processing of Per-sonal Data' (European Commission, 24 July) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf> accessed 9 May 2022.

European Data Protection Board, 'Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data' (European Data Protection Board, 18 June 2021) <https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf> accessed 5 May 2022.

Ewen Macaskill and Gabriel Dance, 'NSA Files: Decoded' (The Guardian, 1 November 2013) <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1> accessed 16 May 2022.

Findlaw's team of legal writers and editors, 'What Is the "Reasonable Expectation of Privacy"?' (FindLaw, 2017) <https://www.findlaw.com/injury/torts-and-personal-injuries/what-is-the--reasonable-expectation-of-privacy--.html> accessed 4 May 2022.

Informacijski Pooblaščenec, 'Smernice glede prenosa osebnih podatkov v tretje države in mednarodne organizacije' (Informacijski Pooblaščenec Republike Slovenije, 2021)

<https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_glede_prenosa_OP_v_tretje_drzave_in_mednarodne_organizacije_po_Splosni_uredbi.pdf> accessed 13 May 2022, p. 14-15.

Julia Fioretti and Foo Yun Chen, 'New European, US data transfer pact agreed' (Reuters, 2 February 2016) <https://www.reuters.com/article/us-eu-dataprotection-usa-accord/new-european-u-s-data-transfer-pact-agreed-idUSKCN0VB1RN> accessed 17 May 2022.

Law Library - American Law and Legal Information, 'National Association for the Advancement of Colored People v Patterson' (Law Library - American Law and Legal Information) <https://law.jrank.org/pages/22818/National-Association-Advancement-Colored-People-v-Alabama-Significance.html> accessed 30 April 2022.

noyb, '"Privacy Shield 20"? - First Reaction by Max Schrems' (*Noyb*, 25 March 2022) <https://noyb.eu/en/privacy-shield-20-first-reaction-max-schrems> accessed 10 May 2022.

Oyez, Griswold v. Connecticut' (Oyez) < https://www.oyez.org/cases/1964/496> accessed 30 April 2022.

Oyez, 'National Association for the Advancement of Colored People v Patterson' (Oyez) <https://www.oyez.org/cases/1957/91> accessed 30 April 2022.

Samuel Gibbs, 'What is 'safe harbour' and why did the EUCJ just declare it invalid?' (The Guardian, 6 October 2015) <https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection> accessed 15 May 2022.

The White House, 'FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework' (*The White House*, 25 March 2022) <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/> accessed 8 May 2022.

9.3. LEGAL TEXTS

5 U.S.C. § 552a.

15 U.S.C. § 1681.

15 U.S.C. § 6501.

15 U.S.C. § 6801.

18 U.S.C. § 2510.

18 U.S.C. § 2721.

20 U.S.C. § 1232g.

47 U.S.C. § 227.

47 U.S.C. § 551.

2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance) [2000] OJ 2 215/1.

Charter of Fundamental Rights of the European Union (CFREU) [2012] OJ C 326/391.

Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union [2016] OJ C202/1 (TFEU).

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).

Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) (Text with EEA relevance) [2010] OJ 2 39/1.

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance) [2016] OJ 2 201/1.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ 2 281/31.

Pub. L. No. 104-191, 110 Stat. 1936 (1996).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 2 119/1.

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007 [2007] OJ 1 306/01

Treaty of Nice amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts [2001] OJ 1 80/01.

Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR).

9.4. CASES

Bensaid v the United Kingdom App no 44599/98 (ECtHR, 6 February 2001).

Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (July 20, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62018CJ0311&qid=1653197642544&from=EN.

Case C-362/14, Maximillian Schrems v Data Protection Commissioner joined party Digital Rights Ireland Ltd (October 6, 2015), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=en.

Griswold v Connecticut, 381 US 479 [1965].

Leander v Sweden App no 9248/81 (ECtHR, 26 March 1987).

NAACP v Alabama, 357 US 449, 462 [1958].

Niemietz v Germany App no 13710/88 (ECtHR, 16 December 1992).

United States v White, 401 US 745, 752 [1971].