UiO : Faculty of Law
University of Oslo

Transfer of Personal Data to Third Countries in a Post-Schrems II World

Candidate number: 8019

Submission deadline: 28.02.2021

Number of words: 17767

Table of contents

1 INTRODUCTION 1

1.1 Background 1
1.2 Aim of Study and Research Question 2
1.3 Clarification of Terms and Definitions 2
1.3.1 Controller and Processor 2
1.3.2 Data Exporter and Data Importer 3
1.3.3 Third Country 3
1.3.4 Transfer 3
1.3.5 Electronic Communications Service Provider 4
1.4 Delimitation, Methodology and Structure of the Thesis 4

2 PRIVACY AND DATA PROTECTION AS A FUNDAMENTAL RIGHT 6

3 GDPR ON THE TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES 7

3.1 The General Rule for Transfer 7
3.2 Transfer Tools 7
3.2.1 Adequacy Decisions 7
3.2.2 Appropriate Safeguards 9

4 PREVIOUS CASES ON TRANSFER OF DATA TO THIRD COUNTRIES 11

4.1 The EU-US PNR Dispute 12
4.2 ECJ Opinion on EU-Canada PNR Agreement 13

5 SCHREMS I 14

6 US LEGISLATION 15

7 THE EU-US PRIVACY SHIELD 17

7.1 Content 17
7.2 Criticism 19

8 SCHREMS II 19

8.1 Background and Outcome 19
8.2 The Invalidation of the EU-US Privacy Shield 22
8.2.1 US authorities' Access to Personal Data 22
8.2.2 Compliance with Article 52 of the CFREU 23
8.2.3 Effective Judicial Protection 25

8.3 Validation of SCCs 27
8.3.1 The Court's Decision 27
8.3.2 Requirements for the SCCs to Ensure an Adequate Level of Data Protection 29
8.3.3 Case-by-Case Assessment of the SCCs 30
8.3.4 Transfer of Personal Data to US with SCCs 31

9 EDPB RECOMMENDATIONS 32

9.1 The Step-by-Step Guidance 33
9.1.1 The First Step and Second Step 33
9.1.2 The Third Step 34
9.1.3 The Fourth Step 41
9.1.4 The Fifth Step and Sixth Step 52
9.2 Remarks on the EDPB Recommendations 53
9.2.1 The EDPB Ignores the Risk-Based Approach 53
9.2.2 Data Localization 55

10 THE FUTURE OF PERSONAL DATA TRANSFERS TO THIRD COUNTRIES 56

TABLE OF REFERENCE 58

List of Abbreviations

AG	**Advocate General**
BCRs	**Binding Corporate Rules**
CBP	**US Bureau of Customs and Border Protection**
CFREU	**Charter of Fundamental Rights of the European Union**
CSP	**Cloud Service Provider**
DNI	**Director of National Intelligence**
DoC	**US Department of Commerce**
DPA	**European National Data Protection Authority**
DPC	**Data Protection Commission**
DPD	**Data Protection Directive**
EC	**European Commotion**
ECJ	**European Court of Justice**
ECHR	**European Convention of Human Rights**
ECtHR	**European Court of Human Rights**
ECSP	**Electronic Communications Service Provider**
EDPB	**European Data Protection Board**
EDPS	**European Data Protection Supervisor**
EEA	**European Economic Area**
EEG	**European Essential Guarantees**
E.O	**Executive Order**
EP	**European Parliament**
EU	**European Union**
FISA	**Foreign Intelligence Surveillance Act**

FISC	**Foreign Intelligence Surveillance Court**
GDPR	**General Data Protection Regulation**
HR	**Human Resources**
IC	**Intelligence Community**
NSA	**National Security Agency**
PNR	**Passenger Name Record**
PPD-28	**Presidential Privacy Directive 28**
PS	**Privacy Shield**
SA	**Supervisory Authorities**
SCA	**Stored Communications Act**
SCCs	**Standard Contractual Clauses**
SMEs	**Small and Medium-sized Enterprises**
SH	**Safe Harbor**
US	**United States of America**

1 Introduction

1.1 Background

The rise of the internet and rapid technological development has significantly increased personal data volume across national borders. Certainly, a lot of the transferred data contains personal information; hence regulated by the General Data Protection Regulation (GDPR) as the GDPR seeks to protect individuals' personal data, which is any information that can, directly or indirectly, identify the natural person.[1]

The flow of cross-border data is vital for the exchange of information, which facilitates international trade and promotes the global economy. It is also essential for scientific cooperation, particularly during the COVID-19 pandemic, where sharing data is vital to fight the Coronavirus globally. Additionally, the exchange of information is essential for the global freedom of speech.

Thus, sharing and collecting personal data is important to private companies and public authorities, i.e., for ensuring crucial functions of the company or authorities function adequately, e.g., technical support from a third country.

Additionally, sharing and collecting personal data is vital for natural persons as the data contains information about the individual's private life. Misuse of such information could affect the individual to a great extent, e.g., by identity theft. Therefore, it is vital to ensure the data is not misused. Hence, when transferring personal data, it is important to safeguard the fundamental rights to private life and respect for personal data. Due to the amount of data transferred daily, the rush of new technology which challenges the legal framework, and the differences in data protection in the third countries, it is challenging to protect personal data.

The balance between the free flow of data and the right to privacy is the basis for the provisions on the transfer of personal data to third countries under the GDPR. However, in practice, the balance is not easy, which is highlighted by the *Schrems I* and *Schrems II* judgments.

[1] Articles 1 (1) and 4 (1) GDPR

In July 2020, the European Court of Justice Union (ECJ) invalidated the EU-US Privacy Shield (PS), known as the *Schrems II* judgment, and upheld the validity of SCCs as a transfer tool. The judgment had effect on the transfer of personal data to the US, in addition to transfer to other third countries. Thus, the judgment had great impact on the transfer of personal data from the EEA to third countries worldwide.

1.2 Aim of Study and Research Question

The aim of the thesis is to show how the *Schrems II* judgment affects the transfer of personal data from EEA countries to third countries by analyzing and discussing the requirements prescribed by the *Schrems II* and the subsequent recommendations by the European Data Protection Board (EDPB).

The overarching question examined in this thesis is: *What does the Schrems II judgment mean for transfers of personal data from EEA countries to third countries?*

As *Schrems II* addresses general issues regarding the transfer of personal data to third countries and also specific issues related to the transfer of data to the US, this thesis will also seek to answer:

> Sub-question 1: *How to legally transfer personal data to third countries after the Schrems II judgment?*
>
> Sub-question 2: *Is it practicable to transfer personal data to the United States after the Schrems II judgment?*

1.3 Clarification of Terms and Definitions

1.3.1 Controller and Processor

The "*natural or legal person, public authority, agency or other body*" which "*determines the purposes and means of the processing of personal data*" "*alone or jointly with others*" is defined as "**controller**" per Article 4 no. 7 of the GDPR.

The controller can engage "*natural or legal person, public authority, agency or other body"* ("**processor**"), to process "*personal data on behalf of the controller*" per Article 4 no. 8 of the GDPR.

1.3.2 Data Exporter and Data Importer

The terms "data exporter" and "data importer" are not defined in the GDPR. However, the terms are used in the context of cross-border transfer of personal data.

If controllers or processors located within the EEA transfers personal data to controllers or processors located in a third country, the term "**data exporter**" is used.

Hence, the term "**data importer**" is used when controllers or processors in a third country receive or obtain access to personal data transferred from controllers or processors in the EEA.

1.3.3 Third Country

The term "third country" means any country that is not an EU member state.[2] As the three European Economic Area (EEA) countries, Iceland, Norway and Lichtenstein, have incorporated the GDPR into Annex XI of the EEA agreement, the EEA countries equate with the EU.

1.3.4 Transfer

The content matter of the term "transfer" is essential as it determines when the provisions in Chapter V if the GDPR applies.[3] Neither the GDPR nor the Data Protection Directive (DPD)[4] defines the term "transfer".

The European Data Protection Supervisor (EDPS) states that the natural meaning of "transfer" is data moved between different users.[5] However, "transfer" usually consists of several elements than just the movement of data. According to the EDPS, "transfer" also consists of the following elements:

---

[2] Recital 101 GDPR

[3] Bygrave et al, 2020, p. 762

[4] 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.

[5] EDPS, 2014, p. 6

> *"communication, disclosure or otherwise making available of personal data, conducted with the knowledge or intention of a sender subject to the Regulation that the recipient(s) will have access to it[6]."*

As such, the term "transfer" implies deliberate transfers and permitted access to personal data.[7] Such an operation performed on personal data is processing of data per the GDPR.[8]

As the natural interpretation of the wording dictates, the GDPR applies when data is moved. The GDPR also applies when a party located in a third country is given access to personal data, both physical- and remote access. This means, that if someone in a third country is given remote access to a server storing personal data located in an EEA country – this is considered a transfer of personal data, and the GDPR applies.

1.3.5 Electronic Communications Service Provider

The definition of electronic communications service provider (ECSP) is broad as it includes "telecommunications carrier", "provider of electronic communication service" which provides its subscribers access to electronic communication services such as email etc., and provider of a remote computing service" which provides computer facilities for the storage and processing of electronic communications.[9]

1.4 Delimitation, Methodology and Structure of the Thesis

First this thesis presents the normative basis for European data protection in *Chapter 2*. As *Schrems II* interpret the GDPR in light of the European Charter of Fundamental Rights (CFREU) it is essential to underscore the background and content of the right to privacy and data protection as a fundamental right. The CFREU is a legally binding instrument after the adoption of the Treaty of Lisbon in 2009, thus constitutes primary EU law. This means that the provision set out by the CFREU can examine the validity of secondary EU legislation such as the GDPR, which the ECJ did in the *Schrems II* judgment.

---

[6] EDPS, 2014, p. 6

[7] Ibid. Note that the quote excludes illegal and undue access to personal data, cf. "knowledge" and "intention".

[8] Article 4 (2) GDPR

[9] FISA Section 702 50 U.S.C § 1881 (b)

Further, in *Chapter 3* of the thesis, Chapter V of the GDPR is presented as it regulates transfer of personal data to third countries. In particular, Articles 45 and 46 if of importance for the thesis as *Schrems II* mainly assessed these provisions. The GDPR Recitals are used to support the assessment; however, they are not binding.

The thesis does not assess other requirements for processing of personal data, than Chapter V; however, some other provisions may be mentioned to underscore an argument. Moreover, the thesis only presents transfers from the EEA to third countries and does not include transfers within the EEA, transfers from third countries to the EEA, or transfers between third countries.

Then in *Chapters 4, 5* and *6* I will present the EU-US relations. Starting with presenting jurisprudence of the ECJ in *Chapter 4*. The cases presented are the 1/15 Opinion on the EU-Canada PNR agreement and joined Cases C-317/04 and C-318/04 on the 2004 EU-US PNR agreement. The first mentioned case is concerning EU-Canada relations and it is an ECJ Opinion. It is presented as it is directly related to the issue of EC adopting transfer agreement that does not offer an adequate data protection level. The Opinion is not binding, and it is considered soft law; however, it has legislative value as EEA member states must consider them. Moreover, *Schrems I* is presented in *Chapter 5*. Following *Chapter 6*, where US legislation assessed in *Schrems I* and *Schrems II* is presented.

In *Chapter 7* the *Schrems II* judgment is analyzed. I do not differ between *ratio decidendi* or *obiter dicta* as it is hard to distinguish the two a part. The invalidation of the PS is first assessed due to the flow of the text.

Moreover, due to the unclarity after the *Schrems II*, the EDPB Recommendations are presented in *Chapter 8*. The statements from the EDPB are not binding, and they are only drafts, but they constitute an authoritative view of the effects of *Schrems II* on SCCs.

Lasty, *Chapter 9*, I will shortly present the way forward for the transfer of personal data to third countries and give a brief opinion on what the future should bring.

2 Privacy and Data Protection as a Fundamental Right

The formal normative basis for European data protection is fundamental human rights. Privacy as a fundamental right is particularly enshrined in the European Convention on Human Rights (ECHR) Article 8 and the European Charter of Fundamental Rights (CFREU) Articles 7 and 8.

The ECHR Article 8 (1) expresses a general-purpose for the right to privacy by stating the right to "*respect private life, family life, home, correspondence*" and sets out terms for legal interference. The specific content and the reach of protection of this provision has been interpreted by the European Court of Human Rights (ECtHR) on several occasions, thus laid the basis for interpretating personal data within the right to private life.[10]

Like the ECHR Article 8, "*the right to respect for private life, family life, home, and correspondence*" is enshrined in Article 7 of the CFREU. The continuation of this human right in the CFREU reaffirms the right to privacy as a fundamental right in the EU. The purpose of the CFREU was precisely to affirm and enlighten enforceable fundamental rights for the EU. According to the preamble of the CFREU, the enshrined rights are based on rights set out by EU primary law, EU case-law, and Member States.[11]

The right to protection of personal data was first established as an individual fundamental right through Article 8 of the CFREU, which stipulates that everyone has the right to data protection.[12]

These rights, per the CFREU, were ratified by the Lisbon Treaty in 2009 and thus granted legally binding force in all EU member states.[13] This means that all EEA countries must ensure compliance with Article 7 and 8 of the CFREU, regardless of where the personal data is located.

[10] Fuster, 2014, p. 2
[11] Ibid.
[12] Fuster, 2014, p. 2
[13] Ibid., and Article 6 TEU

3 GDPR on the Transfer of Personal Data to Third Countries

3.1 The General Rule for Transfer

The general requirements for transferring personal data to third countries is set out in Article 44 of the GDPR. It is prohibited to transfer personal data to a third country unless the conditions in Chapter V and the general requirements of the GDPR are fulfilled, which applies to both controller and processor. The purpose of Chapter V is to ensure that the level of protection provided by the GDPR is not undermined when transferring personal data.[14]

Chapter V of the GDPR stipulates three legitimate bases for transferring personal data to third countries: adequacy decisions, appropriate safeguards, and derogations for specific situations. In Chapter 3.2 of this thesis, adequacy decisions and appropriate safeguards will be presented.

There are several derogations to the general rule on the prohibition of transferring data to third countries under Article 49, which are applicable when the conditions of Articles 45, 46 or 47 have not been met.[15] The derogations mentioned in Article 49, can be summarized as necessary transfer for specific situations. Some of these derogations are consent, necessary to fulfill a contract, and necessary for the sake of important public interests.[16] As these derogations are not relevant to the thesis, this legitimate transfer tool will not be considered further.

3.2 Transfer Tools

3.2.1 Adequacy Decisions

According to Article 45 (1) of the GDPR, transfer of personal data may only occur if the third country ensures an "*adequate*" data protection level. The European Commission (EC) has the power to determine which countries, outside the EU, that fulfill the requirement of adequacy.[17]

[14] Article 44 Sentence 3 GDPR

[15] Article 49 GDPR

[16] Ibid. The public interest must be recognized in EU law or in the law of the Member State of question, cf. Article 49 (5).

[17] Article 45 (1) GDPR

The precise meaning of the term "adequate" is neither defined in the provision nor the GDPR. However, recital 104 stipulates that "*an adequate level of protection essentially equivalent to that ensured within the Union*".[18] As such, the term is a measure of a third country's appropriateness of receiving personal data from controllers or processors located within the EEA. Such an understanding is consistent with the purpose of Article 45, i.e. to create uniformity and legal clarity in the EEA.[19] The effect of Article 45 is that personal data can be transferred to third countries without requiring additional safeguards.[20]

The term "adequate level of protection" and the interpretation thereof suggest that an assessment of whether the specific country meets the criteria for obtaining data adequacy status in the EEA must be made.

When determining whether a third country fulfills the requirement of adequacy, the EC shall consider whether the criteria as set out in Article 45 (2) of the GDPR have been met. The list of criteria is long and mainly concerns the specific characteristics of the third country in question.[21] As the EC shall make an overall assessment of the specific circumstances, not all the criteria have to be equally fulfilled.[22] Some of the elements listed are: respect for fundamental rights, independent Supervisory Authority (SA), and international commitments to protect personal data.[23]

The EC has a published list of third countries, territories, and specified sectors within a third country, which have been recognized by the EC for providing adequate protection of personal data. Today, there are 13 third countries on the list.[24] The EU-US PS Decision was previously on this list recognized within the scope of the decision. An elaboration of the PS is presented in Chapter 7.

[18] The background for this recital is the Schrems I judgment.
[19] Recital 103 GDPR
[20] Ibid.
[21] Skullerud et al., 2018, p. 259.
[22] Voigt et al, 2017, p. 117
[23] Article 45 (2) letter a-c GDPR
[24] See: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

3.2.2 Appropriate Safeguards

In the absence of an adequacy decision, controllers or processors under Article 46 (1) of the GDPR may transfer personal data to third countries if "*appropriate safeguards*" are provided. Additionally, the data subject must have enforceable rights and effective remedies when personal data is transferred.[25]

The term "appropriate safeguards" is not defined in the regulation, but recital 108 states that the safeguards must ensure compliance with data protection requirements and -principles and ensure compliance with data subject's rights per the regulation.

The purpose of Article 46 is to ensure sufficient protection of personal data during and after the data has been transferred to another jurisdiction to compensate for the weakened protection of personal data in the relevant recipient third country.[26]

Pursuant to Article 46 (2), such appropriate safeguards may be secured by the listed alternative transmissions in (2) (a-f). As these listed tailored types of transfer are not exclusive other safeguards ensuring additional protection can also be applied.[27] For the sake of delimitation of the thesis, only letter b, c, and d are further discussed.

3.2.2.1 Standard Contractual Clauses

The first relevant alternative is Standard Contractual Clauses (SCC) under Article 46 (2) (c and d).[28]

SCCs are standard sets of contractual terms and conditions that commits the signing data importer and data exporter to process personal data according to the GDPR.[29] This way, the signed SCC guarantees an adequate data protection level between the parties, and the data

[25] Article 46 (1) GDPR
[26] Skullerud et al., 2018, p. 263
[27] Bygrave et al, 2020, p. 802 and 803
[28] Article 46 letter c and d GDPR
[29] Skullerud et al, 2018, p. 265

subjects are granted third-party beneficiary rights.[30] SCCs are widely used and are an essential means of achieving secure data flow between countries.[31]

Following letter c, the SCCs must be adopted by the EC in accordance with Article 93 (2) to be considered a valid transfer tool.[32] Also, national SA can adopt SCCs per the letter d. However, the EC must approve these SCCs and be in accordance with Article 93 (2).[33]

After the *Schrems II* judgement, there are now further clarifications when SCCs are considered valid. Further elaborated in Chapter 8.

The EC has adopted three sets of SCCs pursuant to the DPD. These sets cover EU-based controllers to third country-based controllers and EU-based controllers to third country-based processors.[34] In practice, this has been deficient and not covered all cases. Thus, the EC has reviewed the SCCs and has recently published drafts of new SCCs after being on hold because of the *Schrems II* judgment, which questioned the validation of the SCCs adopted under the DPD. The drafts to the new SCCs, cover all four alternatives: the two original alternatives as well as EU-based processors to third country-based processors, and EU-based processors to third country-based controllers.

3.2.2.2 Binding Corporate Rules

According to letter b, binding corporate rules (BCRs) is another alternative transfer tool.[35]

"*Binding corporate rules*" is defined in Article 4 (20) as legally binding internal personal data protection policies for transfer of personal data from an EEA-based controller or processor to a third country-based controller or processor "*within a group of undertakings, or group of enterprises engaged in a joint economic activity*".[36] In practice, this means that a multination-

[30] Skullerud et al, 2018, p. 265 and Voigt et al, 2017, p. 119
[31] Voigt et al, 2017, p. 119
[32] Article 46 letter c GDPR
[33] Article 93 (2) refers to Article 5 of the Comitology Regulation.
Article 46 letter d GDPR and Voigt, 2017, p. 120
[34] Voigt et al, 2017, p. 120
[35] Article 46 letter b GDPR
[36] Article 4 (20) GDPR

al company, with entities both inside and outside the EEA, can transfer personal data within the company's entities with this transfer tool.

Article 47 (1) and (2) sets out cumulative minimum requirements to the content of BCRs. These must be fulfilled to be approved as a valid transfer tool by the competent national SA after the EDPB has stated their opinion.[37]

Firstly, the BCRs must have a binding effect internally in the concerned group, as they must be legally binding as well as applied to and be enforced by every member and employee of the applicable group.[38]

Secondly, the BCRs must have a binding effect externally by deriving enforceable data subject's rights.[39]

Thirdly, the BCRs must fulfill the listed minimum requirements set out under the provisions' second section letter a-n.[40] A review of these is not carried out due to the limitation of the thesis.

4 Previous Cases on Transfer of Data to Third Countries

In this chapter, the purpose is to shed light on thesis-relevant previous judgments concerning data transfer to third countries. The cases presented are the 1/15 Opinion on the EU-Canada PNR agreement and joined Cases C-317/04 and C-318/04 on the 2004 EU-US PNR agreement. The latter judgment portrays the need for an EU-US agreement on the transfer of personal data. Simultaneously, both judgments infer the difficulties of achieving adequacy decisions that sufficiently balance fundamental rights and national security. The hitherto adopted agreements indicate a willingness to find compromises that do not adequately safeguard fundamental rights. In the quest for a future solution between the US and EU, these rulings will be important.

[37] Article 47 (1) and Article 64 (1) letter f GDPR
[38] Article 47 (1) letter a GDPR
[39] Ibid. letter b
[40] Ibid. letter c

4.1 The EU-US PNR Dispute

The joined Cases C-317/04 and C-318/04 revolves around Passenger Name Records (PNR), which is travel records for individuals. A PNR contains information about the passenger's name, address, date of birth, and other similar information relevant to a flight journey.[41] Thus, of relevance in the context of protection of personal data.

In the aftermath of the terrorist attack of September 11, 2001, airlines landing on US soil were required to provide the US Bureau of Customs and Border Protection (CBP) with electronic access to data processed by their reservations and departure control systems, including PNR. The purpose of CBPs' information gathering was to prevent future terrorist attacks.[42]

According to EU data protection standards, the CBPs collection of this type of information was inconsistent with provisions set out in the DPD, in particular, the provisions on data limitation and transfer of data.[43] Therefore, airlines were stuck between conflicting legislations. An agreement between the EU and the US sought to resolve this.[44] The EC drafted two decisions; the adequacy decision and the Council decision.[45] These decisions constituted the 2004 EU-US PNR agreement.[46]

The European Parliament (EP) disagreed that the PNR agreement provided sufficient data protection and filed a case to the ECJ.[47] The Court held that both decisions should be annulled as the adequacy decision was based on US domestic law on public security and law enforcement activities, which according to the ECJ fell outside the scope of the DPD.[48] This was the beginning of adopting adequacy decision based on EU data protection standards.

[41] Suda, 2018, p. 55
[42] Ibid.
[43] The Principle of limitation, Article 6 and Article 25 of the DPD. Suda, 2018, p. 56
[44] Suda, 2018, p. 57
[45] Cases C-317/04 and C-318/04
[46] Suda, 2018, p. 57
[47] Ibid. p. 58
[48] Cases C-317/04 and C-318/04

4.2 ECJ Opinion on EU-Canada PNR Agreement

The EU signed a PNR agreement with Canada in 2006 which allowed the Canada Border Service Agency to obtain PNR data from airlines transporting passengers to Canada.[49] After the agreement expired, the EC negotiated a new PNR agreement with Canada, signed by the European Council and Canada in 2014.[50] For the agreement to be adopted, the Council needed consent from the EP. Before consenting to the agreement, the EP asked the ECJ for an opinion on the agreement's compliance with primary EU law, particular Article 218 (11) of the Treaty on the Function of the European Union (TFEU) and Articles 7, 8 and 52 (1) of the CFREU. This was the first time the compatibility of an agreement on cross-border transfer of data were assessed under the Treaties and CFREU.[51]

The ECJ issued Opinion 1/15, stating that the agreement was incompatible with the CFREU and must be revised before it is finally adopted.

Through the judgment's statements, the ECJ stipulated the importance of protecting privacy when transferring data to third countries. Inter alia, the ECJ stated that multiple provisions in the agreement interfered with privacy and data protection rights, after Articles 7 and 8 of the CFREU, as they were not proportional and limited to the strictly necessary per Article 52 of the CFREU.[52] Additionally, the ECJ emphasized the importance of the provision's precise specification of what categories of personal data can be processed and the importance of ensuring sufficient protection for categories of sensitive personal data.[53] In addition, the Court held that the air passengers' data must be fully respected and ensured by an independent authority and stated that the agreement does not ensure such independence.[54]

[49] Suda, 2018, p. 66
[50] EPRS, 2017, p. 1
[51] Ibid., p. 2
[52] Opinion 1/15, paragraph 181, 206 and 217
[53] Ibid., paragraph 141
[54] Ibid., paragraphs 228-231

5 Schrems I

This judgment is presented as it is the predecessor to the *Schrems II* and portrays the need for an EU-US agreement on the transfer of personal data. In addition to infer the difficulties of achieving adequacy decisions that sufficiently balance fundamental rights and national security.

In 2011 the Austrian law student Maximillian Schrems requested access to his personal data from the social network Facebook.[55] When creating a Facebook user, Mr. Schrems entered a private agreement with Facebook Ireland.[56] It turned out that the Irish subsidiary collected and transferred Mr. Schrems data to Facebook Inc., the parent company, based in the US.[57] At the time, data transfer between the EEA and the US was based on the Safe Harbor (SH) Decision.[58] According to the EC, the SH principles ensured adequate data protection per European standards of data protection.[59]

Following the Snowden revelations, where mass surveillance operations in the US were exposed, Mr. Schrems started investigating if Facebook users within the EEA were subject to surveillance.[60] It turned out that the National Security Agency (NSA) and ECSPs, such as Facebook, had a surveillance partnership, which enabled the government to access personal data about, among others, Facebook users.[61]

Mr. Schrems believed that his data would not be adequately protected upon transfer to the US based on the SH Agreement. Thus, Mr. Schrems complained to the Irish Data Protection Commissioner (DPC) to prevent Facebook from transferring his personal data to the US.[62] The Irish DPC rejected the complaint, stating that the SH Agreement, according to the EC, ensured an adequate level of protection under European standards of data protection; thus, the

[55] Schrems I, paragraph 26
[56] Ibid, paragraph 27
[57] Ibid.
[58] Decision 2000/520/EC
[59] Fahey, 2018, p. 79
[60] Ibid.
[61] Ibid.
[62] Schrems I, paragraph 28

EC had no competence to take a position on the matter.[63] Mr. Schrems filed a judicial review, and then the Irish High Court referred questions to the ECJ.[64]

The ECJ provides several statements of interest in the pronunciation of the judgment. Firstly, the Court states that the term "*adequate [level of] protection*" means "*essentially equivalent*" to European data protection standards.[65] Meaning that the data protection level in the concerning third country does not need to be identical to the European standard of data protection, but the third country in question must have "*effective detention and supervision mechanisms*". [66]

As the ECJ found that mass surveillance was conducted in the US, the Court concluded that this ran contrary to the essence in Articles 7, 8, and 47 of the CFREU, thus violated Mr. Schrems fundamental rights.[67] The Court ruled the SH Decision invalid because it failed to ensure a level of data protection essential equivalent to the level guaranteed within the EEA.[68]

Additionally, the ECJ stipulated that even if adequacy decisions are adopted by the EC, it did not limit or eliminate the national SA powers to ensure compliance with EU legislation.[69] However, solely the ECJ can declare such a decision invalid.

6 US Legislation

The Foreign Intelligence Surveillance Act (FISA) of 1978 is an American federal law providing a statutory framework for, inter alia, electronic surveillance in foreign intelligence collection.[70] To protect national security and public safety, FISA Section 702 authorizes the National Security Agency (NSA), Central Intelligence Agency, and Federal Bureau of Investigation to collect intelligence of non-US persons to obtain foreign intelligence.[71] Section 702 applies to ECSPs and permits surveillance of any non-US persons communicating specified

[63] Schrems I, paragraph 29

[64] Fahey, 2018, p. 81 and Schrems I, paragraph 36

[65] Schrems I, paragraph 73

[66] Schrems I, paragraph 74 and 81, Fahey, 2018, p. 82.

[67] Fahey, 2018, p. 82

[68] Schrems I, paragraph 107

[69] Ibid.

[70] Bazan, 2004, p. Summary. In addition to electronic surveillance, FISA also regulates physical searches, pen register and trap and trace surveillance.

[71] Adams, 2019, p. 402

kinds of foreign intelligence information and facilitate authorization of sizable surveillance programs.[72]

An Executive Order (E.O) is a federal directive issued by the President that manages the federal government's operations. According to E.O 12333, the US intelligence authorities is permitted to "*collect, retain, or disseminate information*", outside the US, in the purpose of providing accurate and insightful information about, inter alia, foreign intelligence.[73]

FISA Section 702 and E.O 12333 provides US authorities access to personal data through surveillance programs.[74] Two such authorized surveillance programs, collecting multiple electronic communications types is PRISM and UPSTREAM.[75] These surveillance programs lay out how the US conducts monitoring; "in transit" surveillance and data "at rest" surveillance. The wording "data in transit" means data actively moving from one location to another. Opposite, "data at rest" means not moving data, e.g., data stored on data servers.

The PRISM surveillance program facilitates "data at rest" surveillance as the program obtains electronic communication after transit to the US from ECSPs.[76] Electronic surveillance in foreign intelligence collection after Section 702 is primarily conducted by PRISM.[77] Section 702 only applies to specific data processors, precisely solely ECSPs.[78] The collection and surveillance of electronic communication are a collaboration between US-based ECSPs and the IC.[79] According to Section 702, the Advocate General (AG) and the Director of National Intelligence (DNI) may demand communication disclosed if foreign persons located abroad are reasonably believed to communicate specified kind of foreign intelligence information.[80]

The UPSTREAM surveillance program is authorized under the E.O 12333 and Section 702 and collects "data in transit". Meaning, when data goes through international network cables,

[72] Adams, 2019, p. 410
[73] Executive Order 12333 Section 2.3 and Johnson, 2015, p. 233
[74] Johnson, 2015, p. 233
[75] Adams, 2019, p. 410 and Schrems II, paragraphs 109 and 165
[76] Adams, 2019, p. 416 and 417
[77] Ibid.
[78] Ibid., p. 402
[79] Ibid., p. 416
[80] Ibid., p. 412

switches, and routers from the EU to the US, data is scanned and checked for identifiers to filter out relevant information on a target.[81] An identifier can typically be a telephone number or e-mail address, etc. but never an individual's name or keywords like "bomb".[82]

The Presidential Policy Directive 28 (PPD-28) seek to limit the reach of FISA Section 702 and E.O 12333.[83] President Obama issued this binding force for the U.S intelligence authorities in 2014 in response to political pressure due to the international reaction to the Snowden-revelation.[84] The limitations in PPD-28 set out as a series of principles and requirements and stipulate that non-US persons shall have privacy rights.[85] Thus, the US intelligence authorities must implement appropriate safeguards to ensure that all persons are treated with dignity and respect.[86] However, the PPD-28 does not limit bulk collection of data.[87]

7 The EU-US Privacy Shield

7.1 Content

As a replacement for the SH Agreement, the EC adopted the PS framework in accordance with the DPD, which came into operation on 1. August 2016.[88] The PS sought to provide an adequate level of protection for persons located in the EU who had their data transferred to the US under the PS framework.[89]

The preamble of the framework, six articles, and seven attachments constitutes the PS, which mainly passes on the SH framework; thus, there are several similarities and some upgrades from the SH to the PS.

Like the predecessor SH, the PS allows personal data transfer from the EEA to certified PS US companies. An US based company is certified when voluntarily joining the PS by declar-

[81] Executive Order 12333, paragraph 62 and Privacy Shield Decision, paragraph 81
[82] Privacy Shield Decision, paragraph 81
[83] Schrems II, paragraph 45
[84] Johnson, 2016, p. 242
[85] Suda, 2018, p. 50 and PPD-28, Section 4 paragraph 1
[86] PPD-28, Section 4 paragraph 1
[87] Johnsen, 2016, p. 253
[88] Voigt, 2017, p. 122
[89] The Privacy Shield Article 1 (1).

ing its commitment to adhere to the PS Principles.[90] The US Department of Commerce (DoC) has a publicly available list with an overview of the companies that can verify compliance with the self-certification requirements set out in Annex I.[91]

The framework sets out seven principles with extensive obligations for EEA data subjects' rights, US PS certified companies, and the US government.

The principles ensure data subjects within the EEA several individual rights, including more information about the processing of personal data, inter alia, types of data and purpose of the data, the right to access, alteration and erasure of personal data, the opportunity to opt-out of processing where there is a change in processing purpose, and the right to file a claim when the PS is not complied with.[92]

Additionally, the principles ensure stricter requirements for US businesses as they need to provide redress, report privacy records upon request, and be compliant with the PS framework.[93]

Per these principles, the US government's obligations entail the US authorized statutory bodies' involvement in the enforcement processes undertaken by the DoC, the Federal Trade Commission, and the Department of Transportation, and follow up US companies.[94] Moreover, one of the essential purposes the principles set out is to limit access to personal data for US authorities.[95] Throughout the PS, it is stated that there is no mass surveillance by the US government nor indiscriminating surveillance, and the framework ensures that collection of personal data of non-US persons is limited through safeguards and an oversight mechanism.[96] This assessment and conclusion is based on US legislations FISA Section 702, E.O 12333 and PPD-28, and is also subject to discussion in the *Schrems II* judgment; thus of relevance for the thesis to further present.

---

[90] The Privacy Shield Article 1 (3) and Annex II Section II
[91] Ibid., Article 1 (3) and Annex I
[92] Ibid., Annex II Section II
[93] The Privacy Shield Annex II Section II
[94] Ibid.
[95] Ibid.
[96] Ibid., Annex VI Section VI

7.2 Criticism

The PS framework has received criticism on multiple aspects.[97] Inter alia, the redress mechanisms are composite and indistinct as the redress mechanisms' overall setup undermines the data subject's rights.[98] Additionally, the ambiguity on limitation and access of personal data for the US government, which does not clarify to what extent the US authorities have access to personal information, nor does it appear how access to such information is restricted to the US authorities through the PS.[99]

Another aspect that has received criticism is that some principles are not being adequately fulfilled; thus, the data subjects' rights, by GDPR, are being undermined in the PS. This applies to the principles of access, where the individual does not have the right to correct or erase data under the PS unless the relevant data has been used in a way that violates the PS principles.[100] It also applies to the principle of storage limitation set out in the GDPR, which is not mentioned as one of the principles in the PS; thus, the processor or controller can keep the data as long as they need it, and the data subject does not have the right to have their data deleted when it is unnecessary to keep the data according to the original collecting purpose.[101]

8 Schrems II

8.1 Background and Outcome

After the ECJ declared the SH Decision invalid, Mr. Schrems reformulated his complaint to the Irish DPC as he became aware that Facebook most often used SCCs as a transfer tool when transferring personal data from Facebook Ireland to Facebook Inc. located in the US.[102] Thus, in the renewed complaint Mr. Schrems claims that Facebook's use of SCCs to transfer data on EEA-based data subjects to the US does not adequately protect these EEA-based data subjects' personal data.[103] As Mr. Schrems argued that transferred data is

[97] E.g. WP29
[98] Sharma, 2019, chapter 5.3.4 and WP29 Opinion 01/2016, p. 26
[99] WP29 Opinion 01/2016, p. 17
[100] Ibid., p. 25
[101] Ibid., p. 24
[102] Schrems II, paragraph 54
[103] Ibid., paragraph 55

subject to access by US authorities due to the US legislations FISA Section 702 and E.O 12333, the transfer of data by Facebook is incompatible with Articles 7, 8, and 47 of the CFREU: hence the claim that the SCCs does not offer an adequate protection of personal data. Therefore, Mr. Schrems requests the Irish DPC to prohibit or suspend transfer of personal data from Facebook Ireland to Facebook Inc. based on the SCCs.

The Irish DPC referred the case to the Irish High Court requesting a preliminary reference to the ECJ as, in accordance with *Schrems I*, the validity of the SCCs decisions could only be determined by the ECJ.[104] Hence, requesting a decision on 11 questions was referred to the ECJ.[105]

The questions seek clarification on general issues regarding the transfer of personal data to third countries and specific issues related to the transfer of data to the US. Nevertheless, the Court's interpretations and statements on these issues will be relevant for other third countries and other transfer tools, such as BCRs, to ensure a consistent and high level of data protection of the data subjects.

As to the outcome of the judgment, the ECJ concluded that the SCCs is a valid transfer tool and emphasized that the level of protection in the third country must be essential equivalent to the level of protection under EU law, and this level can be, where necessary, provided for by additional measures.[106]

Moreover, the Court invalidated the EU-US PS framework, as US authorities' access to personal data exceeds what is strictly necessary and violates the fundamental rights to privacy and data protection under the CFREU.

This means that no transfers to the US can be based on the PS framework. Additionally, the assessment must be taken into account for any transfer to the US. Meaning that it is not longer valid to transfer personal data on another transfer tool, such as SCCs or BCRs, without ensur-

[104] Schrems I, paragraph 62
[105] Schrems II, paragraph 57 and 68
[106] Ibid., paragraph 134 and 149

ing an adequate level of protection. Thus, it is still a practicable limited possibility to transfer personal data to the US.

Further presented is shortly the first and eight question in the judgment. Then the invalidity of the EU-US PS is presented and analyzed before the validity of SCCs is presented and analyzed.

Under the first question in the judgment, the Court states that transfers of data to a third country by an economic operator for commercial purposes, is regulated under the GDPR, even if the transferred data is accessed by the third country's public authorities for national security reasons.

Under the eight question the Court affirms that national SA role also includes checking compliance with the GDPR requirements and monitoring European legislation compliance.[107] Regarding compliance, national SAs' are required to prohibit and suspend, as appropriate, the transfer of personal data when transferred with SCCs, when the level of protection in the third country does not offer an adequate level of protection.[108] As regards an adequacy decision, a valid adequacy decision is binding until such time as it may be declared invalid; this does not stop individuals from being able to complain to the national SA's about their data protection rights.[109]

In late 2020, the Irish DPC required, through a draft preliminary decision, requiring Facebook to suspends data transfers to the US due to the absence of a guaranteed level of protection to data subjects equivalent to those provided for in EU law. However, Facebook has filed a judicial review against the Irish DPC challenging this preliminary order. The decision ruling if the Irish DPC must review the preliminary decision or not, is exciting as it says something about how SA can exercise the compliance role in practice.[110]

[107] Schrems II, paragraph 108 and 112
[108] Ibid., paragraph 113
[109] Ibid., paragraph 119 and 120
[110] Noyb, 2021

8.2 The Invalidation of the EU-US Privacy Shield

As formerly stated, the PS Decision allows transfers of personal data from the EEA to the US, in accordance with an adopted adequacy decision per Article 45 of the GDPR.[111] When the ECJ assessed the PS, the Court emphasized that the GDPR must be interpreted in the light of the CFREU, including the right to private life, to data protection, and to an effective remedy.[112]

The underlying before the Court issue was whether the US authorities' access to personal data through surveillance programs violated the fundamental right to privacy and data protection under the CFREU.

The Court examined whether the PS was incompatible with US legislation, in particular FISA Section 702, E.O 12333 and PPD-28. These facilitate the US authorities' access and use of personal data and are not limited in a way that is essentially equivalent to EU law. Additionally, the data subjects were not offered an effective judicial oversight.

8.2.1 US authorities' Access to Personal Data

In assessing the PS, the ECJ did not assess the specific surveillance programs but affirmed on a general basis that retention, access, and communication of personal data to a third party constitutes an interference with the fundamental rights per Articles 7 and 8 of the CFREU, regardless of the data's character and to whom such access and communication are given.[113] This is indicating a low threshold for interference with the fundamental rights.

The ECJ did not take a direct position on the issue if surveillance programs violate fundamental rights, which differs from the *Schrems I* judgment where the criticism of surveillance is more distinct:

> "[L]*egislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the*

[111] See Chapter 7

[112] Schrems II, paragraph 99

[113] Ibid., paragraph 171

essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter[114]."

Why the Court did not uphold this position on surveillance programs is unclear. However, this should not be taken to mean that the Court has eased up on surveillance and its interference with fundamental rights. Retention, access, and communication of personal data are essential features of a surveillance process. It may seem like the Court worded itself differently in order to account for all forms of monitoring, regardless of whether the surveillance has is basis in legislation or not.

Moreover, in *Schrems II*, Article 8 has been included in addition to the original Article 7. This addition of Article 8 is probably included due to the criticism of not including the provision in *Schrems I*. [115]

As US authorities access personal data through surveillance programs, this entails an interference with the right to privacy and data protection.

8.2.2 Compliance with Article 52 of the CFREU

Like the *Schrems I* judgment, the ECJ held that the surveillance programs must be limited to what is strictly necessary.[116] Articles 7 and 8 of the CFREU are not absolute rights, and may be restricted, provided that exemptions are compliant with Article 52 of the CFREU.

According to Article 52 (1), limitations of fundamental rights must be "*provided by law*", and the limits cannot restrict the "*essence*" of the fundamental rights. Additionally, limitations must be in accordance with the "*principle of proportionality*".[117] All these conditions must be fulfilled to be compliant with the provision. In the judgement, the Court sought to clarify the content of the requirements.

[114] Schrems I, paragraph 94
[115] Kuner, 2016 p. 892
[116] Schrems II, paragraph 176
[117] Article 52 Section 1 of the CFREU

Firstly, the "essence" of the fundamental right must not be exceeded beyond the limitation of those rights.[118] The ECJ held that providing general access to the content of electronic communications is contrary to the essence of Art. 7 and 8 of the CFREU.[119] Thus, the Court reiterated the position under the Schrems I case.[120]

However, this statement differs from the subsequent *Tele2 Sverige/Watson* judgment's statement, where the ECJ emphasized that the essence of the right to privacy is not affected when national legislation allows public authorities' general access to traffic and location data.[121] In other words, the Court made a distinction between general access to the content of communication and general access to metadata.[122] A further comparison of the two cases is not made beyond mentioning that it has been questioned whether such a distinction is valid.[123]

A further requirement is "provided by law" which requires that the law that permits the interference of the fundamental rights must itself define the extent of this interference.[124] The ECJ stipulated that FISA Section 702, E.O 12333 and PPD-28 did not to contain any restrictions that justify interference with Articles 7 or 8 of the CFREU.[125] Thus, the ECJ did not take a directly position on whether national security can justify the encroachment on fundamental rights.

Article 23 of the GDPR, case law, and Article 6 of the CFREU indicates that limitation on fundamental rights is legitimate when national security is the restriction.[126] The right to security is also vital as a fundamental right and must be balanced with the right to private life, as they are closely linked.

---

[118] Article 52 Section 1 2. sentence of the CFREU

[119] Schrems II, paragraph 171

[120] Schrems I, paragraph 94

[121] Joined Cases C-203/15 and C-698/15, 2016

[122] Opinion on C-311/18 of Advocate General Saugmandsgaard Øe, 2019, footnote 149

[123] Ibid.

[124] Schrems II, paragraph 175

[125] Ibid., paragraph 184

[126] Article 23 GDPR states that some rights under the GDPR can be limited to the consideration for national security etc. if particular demands are fulfilled.
Article 6 CFREU states the right to security
Case law: Schrems I, paragraph 88

One can assume that the ECJ did not assess whether national security could be justified as a limitation of fundamental rights because the US legislation facilitating the surveillance programs did not meet the other requirements under Article 52 of the CFREU.

Lastly, a proportionality assessment must be fulfilled. The ECJ emphasized that only "strictly necessary" restrictions can limit fundamental rights.[127]

According to the ECJ, the requirement of "strictly necessary" are met when the law in question has "*clear and precise rules*" on how conditions and circumstances infringement of fundamental rights occur.[128] It must be explicitly stated through the legal basis that the interference is limited to what is strictly necessary.[129] Such an approach to the proportionality assessment has also been made in previous case-law.[130]

That the Court concluded that the principle of proportionality was not fulfilled is not surprising since such a statement upholds the *Schrems I* judgment and continues the development of a stricter principle of proportionality.

8.2.3 Effective Judicial Protection

The GDPR emphasizes the importance of effective judicial protection in Article 45 (2) (a), which requires the EC to take into account "*effective and enforceable data subjects rights and effective administrative and judicial redress*" in the assessment of whether a third country ensures an "adequate" level of data protection. According to recital 104 this includes ensuring an "*effective independent data protection supervision*".

This provision must be read in light of Article 47 of the CFREU and the EC must ensure compliance with this provision before adopting the adequacy decision.[131] This provision stipulates the right to an "*effective remedy*" before an "*independent and impartial tribunal*" if fundamental rights guaranteed under EU law is violated.[132] Hence, compliance with this right

[127] Schrems II, paragraph 176
[128] Ibid.
[129] Ibid. paragraph 175 and 176
[130] EU-Cananda PNR agreement and Schrems I
[131] Schrems II, paragraph 186
[132] Article 47 (1) CFREU

is essential to ensure that the level of data protection is essentially equivalent to the protection level guaranteed within the EEA.

As stated in the chapter above, the limitation of the fundamental rights must still respect the essence of such rights. In the context of Article 47 of the CFREU, the essence that must be respected according to the ECJ is the data subject's possibility to "*pursue legal remedies in order to (…) access (…) personal data, or obtain the rectification or erasure of such data*".[133] It is what is stipulated by legislation that is decisive. Such an understanding is consistent with the previous case-law, inter alia, *Schrems I*.[134]

In assessing whether the mechanisms after PS are adequate, the ECJ emphasized the EC finding, in the PS Decision, that FISC limits its supervisory role to surveillance programs' authorization, and further held that neither E.O 12333 nor PPD-28 gives EEA-based data subjects effective and enforceable rights.[135]

Previous case-law, *1/15 Opinion* and *Schrems I*, highlights the EC difficulties to ensure adequate judicial protection. Due to the shortcomings identified in the SH Decision's invalidation, an Ombudsperson mechanism was set out under the PS to ensure effective judicial protection.

According to the ECJ, the ombudsperson mechanism must be independent, impose meaningful remedies, and have enforcing powers.[136] The Court concluded that the Ombudsperson is not independent due to the Ombudsperson is appointed by and reporting to the Secretariat of State and is an integral part of the US State Department.[137] Thus, the Ombudsperson would work closely with the DNI who may demand communication disclosed if foreign persons located abroad are reasonably believed to communicate specified kind of foreign intelligence information.[138]

---

[133] Schrems II, paragraph 187.
[134] Ibid.
[135] Schrems II, paragraph 179-183
[136] Ibid., paragraph 195 and 196
[137] Ibid., paragraph 195
[138] See Chapter 6

Furthermore, the Court concluded that the ombudsperson mechanism did not impose meaningful remedies or have enforcing powers as the Ombudsperson did not have the power to enforce legally binding decisions. Consequently, the level of data protection provided by the PS is not essentially equivalent to the protection level guaranteed within the EEA.

Thus, the ECJ concluded that the EC attempt to ensure effective judicial protection for data subjects having their data transferred to a third country did not comply with Article 45 of the GDPR, read in light of Article 47 of the CFREU. This implies the EC's willingness to compromise to reach an agreement. In a possible future EU-US agreement it is vital that the EC ensures effective remedy and an independent court or administrative body.

8.3 Validation of SCCs

The following chapters will contain an analysis of the judgment's statements regarding the validation of SCCs. In addition, the chapters will assess whether the SCCs must be considered an invalid transfer tool for transfers of data to US due to the Court's findings under the PS invalidation assessment.

8.3.1 The Court's Decision

The ECJ upheld the EU SCCs of 2010, amended in 2016, as a valid transfer tool as the SCCs can be an effective mechanism to ensure adequate data protection and ensure the competent SA the opportunity to suspend transfers or terminate contracts.[139]

The SCCs contains contractual obligations for the controllers and processors as well as contractual ensured rights for data subjects, in addition to the powers of the competent SA's to suspend transfers and terminate contracts.[140]

It may seem like the main reason the SCCs is an effective mechanism for ensuring an adequate data protection level is due to the aforementioned power of the SA's. As stated in the Chapter 8.1, with respect to the Facebook judicial review by the Irish DPC, if the Court rules that the Irish DPC must review the preliminary decision, one can question if the SCCs is weakened as a transfer tool as the SAs decisive voice is less "powerful" than anticipated by

[139] Schrems II, paragraph 148

[140] Ibid., paragraph 138-147

the Schrems II case. After all the contractual mechanism of the SCCs is based on the responsibility of the competent SA's, or the controllers or processors.[141]

In assessing the SCC Decision, the ECJ establishes that the SCCs is valid on a general basis. In other words, contrary to the complaint of Mr. Schrems, the ECJ did not consider the validity of the SCCs in the view of transfers to the US specifically.

Even though the SCCs are valid transfer tools on a general basis, it is decisive whether the specific SCCs in the individual case in practice ensures an adequate level of protection. For the SCCs to be effective in practice, the data exporters need to consider, through an assessment of the third country's legislation, whether such legislation provides a level of data protection that is essentially equivalent to that of the GDPR and, where necessary, whether additional measures must be adopted.

The Court defended such an approach, arguing that the EC cannot adopt SCCs with detailed and specific clauses adapted to each receiving third country, as such SCCs would be the same as an adequacy decision under Article 45 of the GDPR. This argument supports the purpose of enabling the use of the SCCs as a transfer tool where the EC has not adopted an adequacy decision. Hence, the ECJ confirmed that SCCs contains generic contractual terms and must be supplemented by the contractual parties, as ordinary standard contracts usually must. The advantages of a contractual approach's are that standard agreements are easier to change and adapt than formal law.

One could argue that a transfer tool depending on the provided safeguards' soundness should not be considered a valid transfer basis as this may weaken the data protection of the individual. Thus, the SCCs are dependent on clarity in which additional measures are necessary to ensure an adequate level of protection.

[141] Schrems II, paragraph 134

8.3.2 Requirements for the SCCs to Ensure an Adequate Level of Data Protection

As stated in Chapter 3.3.2, data transfer to third countries can occur where "appropriate safeguards" are provided and where the data subject has enforceable rights and effective remedies per Article 46 of the GDPR.

When the ECJ assessed the term "appropriate safeguards", the Court read Article 45 and Article 46 in a complementary manner.[142] Consequently, the analysis used in determining the sufficiency of protections under Article 46 must consider the essential equivalence test and various factors per Article 45.

By referencing both Articles 45 and 46, it can be argued that the Court chose to disregard the hierarchical arrangement between these provisions, which is contrary to the structure of the GDPR.[143] Namely, one must first assess if the requirements of Article 45 is fulfilled and if not, then the requirements of Article 46 can be assessed. Such an understanding is based on the wording of Article 46 "*in the absence of a decision pursuant to Article 45(3)*[144]", and Recitals 107 and 108, as well as several statements from the ECJ in *Schrems II*.[145]

On the other hand, it can be argued that the reference from Article 46 to Article 45 does not lead to the Court scrapping the hierarchical system. But that the statement is intended as a pointer to which factors can be considered and the GDPR must be understood as an entirety. In addition, the fundamental rights must provide equal protection regardless of the transfer tool. Thus, all the provision under Chapter V of the GDPR should be read in connection with each other.

An effect of reading Article 46 and Article 45 in a complementary manner is that controllers and processors must carry out the same assessment as the EC. The difference in the level of expertise between the two is, in most cases, great. The point of reading the provisions in their entirety was to ensure equally adequate protection regardless of the transfer tool. It will be almost impossible, if not impossible, for controllers and processors in SMEs to ensure suffi-

[142] Schrems II, paragraphs 92-96 and 104

[143] Ibid.

[144] Ibid., paragraph 162

[145] E.g. Schrems II paragraph 95

cient data protection if they must make the same assessment as EC. Finally, it is the data subject's level of data protection that is weakened.

8.3.3 Case-by-Case Assessment of the SCCs

Even though the SCCs are valid transfer tools on a general basis, it is decisive whether the specific SCCs in the individual case in practice ensures an adequate level of protection.

As the SCCs are mere contractual guarantees, additional measures may have to be implemented to ensure that the SCCs, as a transfer tool, in practice, protect the individual's personal data.[146] However, the Court neither clarifies what additional measures shall entail nor how such measures shall achieve sufficient data protection level. Additionally, the Court did not state what the third country legislation assessment should entail. According to the ECJ, it falls to the data exporter to assess the applicable third country's legislation to confirm whether one must supplement SCCs with additional measures to ensure a level of protection that is essentially equivalent to that guaranteed by the GDPR.[147] The Court's lack of guidance with respect to these assessment creates several issues.

Regarding the uncertainty of the third country assessment, the ECJ, "*all circumstances*" of the transfer must be taken into consideration, including the "*relevant aspects of the legal system*" and "*any access by the public authorities*".[148] Additionally, according to Article 46 (1) of the GDPR, the data subjects must be afforded "*enforceable rights and effective legal remedies*". Thus, this will probably be relevant in the third country assessment. These statements offer some clarity to the assessment.

Assessing the legislation of a third country is comprehensive. The EC can spend several years on such an assessment. It will be very difficult for controllers and processors to discover essential "shortcomings" in the legislation and make sufficient assessment without clear guidelines on what such an assessment should entail.

[146] Schrems II, paragraph 133

[147] Ibid., paragraph 134

[148] Ibid., paragraph 104 and 146

Moreover, clarity is essential to identify which additional measures to implement as one must adjust the additional measures according to the level of protection in the applicable third country. Without knowing what possible "shortcoming" the third country's legislation has, it is impossible to implement reasonable enough additional measures that ensure adequate data protection.

However, as the ECJ did not provide any information about what additional measures shall entail or how the additional measures shall ensure an adequate level of protection, such unclarity may lead to discrepancies in the protection level, contrary to the continuity of afforded data protection under the GDPR.[149]

A practical response to the uncertainty and complexity of transferring personal data is data localization, which means placing data within the EEA. With data localization data the controllers and processors does not need to comply with the complex assessments and implementations as there will be no transfers outside the EEA. However, this is not a satisfactory solution as it will be contrary to the purpose of facilitating trade and the free flow of personal data under the GDPR. More about this in Chapter 9.2.2 of the thesis.

8.3.4 Transfer of Personal Data to US with SCCs

In assessing the SCC Decision, the ECJ establishes that the SCCs is valid on a general basis. In other words, and contrary to the complaint of Mr. Schrems, the ECJ did not consider the validity of the SCCs in the view of transfers to the US specifically.

After the invalidation of the PS, there is limited possibility to transfer personal data to the US, with other transfer tools, as the ECJ's concluded that FISA Section 702 and E.O 12333 provide the US authorities access to personal data through surveillance programs which interfere with the fundamental rights to privacy and personal data.

However, exporters can still transfer personal data to third countries with SCCs as transfer tool if additional measures are implemented and such additional measures ensures an adequate level of protection.

[149] EDPB 01/20, paragraph 64

As FISA Section 702 facilitates US authorities' access to personal data it is decisive that the additional measures prevent such access from the authorities as retention, access, and communication constitute interference with the fundamental rights.

FISA Section 702 only applies to ECSPs. This means transferring data to other importers than ECSPs implementing additional measure may prevent US authorities' access to the transferred data.

However, regarding transfer of personal data to the US where the importer is considered an ECSPs one can question if implementing additional measures in the SCCs will in fact ensure an adequate level of protection for transfer of personal data to the US.

9 EDPB Recommendations

The EDPB has adopted two recommendations due to the complexity of complying with the requirements set out in the *Schrems II* judgment. These Recommendations are submitted to public consultation, but they constitute an authoritative view of the effects of *Schrems II* on SCCs. Thus, the recommendations are based on the interpretation of the GDPR and the *Schrems II* judgment and contain several steps to assist data controllers and data processors complying to the Chapter V of the GDPR and the principle of accountability in practice. [150] These steps should be assessed case-by-case and before each transfer to ensure an essentially equivalent level of protection for the transfer of personal data to third countries.

The first recommendation describes measures that supplement transfer tools and set out six steps for data exporters to follow to ensure an adequate level of personal data protection.[151] Due to the invalidation of PS, in *Schrems II*, this recommendation is of particular importance for transfer of personal data to the US. Additionally, as is was no grace period after the decision it is reprehensible that EDPB spent five months before adopting these recommendations.

[150] EDPB Recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, p. 2
[151] Ibid.

The second recommendation provide guidance on the assessment of a third country's public authorities` access to personal data is justifiable. This is useful for data controllers and data processors when assessing if third countries legislation offer an adequate level of personal data protection, and probably for the EC when adopting new adequacy decisions.

Further, the following chapters will present and analyze the content of the six steps set out by the recommendations.

9.1 The Step-by-Step Guidance

9.1.1 The First Step and Second Step

The first step is to "*know your transfers*", which means that as a data exporter, one must have an overview of personal data that are and will be transferred, which is necessary to ensure sufficient protection of the transferred personal data. This step must be carried out before each transfer of personal data, including resuming ongoing transfers.[152]

The EDPB does not pronounce exactly what information about the transfers that must be mapped, beyond where the data is located and that one may look to the protocol register under Article 30 of the GDPR, also including onward transfers.[153] However, a precise elaboration is probably not necessary as the one processing data must decide what aspects of the transfers need to be mapped in order to gain full awareness.

According to the EDPB, the data must ensure compliance with the principle of data minimization under the GDPR, ensuring the data are adequate, relevant, and limited to what is necessary according to the transfer's purpose.[154]

Complying with this step is a difficult exercise, which the EDPB acknowledges. However, on a general basis, such an overview of personal data is necessary and vital to protect personal data in line with the GDPR.

[152] EDPB Recommendation 01/20, paragraph 12

[153] Ibid. paragraph 9 and 10

[154] Ibid. paragraph 11

After the exporter has identified and clarified the data transfers, the **second step** is to verify the transfer tool the data transfer relies on.[155] The recommendation refers to the transfer tools per Chapter V of the GDPR.[156] Inter alia, adequacy decisions, SCCs and BCRs, and derogations.

If an adequacy decision, after Article 45 of the GDPR, is the identified transfer tool, the exporter does not need to take any further steps other than monitoring the adequacy decision is still in force.[157] Thus, per *Schrems II*, transfers based on the PS must immediately terminate.

Like adequacy decisions, if the transfer tool is identified as derogations after Article 49 of the GDPR, the exporter does not need to follow any further steps.[158]

Lastly, if the verified transfer tool is one of the listed types in Article 46, like SCCs or BCRs, the recommendation requires the exporter to follow the set out steps and further assessment to ensure essential equivalent data protection level in the third country.[159]

9.1.2 The Third Step

According to this step, the data exporter must assess whether the "*appropriate safeguards*" of the selected transfer tool ensures that the level of protection guaranteed by the GDPR is in practice essentially equivalent to that guaranteed in the EEA, in the context of the specific transfer.[160] This assessment entails assessing if the third country's legislation prevents the transfer tool from complying with the requirements stipulated by the GDPR. Due to the uncertainty of what a third country assessment entails after *Schrems II*, the EDPB provides guidance through this step and the second recommendation.

[155] EDPB Recommendation 01/20, p. 2
[156] Ibid. paragraph 14
[157] Ibid. paragraph 19
[158] Ibid. paragraph 27
[159] Ibid.
[160] Ibid. paragraph 29 and 30

The assessment is vast and complex, where all actors involved in the transfer, the characteristics of every transfer, and the transfer's legal context should be taken into account in the assessment process.[161] Also, in some instances, in collaboration with the data importer. [162]
The EDPB lists circumstances that may impact the relevant legal context.[163] Inter alia, categories of personal data, the purpose of the data transfer, location of the stored data, if the data is in plain text or pseudonymized or encrypted, and if the data shall be transferred from the third country to another third country.[164]

The assessment of the third country's legislation is complicated as the exporter must consider all legislation that could affect the transfer tools and the protection per the transfer tools, especially the data subject's rights and laws regarding public authorities` access to personal data.[165] Thus, the EDPB has provided a second recommendation on European Essential Guarantees for Surveillance Measures (EEG), which sets out four requirements for assessing if the legislation governing the third country's public authorities` access to personal data is justifiable.[166] These are presented and discussed in the chapters below.

Regarding transfers of personal data to the US, the third country assessment is not necessary as the *Schrems II* judgment concluded that the public authorities` access to personal data is not justifiable.

9.1.2.1 The European Essential Guarantees for Surveillance Measures

These guarantees require an overall objective assessment, which means that all four guarantees must be seen in context and i.e. the likelihood of public authorities accessing personal data is not relevant.[167]

The recommendation is of importance to controllers and processors when assessing if the third country's data protection level is essential equivalent to the level within the EEA.[168] Ad-

[161] EDPB Recommendation 01/20, paragraph 30,31, 32 and 33
[162] Ibid. paragraph 30
[163] Ibid. paragraph 33
[164] Ibid.
[165] Ibid. paragraph 35 and 36
[166] Ibid. paragraph 39
[167] Ibid. paragraph 42 and 48

ditionally, the four guarantees must be a part of the EC assessment when issuing an adequacy decision, per Article 45 of the GDPR.[169]

After the data exporter has assessed all four guarantees, and if the assessment concludes that the third country does not fulfill the essential guarantee requirements the third country has an insufficient data protection level. [170] In that case, the exporter must follow the next step in the recommendation on surveillance measures. Thus, the transfer of data to the US must follow the next step. If opposite, the third country legislation can be regarded as justifiable, the transfer tool is effective and thus offers adequate protection. In that case, the exporter does not need to follow any further steps.

The purpose of the following chapters is to present the content of the four essential guarantees that must be included in the assessment of a third country.

9.1.2.1.1 Guarantee 1

The first listed guarantee is that the "*processing should be based on clear, precise, and accessible rules.*"[171] This is based on the fact that encroachment on fundamental rights, such as the right to the protection of personal data, must be stipulated by law according to Articles 8 (2) and 52 (1) of the CFREU. This means that the interference must be "provided by law".[172]

The EDPB clarifies the requirement, set out by the *Schrems II*, that the applicable law must be "clear and precise" as the recommendation provides numerous features the law should contain.[173] Among others, the subject to surveillance, duration on the interfering measure, the procedure to be followed for examining, using and storing the data obtained, and the precautions to be taken when communicating the data to other parties.[174] Additionally, the individual

[168] EDPB Recommendation 01/20, paragraph 53
[169] Ibid., paragraph 52
[170] Ibid. paragraph 51
[171] EDPB Recommendation 02/2020, paragraph 24
[172] Ibid., paragraph 26
[173] Schrems II, paragraph 176 and EDPB Recommendation 02/2020, paragraph 30
[174] EDPB Recommendation 02/20, paragraph 30

must be able to enforce the applicable law before an individual court and the interference must be foreseeable.[175]

It may seem like the recommendation means the term "law" only to apply to statutory law as the EDPB states that "law or practice" should be assessed. However, the term should also apply beyond statutory law.[176] Thus, the wording should be "law and practice". Such clarity of "law" is essential as it is decisive for the third country assessment outcome. If essential aspects of the third country's legislation are left out due to the lack of clarity of the term "law", it will impair the data subjects' data protection.

9.1.2.2 Guarantee 2

The second listed guarantee is the "*necessity and proportionality regarding the legitimate objectives pursued need to be demonstrated.*"[177] Like the guarantee above, this guarantee seeks to provide clarity to the Article 52 requirements of the CFREU.[178] Pursuant to this provision, a proportionality and necessity test must be met.

In regard to the principle of proportionality, "*the seriousness of the interference*" and "*the importance of the public interest*" must be proportionate to justify the limitation set out by law.[179] The more solid basis in assuming national security is threatened, the more interference with fundamental rights is justifiable.[180]

This way, the controller and processor know with certainty that disproportionate interference exists when the interference with the fundamental rights is great and there is little public interest in access to personal information. However, solely with such guidance, it will still be difficult to sufficiently complete the proportionality test.

Case-law can give more accurate guidance on the balance of legitimate encroachment on fundamental rights in relation to surveillance measures. An encouragement by the EDPB to look

[175] EDPB Recommendation 02/20, paragraph 27 and 31
[176] Recital 41 GDPR
[177] EDPB Recommendation 02/2020, paragraph 24
[178] Ibid., paragraph 32
[179] Ibid., paragraph 33
[180] Ibid., paragraph 34

to such relevant case-law might be helpful for controllers and processors. On the other hand, it may be too extensive for controllers or processors to make such case-law assessment.

Regarding what is considered serious interference, following the Schrems II judgment, the interference must be limited to what is strictly necessary. [181] With regard to the principle of necessity, the EDPB states that third country legislation allowing public authorities general access to data exceeds the limit of what is strictly necessary and does not respect the essence of the fundamental right to respect for private life.[182] Moreover, the recommendation holds that the objective criteria in light of the relevant processing's purpose in the third country legislation are decisive.

Even though the EDPB offers some guidance, the level of expertise to complete this assessment satisfactorily is high and one can question how data controllers and data processors can successfully complete this assessment.

9.1.2.3 Guarantee 3

The third listed guarantee is "*independent oversight mechanism*".[183] The EDPB seeks to clarify what is essential to assess for the oversight system to be considered independent.

Firstly, the EDPB emphasizes that both a court and an independent body, including the supervisory role, can constitute the oversight mechanism.[184]

Moreover, the EDPB holds that the oversight mechanisms' scope should be assessed, where the decisive factor is whether the oversight mechanism is effective, independent, and impartial.[185]

Regarding independence, the court or body must be sufficiently independent of both the executive and the public authorities that carry out the surveillance.[186] Also, the court or body must

[181] Schrems II, paragraph 176
[182] EDPB Recommendation 02/2020, paragraph 37
[183] Ibid. paragraph 24
[184] Ibid. paragraph 39
[185] Ibid.
[186] Ibid. paragraph 42

have sufficient power to be able to render binding decisions.[187] When assessing the supervisory body's independence, one must also consider the body's access to relevant documents, the member's legal status and the way they are appointed, and whether the supervisory body's activities are open to public scrutiny.[188]

Furthermore, the Recommendation stipulates that the review of surveillance measures should be assessed *ex-ante* or within a short time and further lays down what to consider when assessing surveillance measures.[189] It is the actual surveillance operation that is the subject of the assessment, where the measure must be limited to what is strictly necessary, as well as be subject to effective review by a court or a body whose decisions are binding.[190]

Making such an assessment in practice is complicated. After all, the EC has several times approved what should have been independent oversight mechanisms, but which has proven not to be independent after a judicial assessment by the ECJ.[191] Again, one can question the how data controllers and data processors can successfully complete this assessment.

9.1.2.4 Guarantee 4

Lastly and the fourth guarantee is that "*effective remedies need to be available to the individual.*" This guarantee follows from Article 47 of the CFREU, which stipulate that everyone has the right to an effective remedy before a court, and the essence that must be respected is the data subject's possibility to pursue legal remedies to access data or obtain the correction or erasure of such data.[192] Hence, the controller or processor must ensure the third country's compliance with the essence of Article 47 to make the limitation of the fundamental right to privacy justifiable.[193]

[187] EDPB Recommendation 02/20, paragraph 42
[188] Ibid.
[189] Ibid., paragraph 41
[190] Ibid., paragraph. 41
[191] Schrems I and Schrems II
[192] Article 47 CFREU
[193] EDPB Recommendation 02/20, paragraph 43

Additionally, the EEA data subjects should have the right to be notified when their data has been collected is highlighted as important by the EDPB.[194]

Moreover, the EDPB emphasizes that the court or the body must be "*independent and impartial*," as stated in the *Schrems II* judgment. Where the ability to examine individuals' complaints, the possibility to access all pertinent information, the power to make binding decisions on the intelligence services, and the ability to remedy non-compliance are essential.[195]

9.1.2.5 Further Remarks on the EEG Recommendation

As the strict requirements laid down by the EEG Recommendation offer little flexibility in the assessment of the legislation facilitating the third country's public authorities` access to personal data is justifiable and it is an objective assessment, one can question if the guarantees are to strict. Additionally, when requiring an objective assessment, the EEG guarantees ignores the risk-based approach. This is elaborated in the thesis Chapter 9.2.1.

Even if the EEG recommendation provides some guidance on the assessment of third country's legislation regarding surveillance measures, the third country legislation assessment is still comprehensive.

The comprehensive assessment suggests that in-depth knowledge or expertise is required to carry out the assessment to a sufficient degree. The fact that the EC can spend several years on such an assessment supports this argument. Thus, again, one can question how all types of SMEs can carry out this assessment for each transfer.

Due to the fact that the assessment is comprehensive, the assessment is at risk of not being sufficient, hence, data subjects' data protection level is at risk of being weakened.

Additionally, in some cases, other third country legislation must be assessed, as the ECJ states that all relevant legislation must be assessed. The Annex II in the recommendation of supplementary measures sets out a list with sources of information to look to when assessing a third

[194] EDPB Recommendation 02/20, paragraph 44

[195] Ibid., paragraphs 45 and 47.

country. This provides some guidance but also emphasizes the extensive task as the list is non-exhaustive, meaning other legislation can be relevant, and the list is comprehensive.

One can question why the EDPB has not published an assessment of third countries with numerous large data importers. Such guidance would make it easier for many data exporters to transfer data cross-border, in particular for the SMEs.

Overall, such an approach set out by the recommendation; the assessment outcome will most likely vary within the same third country legislation. One can argue that this is not fortunate as it underestimates the consistency of data protection for the EEA citizens, which the GDPR is seeking to facilitate as underscored by the *Schrems II* judgment.[196]

9.1.3 The Fourth Step

After the transfer impact assessment, identifying and adopting supplementary measures is the next step to ensure that the third country's data protection level is essentially equivalent to that guaranteed within EEA.[197] The fact that the EC clarifies additional measures is essential as the ECJ in the Schrems II case does not mention what these measures entail. These additional measures supplement the listed safeguards per Article 46 of the GDPR, in light of Article 45 (2) (a).[198]

The precondition for reaching this step, is that the third country does not have sufficient personal data protection, such as the US; thus, this guidance on additional measures is of particular importance to ensure an adequate level of data protection for transfers of personal data to the US. Is it possible to transfer data to the United States with these additional measures?

First, the data exporter must identify which supplementary measures will be most effective in protecting the personal data.[199] It is a subjective assessment of the specific case.[200] The EDPB sets out a non-exhaustive list of relevant factors; the type of data, whether this data should be

[196] Schrems II, paragraph 93
[197] EDPB Recommendation 01/20, paragraph 45
[198] Ibid. and Schrems II, paragraph 133
[199] EDPB Recommendation 01/20, paragraph 46
[200] Ibid.

transferred in plain text or pseudonymous or encrypted, as well as the complexity of the data transfers, and whether any further transfers should be mentioned.[201]

Moreover, the EDPB recommends several supplemental measures relevant for ensuring adequate personal data protection in the third country. The measures are non-exhaustive, thus other measures can be implemented.[202] The Recommendation divides the supplementary measures into contractual-, organizational-, and technical measures.

Combining different supplemental measures within these three listed categories will increase the data protection level.[203] However, according to the EDPB, contractual- and organizational measures will probably not ensure sufficient protection level without technical measures.[204]

It may seem like the EDPB holds that the technical measures are more important than the other measures. The technical measures' description is more comprehensive than the other measures, and several times, it is stipulated that the contractual- and organizational measures may only complement the technical measures, emphasizing that the EDPB is in such an opinion. There is great disagreement about whether contractual- or organizational measures can or cannot provide sufficient additional measures alone.

If the supplementary measures are effective, in practice, and provide essentially equivalent protection to the transferred personal data, data transfer can start or continue.[205] However, the fifth and sixth step must also be fulfilled. Suppose the essentially equivalent data protection does not exist due to the inability to identify and implement effective supplementary measures. In that case, the transfer of data cannot start, or the transfer must be suspended or ended.[206] However, if the transfer continue regardless of the inability to ensure an adequate level if protection the competent SA's must be informed and the SA can suspend or prohibit the transfer of personal data.[207]

---

[201] EDPB Recommendation 01/20, paragraph 49
[202] Ibid., paragraph 69
[203] Ibis., paragraph 47
[204] Ibid., paragraph 48
[205] Ibid., paragraph 51
[206] Ibid., paragraph 52
[207] Ibid., paragraph 53

Further, the contractual-, organizational-, and technical measures will be presented.

9.1.3.1 Organizational and Contractual Measures

The recommendation lays down a list of **organizational measures** that exporters can implement to ensure data protection consistency.[208] Some of these measures are organization methods, including strict and limited data access, internal guidelines on responsibilities for transfers of data and reporting deviations, as well as procedures for handling public authority's data access requests.[209]

However, organizational measures do not offer sufficient protection alone. Nevertheless, by implementing technical, contractual, and organizational measures in internal policies, exporters will document the fulfillment of measures.[210] Thus, ensure compliance with the demonstrating requirement under the principle of accountability set out under Article 5 (2) of the GDPR. Such documenting is considered another organizational measure, as well as the regular review of such internal policies to ensure implementation and compliance.[211]

Regarding **contractual measures**, the recommendations Annex II set out multiple contractual commitments. Such measures will usually apply to the contract parties, and the measures will not be binding for the third countries authorities. Such an understanding is based on *Schrems II*, which stipulated that the SCCs are not binding on third country authorities as they are mere contractual guarantees, but that SCCs are still valid as supplementary measures can be implemented. Consequently, contractual measures do not offer sufficient protection alone, but they can support and strengthen transfer tools and the third country's relevant legislation.[212]

The Recommendation includes examples of prerequisites for the contractual measures to be useful supplementary measures.[213] Firstly, the EDPB mentions implementing specific relevant

[208] EDPB Recommendation 01/20, paragraph 122
[209] Ibid., paragraph 131
[210] Ibid., paragraph 124
[211] Ibid., paragraph 136
[212] Ibid., paragraph 93
[213] Ibid., paragraph 96

technical measures in the contractual agreement between the parties as a contractual measure. This way, data exporters will ensure that the importer follows up on the technical measures.[214]

According to the EDPB, other contractual measures could be transparency obligations, inter alia, the data importer undertakes to inform the data exporter about public authorities` access to personal data through legislation and changes in such legislation. The implementation of such a clause would help the data exporter with the third country legislation assessment and implement appropriate and sufficient additional measures.

The data importer could also undertake to inform the data exporter about disclosure of such access request.[215] However, it is not certain that the importer will comply with a "disclosure of data access request"-clause in practice as legislation in the third country in question may have a rule stipulating that the importer cannot share such information. In this way, the importer will stand between complying with the contractual clause or the country's legislation. The decisive factor will probably depend on the criminal- and financial consequences.

Nevertheless, the data exporter could try to prevent such circumvention by adding contractual clauses binding the importer to use legal means to reject the public authorities` data access claim and obliged the importer to respect the data subjects` rights by, inter alia, assisting the data subject with enforcing rights.[216]

Lastly, other listed transparency obligations the importer could undertake are to prevent and not provide "back door" access for authorities, as well as provide audit and supervision for exporters.[217]

9.1.3.2 Technical Measures

Technical measures are connected to the technical processing of personal data.[218] The EDPB sets out seven use cases to describe scenarios where technical measures could or could not

[214] EDPB Recommendation 01/20, paragraph 97 and 98
[215] Ibid., paragraph 99
[216] Ibid., paragraph 112 and 120
[217] Ibid., paragraph 103 and 105
[218] Sandtrø, 2020, p. 10

ensure an adequate level of protection. The five first cases describe measures that would be effective, and the sixth and seventh cases describe measures that would not be effective.[219]

In particular, these use cases offer some guidance on which technical measures that can ensure an adequate level of protection for transfer of personal data to the US. However, all the listed scenarios are very specific, with many conditions that must be met, which can lead to a lot of situations not being caught by these use cases. If the situation does not suit these cases, a specific assessment must be made in the individual case.

Due to the thesis's limitation, five of the seven set-out use cases are presented and discussed. The first case not mentioned is Use Case 4, which sets out a scenario where the recipient is protected by a third country's law, e.g., attorney-client privilege. Additionally, Use Case 5 is not mentioned but sets out "split or multi-party processing" as a technical supplementary measure.

9.1.3.2.1 Use Case 1 and 3

Use Case 1 and 3, sets out "*encryption*" as a technical measure. The term "encryption" is not defined in the GDPR but is mentioned as a possible technical measure.[220] Neither is the term explained in the Recommendation. Encryption can be described as a technical procedure where data in clear text, also called data in the clear, becomes unreadable to unauthorized access as the data is being locked with a key, so-called encryption key, which cannot be unlocked again without the correct encryption key.[221]

The overall difference between the cases is that while Use Case 1 applies to data at rest, Use Case 3 applies to data in transit. With regard to transfers to the US, this means that Use Case 1 provides a technical measure to prevent access to data through PRISM surveillance program, legislated by FISA Section 702. While Use Case 3 provides a technical measure to prevent access to data through UPSTREAM surveillance program, legislated by FISA Section 702 and E.O 12333. However, the two cases are described with several premises that must be met for the additional technical measure to be sufficient in EDPB's opinion.

---

[219] EDPB Recommendation 01/20, Annex II

[220] Articles 32 (1) and 82 (2) (c) GDPR

[221] Datatilsynet, 2017

In Use Case 1, the Recommendation stipulates that it is permitted for a data exporter, located within the EEA, to use a hosting provider located in a third country for data storage if the encryption is sufficient and the provider does not require data in the clear.[222]

In Use Case 3, the EDPB sets out, if personal data is "*routed via a third country*" when transferring data to a destination with adequate data protection level per Article 45 of the GDPR, the transfer is permitted where the encryption is sufficient.[223]

For the encryption to be sufficient, several terms must be fulfilled. Multiple terms are similar in the two cases. The encryption must be "*state-of-the-art*" and "*robust against cryptanalysis*", flawlessly implemented, and consider the specific time-period the encryption is used, i.e., future decryption methods.[224]

When assessing whether the implemented encryption is "*robust against cryptanalysis*" the data exporter must consider the public authorities' "*resources and technical capabilities*" to conduct cryptanalysis.[225] As such information entails how authorities conduct investigations, it will probably be difficult to obtain such information. How data exporters should make such an assessment is unclear, especially SMEs that do not have as many resources or in-depth knowledge of such information.

Additionally, for the encryption to be sufficient, the encryption keys must be kept within the EEA or where the personal data is secured with adequate data protection and reliably managed by data exporters or entrusted entities by exporters. [226]

However, it seems that stricter requirements are set out for how the encryption key is handled under Use Case 1 as the EDPB states that the keys must be "*reliably managed*" and "*retained*

[222] EDPB Recommendation 01/20, paragraph 79
[223] Ibid., paragraph 84
[224] Ibid., paragraph 79 and 84
[225] Ibid., paragraph 79 nr. 2, and paragraph 84 nr. 7
[226] Ibid., paragraph 79 nr. 5 and 6, and paragraph 84 nr. 11

solely under the control of the data exporter".[227] While under Use Case 3, the EDPB pronounce that the keys must be "*reliably managed (..) by the exporter*".[228]

The Recommendation makes such a distinction because the encryption key must not be accessible to third-country public authorities, which does not ensure an adequate protection level, such as the US. This means, that US authorities can access data if the encryption key is with the US data importer. However, where the data is only routed via the USA and transferred to a country with an adequate data protection level, it will be more difficult for the authorities to access the personal data.

Furthermore, multiple premises are not alike, presumably because the cases have different scenarios that demand different measures to ensure sufficient data protection. Following Use Case 1, before transfer of data, "*strong encryption*" must be used when processing personal data.[229]

Regarding Use Case 3, the Recommendation stipulated that in those cases where transport encryption is not sufficient end-to-end encryption must be implemented.[230] Moreover, the exporter must rule out possible backdoors, the parties must concur on a "*trustworthy public-key certification authority or infrastructure*", and decryption of personal data must only be possible outside the merely transiting applicable third country.[231]

All these conditions must be met for the encryption to be considered acceptable, which sets out a high threshold for implementation. Whether this is possible to implement in practice can be questioned, also concerning costs. For example, how could an encryption in practice be "flawless"?

When encryption has such a high threshold as in these use cases, it will also often be expensive. According to Article 32 (1) of the GDPR, which stipulates "security of processing," the

[227] EDPB Recommendation 01/20, paragraph 79 nr. 5 and 6
[228] Ibid., paragraph 84 nr. 11
[229] Ibid., paragraph 79 nr. 1
[230] Ibid., paragraph 84 nr. 6
[231] Ibid., nr. 3, 4, and 10

"cost of implementation" could be considered when assessing which measures to implement. If EDPB had taken this into account, it might make the implementation easier for SMEs.

On the other side, public authorities have lots of power and recourses resulting in great opportunities to be able to decrypt information and access data. Which suggests that the measures must be strict in order to provide optimal protection.

However, is encryption the only way to ensure that public authorities not access data in transit and at rest in these scenarios? Perhaps the combination of several measures in these scenarios would be equally effective, but less costly and easier to implement for all types of data exporters.

9.1.3.2.2 Use Case 2

This scenario is especially applicable in these COVID-19 times. Where, inter alia, sharing data for analysis on coronavirus vaccination is essential for the vaccine maker. Suppose such data on individuals within the EEA is to be transferred to the US. Then this Use Case will provide guidance on how such a transfer can take place.

According to Use Case 2, "pseudonymization" of data before transfer for analysis to a third country is a sufficient additional measure when:

(i) It is not possible for the public authority in the third country to link the personal data to a specific data subject, nor can the data subject be singled out in a large group without the use of additional information.[232]

Additionally, when (ii) the additional information that can identify the data subjects, must be held separately within the EEA or a third country with adequate data protection per Article 45 of the GDPR, exclusively by the data exporter.[233]

(iii) Moreover, a thorough analysis must be made, ensuring the additional information is adequately secured against the third country's public authorities. In such an analysis, one must

[232] EDPB Recommendation 01/20, paragraph 80 nr. 1

[233] Ibid., paragraph 80 nr. 2

consider all the information that the third country may possess, which may lead to identifying the data subjects behind the pseudonymized data.[234]

Both (i) and (ii) are based on the definition of "pseudonymization" under Article 4 (5) of the GDPR. The definition stipulates that technical and organizational measures should be implemented to ensure that additional information and the identifying data are kept separate. However, the EDPB does not mention any organizational measures regarding this Use Case.

Regarding (iii) assessing any information leading public authorities to may reidentifying personal data, one can question how to access such knowledge about third-country authorities. Especially for SMEs as such knowledge probably will be comprehensive to access and assess.

As the only technical guidance the Recommendation sets out is (ii) keeping the additional information separately within the EEA or a destination with adequate level of protection, it is an easier measure to implement for all types of data exporters. However, one may question whether this will be sufficient to prevent advanced technicians from third-country authorities, particularly for transfer to the US to ECSP data importers.

9.1.3.2.3 Use Case 6 and 7

These cases stipulate two scenarios where access to data in the clear would not be qualified as supplementary measures as they would not ensure an adequate level of data protection. The cases will be presented separately, then the thesis will look into the set out common justification for the cases.

According to the scenario in Use Case 6, if data importers are "cloud service providers or other processors" located in a third country where the public authorities' access to data is contradicting with fundamental rights set out in Articles 47 and 52 of the CFREU, and data importers "needs access to data in the clear" to "execute the task assigned" from controllers, supplementary measures will not ensure an adequate level of protection for the data subjects.[235]

[234] EDPB Recommendation 01/20, paragraph 80 nr. 3

[235]Ibid., paragraph 88

Regarding, transfers of personal data to the US this means that no transfers of personal data in clear text to data importers in the US is allowed as *Schrems II* concluded that FISA Section 702 and E.O 12333 violates the fundamental rights. One can question if the EDPB have indented such strict interpretation.

Any cross-border transfers of personal data using cloud service providers (CSP) or other processors are affected by this scenario. Also, applying to where CSPs must support the service is considered remote access, which is a transfer of data.[236] This will affect numerous EEA-based controllers using US-based CSPs as having access to data in clear text is often crucial for securing the CSPs' service. For example, having access to email addresses for authorization data in order to manage the solution. In accordance with this Use Case, this will not be legal if these services cannot be delivered without the CSP's access to data in the clear. Whether the consequence is that data only can be transferred if the data is encrypted, pseudonymized, or anonymized or that no such technical measures will be sufficient, is discussed below.

In Use Case 7, the EDPB states that where remote access to data in the clear is possible for business purposes, implementing supplementary measures will not ensure an essentially equivalent data protection level. For this scenario to apply, the data must be available for the data importers through a "*commonly used information system*," typically within the "*same group of undertakings*".[237] Thus, this Use Case is aimed at transfers of data with BCRs as transfer tool. Moreover, "*the importer uses the data in the clear for its own purposes,*" and the applicable third country does not offer adequate protection as public authorities' access to data "*goes beyond what is necessary and proportionate in a democratic society*".[238]

Also in this scenario, for transfers of personal data to the US, this means that no transfers of personal data in clear text to importers in the US is allowed as *Schrems II* concluded that FISA Section 702 and E.O 12333 violates the fundamental rights. Again, one can question if the EDPB have indented such strict interpretation.

[236] See Chapter 7

[237] EDPB Recommendation 01/20, paragraph 90

[238] Ibid., paragraph 90 nr. 2 and 3

Multinational companies, with entities both inside and outside the EEA, which transfer personal data within the company's entities for, inter alia, human resources (HR) purposes will be significantly affected. US-based multinational companies headquarter often manage HR data on behalf of entities outside the United States, such as the EEA. Often fundamental functions of multinational companies depend on the transfer of such data between the entities. Thus, not being able to transfer data in the clear will significantly impact the operations of companies, which in turn can affect, among other things, jobs. Like Use Case 6, whether the consequence is that data only can be transferred if the data is encrypted, pseudonymized, or anonymized or that no such technical measures will be sufficient, is discussed below.

The lower paragraph in Use Case 6 and 7 states:

> "*In the given scenarios, where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection* ***if the data importer is in possession of the cryptographic keys***.[239]" (emphasis added)

It seems like the Recommendation prohibits almost all transfers when the personal data is readable in the third country, as not even the high threshold measures described in Use Cases 1 and 3 will be approved as supplementary measures.

Nonetheless, it may seem like this only applies where the data importer is in possession of the encryption keys. However, it is unclear whether this applies to where the importer has all the encryption keys or whether the importer can have one encryption key while the exporter has the other key.

The latter approach, regarding transfer to the US, where the US-based importer has one key and the EEA-based exporter has the other key, could be a solution as the exporter would have knowledge of the access as well as could assist with the access of the specific decryption of personal data. Additionally, the data exporter should implement encryption for data at rest and

[239] EDPB Recommendation 01/20, paragraph 89 and 91

in transit to ensure US authorities access to data is as limited as possible. If this could be a sufficiently additional measure is hard to know without further clarifications from the EDPB or a Court decision.

9.1.4 The Fifth Step and Sixth Step

If the data exporter implements supplementary measures after step four, the next step is the **fifth step** which sets out procedural steps. Exactly which procedural steps must be carried out depends on the specific transfer tool. [240] Further, SCCs and BCRs are presented.

The EDPB distinguishes between modified and unmodified SCCs. The modified SCCs implies modifying the clauses or adding contradicting additional measures to the SCCs. In that case, the exporter must seek the applicable national SA authorization for continuing the transfer as the modification changed the original transfer basis.[241]

On the other hand, unmodified SCCs do not involve any changes as the supplementary measures are in addition to the SCCs. Hence does not contradict directly or indirectly with the SCCs.[242] This means, that transfers can continue without approval from the competent SA. Nonetheless, according to the principle of accountability, the data exporter must ensure and document that the additional clauses does not undermine the level of protection provided by the SCCs and the GDPR.[243]

Regarding BCRs, the EDPB acknowledges that the interpretation of *Schrems II* applies to BCRs and further emphasizes why the judgment are relevant for this transfer tool. It is further stated that the third countries public authorities cannot be bound by the BCRs, as mere contractual guarantees are solely binding for the signing parties.[244] In addition, third countries legislation could affect the protection level ensured by the BCRs.[245]

---

[240] EDPB Recommendation 01/20, paragraph 55
[241] Ibid., paragraph 57
[242] Ibid., paragraph 56
[243] Ibid., paragraph 56
[244] Ibid., paragraph 58
[245] Ibid., paragraph 59

Unlike the SCCs above, the Recommendation does not advise how these procedural steps must be considered regarding BCRs but instead states that the EDPB are not sure about the precise impact of the judgment on BCRs and must therefore later return to a statement on this.[246]

Additionally, the EDPB states that data exporters and importers using BCRs as a transfer tool must assess whether the third country in question in practice ensures an essentially equivalent level of protection and implements supplementary measures if necessary to ensure an adequate level of protection.[247]

The **sixth step** emphasizes the principle of accountability under Article 5 (2) of the GDPR and holds that the exporter must regularly review development in the third country. Which means having useful internal control measures in place, so exporters make sure to suspend or stop transfers if they become aware of conditions that are not legal.[248] Which applies especially to changes in whether the additional measures are no longer effective in the concerned third country or the importer is unable to comply with the obligations after the transfer tool per Article 46 of the GDPR.[249]

9.2 Remarks on the EDPB Recommendations

9.2.1 The EDPB Ignores the Risk-Based Approach

In order to ensure sufficient data protection, assessing risks is fundamental and decisive. The fact that a risk-based approach is at the core of the GDPR is expressed through several provisions combined with recitals and case-law.[250] Particularly relevant for this thesis are Article 46 of the GDPR and the *Schrems II* case, both of which confirm such an approach. The Recommendations are not in line with neither the GDPR nor the *Schrems II* judgment, as the possibility of a risk-based approach has been eliminated.

[246] EDPB Recommendation 01/20, paragraph 59

[247] Ibid., paragraph 60

[248] Ibid. paragraph 62 and 63

[249] Ibid. paragraph 63

[250] Inter alia, Articles 24, 25, 32, 34, 35 and recitals 74, 83, 89, 90, 91 GDPR

The Schrems II judgment recognizes such an approach when stipulating that controllers and processors must make "case-by-case" assessment and "all the circumstances of the transfer" are relevant when defining the legality of the transfer.[251]

Moreover, Article 46 sets out risk-based transfer tools as "appropriate safeguards", which must be implemented before the cross-border transfer of personal data is valid. In order to implement "appropriate" measures, one must consider the risks of transferring data and factors regarding the processing of data such as the "*the nature, scope, context and purpose*".[252]

As the Recommendations stipulates that the controllers and processors must secure compliance by ensuring implementation of effective legal, technical, and organizational measures, but omit the requirement of "appropriate", the EDPB disregard the risk assessment.[253]

Regarding which factors are to be taken into account when implementing appropriate measures according to the GDPR, the EDPB does not take a position on the "nature" of the transferred data. The GDPR distinguishes between ordinary personal data and special categories of personal data. Such a distinction is stipulated due to the special categories of personal data contain sensitive information on individuals. Hence, stricter requirements are required to process such data.[254]

The fact that the Recommendations do not make such a distinction is blameworthy. The one responsible for the transfer of data is at risk of either using too many resources on protection of personal data that does not need as much protection or, worse, implements too limited measures for the special categories of personal data, endangering the data subjects fundamental right to private life and respect of personal data.

Additionally, the Recommendation six-step assessment does not implement a risk-based approach. Where after step three, an objective assessment of the third country legislation must be carried out, and further states specifically that the likelihood of authorities' access is not

[251] Schrems II, paragraph 112, 134 and 146
[252] Article 25 (1), 32 (1) GDPR, Recital 74
[253] EDPB 01/20, paragraph 3
[254] Article 9 GDPR

relevant.[255] Not considering the risk of public authority's access to data can be criticized. Such an approach would mean that one should only consider the third country's surveillance legislation theoretical aspects. The legislation may give a theoretical impression that the authorities' access to data is not so great, while it is the opposite in practice. This may lead to disproportional measures that could weaken the level of data protection.

Moreover, as previously stated, the six steps set out in the Recommendations stipulate how to apply the principle of accountability to data transfers in practice. Even if the principle differs from the risk-based approach, the effect of the ignoring of risk assessment can affect controllers or processors in practice. According to the principle every controller or processor must comply with the GDPR regardless of size, industry or type of personal data that is processed. In this context, one can argue that the contrary assessment approaches in the GDPR and the Recommendations complicate the compliance for all controllers and processors, especially for SMEs. As they are just as responsible as big cooperate in complying with the GDPR, one can question if there is an unreasonable amount to deal with.

9.2.2 Data Localization

As stipulated in Chapter 6.4.3, the natural response to *Schrems II* is data localization. This means placing the data within the EEA; thus, the controllers and processors do not have to comply with Chapter V under the GDPR. The EDPB could avoid data localization by clarifying the uncertainties and the complexity in complying with the transfer provisions after *Schrems II* in the recommendations.

However, even if the EDPB provided some guidance on assessing the level of protection in third countries and implementing additional measures. The compliance is still comprehensive, particularly for SMEs without the required expertise. In practice, this will pressure organizations to locate information within the EEA or in countries with adequacy decisions, so-called data localization. Alternatively, pressure organizations in countries outside the EEA, like US organizations, not to offer their services to- and process personal data on EEA-based individuals.

[255] EDPB 01/20, paragraph 42

Data localization is not desirable since it will be contrary to the purpose of facilitating trade and the free flow of personal data under the GDPR and could weaken the global economy.

10 The Future of Personal Data Transfers to Third Countries

Transfer of personal data to third countries post-*Schrems II*, in light of the EDPB Recommendations, can be summarized into two words: ambiguity and comprehensive.

To transfer personal data from the EEA to third countries, per *Schrems II*, exporters using transfer tools under Article 46 per the GDPR must assess the third country's legislation, particularly whether authorities have access to data, and the necessity of implementing additional measures accordingly. The unclarity about what such a third country's assessments shall entail and what additional measures shall be implemented may lead to data exporters failing to ensure an adequate level of protection, which weaken the data subjects data protection level, and may lead to discrepancies in the protection level, contrary to the continuity of afforded data protection under the GDPR.

However, according to the EDPB Recommendations, six comprehensive steps should be carried out for each transfer to ensure an adequate level of protection. As these steps are detailed, they do offer some guidance. Nevertheless, the assessments set out are too strict and complex for all types of data exporters to ensure an adequate protection level.

Regarding the transfer of personal data to the US post-*Schrems II*, it is possible to transfer data in practice, but it is limited. It is no longer possible to transfer data based on the PS. This means that exporters must use other transfer tools and must ensure, through additional measures, that the transfer tools provide adequate protection against access to data from US authorities.

However, according to the EDPB, it is impossible to transfer data in clear text to the US, as US authorities can access personal data through surveillance programs legislated by FISA Section 702 and E.O 12333. Such an understanding of *Schrems II* hits very hard, and one may question whether EDPB has been too strict.

I believe that in order to ensure continuity transfer to third countries in the future, EDPB must change its recommendation and offer less stringent and comprehensive requirements, so all data exporters have the opportunity to follow the recommendations with a sufficient result, regardless of industry or knowledge. In addition, I believe that it is important for EC to reach a new transfer agreement with the US, but this time ensure an adequate level of data protection. Which is easier said than done.

Table of reference

Treaties

CFREU	Charter of Fundamental Rights of the European Union, (2012) OJ C 26/391
ECHR	European Convention European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No. 11 and 14 (1950) ETS 5
TEU	Consolidated versions of the Treaty on European, 2012/C 326/01
TFEU	Consolidated version of the Treaty on the Functioning of the European Union, (2012) OJ C 326/47

Legislation

EU Legislation

DPD	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.
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).

US Legislation

FISA	Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261 (codified in scattered sections of 50 U.S.C.).
E.O 12333	Federal Register Vol. 40, No. 235 (December 8, 1981), amended by EO 13284 (2003), EO 13355 (2004), and EO 13470 (2008))

PPD-28 Presidential Policy Directive 28 - Signals Intelligence Activities (January 17, 2014)

Case Law

The European Court of Justice

C-317/04 and C-318/04 EU:C:2006:346

Case C–362/14 Schrems I EU:C:2015:650

Cases C-203/15 and C-698/15 Tele2 Sverige/Watson EU:C:2016:970

Case C-311/18 Schrems II EU:C:2020:559

Opinion by the European Court of Justice

OPINION 1/15 EU:C:2017:592

Non-binding Opinions

Opinion of Advocate General Saugmandsgaard Øe on Case C-311/18 (19 December 2019)

WP29, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision (16/EN WP 238) (13 April 2016)

Non-binding Recommendations

European Data Protection Board (EDPB). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. (10 November 2020)

European Data Protection Board (EDPB). Recommendations 02/2020 on the European Essential Guarantees for surveillance measures. (10 November 2020)

Reports and other Documents

Bazan, E. B. (2004). Report for Congress: The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions. Congressional Research Service.

European Data Protection Supervisor (EDPS). (2014) The transfer of personal data to third countries and international organisations by EU institutions and bodies - Position paper

European Parliament Research Service (EPRS). (2017). At a glance. CJEU Opinion on EU-Canada PNR agreement.

Legal Literature

Books

Fahey, E. (2018). *Institutionalisation beyond the Nation State. Transatlantic Relations: Data, Privacy and Trade Law.* Springer.

Fuster, G. G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU.* Springer.

Bygrave, L., Kuner, C., Docksey, C., Drechsler, L.. (2020). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press.

Voigt, P., Bussche, A.. (2017). *The EU General Data Protection Regulation – A practical guide*. Springer.

Sharma, S. (2019). *Data Privacy and GDPR Handbook*. Wiley.

Skullerud, Å. B., Rønnevik, C., Skorstad, J., & Pellerud, M. E. (2018). *Personvern-forordningen (GDPR)*. Universitetsforlaget.

Suda, Y. (2018). *The Politics of Data Transfer.* New York: Routledge.

Articles

Adams, B. (2019). Striking a Balance: Privacy and National Security in Section 702 U.S. Person Queries. *Washington Law Review Volume 94*, pp. 401-452.

Johnson, B. M. (2016). Foreign Nationals' Privacy Interests Under U.S. Foreign Intelligence Law. *Texas International Law Journal*, 229-257.

Kuner, C. (2016). Reality and Illusion in EU Data Transfer Regulation Post Schrems. *German Law Journal*, pp. 881-918.

Sandtrø, J. (2020). Overføringer av persopplysninger utenfor EØS – hva gjør vi etter Schrems II?. *sandtro.no.*

Web-sources

Datatilsynet, *Kryptering* (07.03.2017) https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikerhet-internkontroll/kryptering/

European Commission, *Adequacy Decision – Third Countries* https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Noyb, *Irish DPC agrees to decide swiftly on Facebook's EU-US transfer*, (13.01.21) https://noyb.eu/en/irish-dpc-agrees-decide-swiftly-facebooks-eu-us-transfers